Cyberdefense

Communiqué de presse
le 3 juillet 2024

Le nombre de victimes de cyber-extorsion a augmenté de 77 % ; les petites entreprises sont 4 fois plus touchées que l'ensemble des moyennes et grandes entreprises, révèle Orange Cyberdefense

- Depuis 2020, la cyber-extorsion touche directement les entreprises dans 75 % des pays du monde.
- Le secteur de la santé et de l'assistance sociale enregistre la plus forte croissance des cyber-extorsions (+160 % d'une année sur l'autre).
- L'IA générative pourrait à terme renforcer l'écosystème des menaces au niveau mondial.

Orange Cyberdefense, la filiale du Groupe Orange dédiée à la cybersécurité, publie aujourd'hui son dernier rapport sur la cyber-extorsion : « Cy-Xplorer 2024 ». En examinant les données de 11 244 entreprises, des victimes confirmées, les résultats montrent une forte augmentation (77 % d'une année sur l'autre) du nombre de victimes de cyber-extorsion (Cy-X) au cours des 12 derniers mois. L'analyse suggère que le chiffre réel soit 50 à 60 % plus élevé que les observations directes effectuées, en raison de la nature dynamique et en constante évolution de l'écosystème.

Une majorité de victimes dans les pays anglophones

La Cy-X continue de se propager à travers le monde. Des victimes sont enregistrées dans 75 % des pays depuis 2020. Les États-Unis, le Canada et la Grande-Bretagne représentent le plus grand nombre de victimes, conformément au poids de la langue anglaise dans l'économie mondiale. En plus d'être la région la plus touchée, les États-Unis ont également connu la croissance la plus rapide, 108 %, suivis de près par la Grande-Bretagne et le Canada, avec respectivement 96 % et 76 %. Parmi les autres régions où la croissance est importante figurent les pays nordiques et l'Afrique, avec des taux de croissance de 78 % et 100 %, bien que sur des bases de départ beaucoup plus faibles.

Les attaquants déploient des schémas de ciblage opportunistes

Alors que les attaques ciblées et sophistiquées contre de grandes entreprises sont les plus connues, nous avons observé des modèles de comportement qui suggèrent une approche beaucoup plus opportuniste. Ainsi, les petites entreprises de moins de 1 000 employés sont 4,2 fois plus susceptibles d'être impactées par la Cy-X que les moyennes et grandes

entreprises. Nous pensons que cela est dû au nombre croissant de petites entreprises qui n'échappent plus aux attaquant qui frappent désormais partout où ils peuvent.

Les secteurs de la santé enregistrent la plus forte croissance des Cy-X

Les entreprises du secteur industriel ont continué d'être les plus touchées dans le monde par la Cy-X (21 %). Cependant, au cours des 12 derniers mois, nous avons vu pour la première fois le secteur de la santé et de l'assistance sociale rejoindre les trois secteurs les plus impactés. Il enregistre le taux de croissance le plus élevé, soit 160 % d'une année sur l'autre. Historiquement, lors de la crise de COVID-19 et jusqu'à récemment, les attaquants avaient fait preuve d'un certain degré de « retenue morale ». Aujourd'hui, cela s'estompe. LockBit s'est attribué le mérite d'avoir compromis deux importants établissements de santé américains, l'hôpital de la région de Carthage et le centre médical Claxton-Hepburn, entre autres, et le groupe ALPHV/BlackCat a revendiqué une attaque importante contre Change Healthcare.

La re-victimisation apparaît comme une nouvelle tendance

Nos recherches ont révélé plus de 200 cas de re-victimisation, une situation à la trajectoire ascendante depuis 2023 et qui semblent s'accélérer. Au premier trimestre 2024, il y a déjà eu 39 re-victimisations et cette tendance devrait se poursuivre. Nos recherches révèlent que les données de certaines victimes ont été publiées jusqu'à trois fois sur un site de fuites dédié. En outre, il existe des incidents où les données des victimes ont été publiées par différents attaquants avec un long délai entre les publications, ce qui indique une tentative d'attaquer et d'extorquer à nouveau les victimes.

L'IA générative renforce l'idée d'une mondialisation des Cy-X

Nos données suggèrent que l'IA n'a pas d'impact significatif sur la Cy-X à ce stade. L'IA générative reste toutefois un sujet de préoccupation sérieux. Elle pourrait permettre en effet d'irriguer l'écosystème des menaces cyber à un niveau mondial, en fournissant aux attaquants les outils dont ils ont besoin pour franchir les barrières linguistiques et culturelles qui, jusqu'à présent, ont potentiellement protégé certaines régions d'impacts plus importants.

Un écosystème appréhendé par les forces de l'ordre mais qui reste dynamique

Malgré le démantèlement par les forces de l'ordre d'importants groupes de cyber-extorsion, tels que RagnarLocker, ALPHV/BlackCat et LockBit, il n'y a pas eu de diminution notable du nombre de victimes. Les recherches ont montré la volatilité générale de l'écosystème des attaquants. Un tiers des groupes que nous suivons disparaissent chaque année, tandis qu'un nombre équivalent apparaissent dans le même délais. De plus, la moitié des attaquants identifiés sont dissous ou renommés en moins de 6 mois.

« *Les récentes opérations menées par les forces de l'ordre sont importantes. Toutefois le nombre de victimes de Cy-X continue d'augmenter à un rythme alarmant notamment en raison d'attaquants de plus en plus opportunistes et qui ne reculent devant rien. C'est une bataille continue et complexe en raison d'un écosystème décentralisé et fragmenté* », déclare **Hugues Foulon, CEO d'Orange Cyberdefense**. *« Les petites entreprises sont désormais les principales victimes de cette criminalité. Dans ce contexte, il y a un réel besoin pour toutes les organisations d'unir leurs forces et d'agir en travaillant ensemble* ».

« *L'émergence et l'accélération de la re-victimisation constituent une tendance préoccupante que nous suivons de près. Son impact est réel et expose les entreprises à plusieurs formes de préjudice lorsqu'elles restent sous l'emprise d'un groupe d'attaquants* », a déclaré Diana Selck-Paulsson, **Lead Security Researcher, Orange Cyberdefense**. « *La cybercriminalité ne connaît pas de frontières. Les menaces continuent d'évoluer parallèlement à l'émergence de nouvelles technologies telles que l'IA générative. Nous devons continuer à nous adapter et nous préparer à la mondialisation des Cy-X et de son écosystème.* »

Orange Cyberdefense surveille les activités de cyber-extorsion en permanence depuis 2020 et a recueilli des informations sur plus de 11 200 victimes à ce jour. La méthodologie complète est disponible dans le rapport :
https://www.orangecyberdefense.com/global/white-papers/cy-xplorer-2024

À propos d'Orange Cyberdefense
Orange Cyberdefense est l'entité du Groupe Orange dédiée à la cybersécurité. Elle fournit ses services à 8 700 clients dans le monde. En tant que leader européen des services de cybersécurité, Orange Cyberdefense s'efforce de protéger les libertés individuelles et de construire une société numérique plus sûre. Nos capacités de services puisent leur force dans la recherche et le renseignement, ce qui nous permet d'offrir à nos clients une connaissance inégalée des menaces actuelles ou émergentes. Forts de plus de 25 ans d'expérience dans le domaine de la sécurité de l'information, de 3 000 experts, de 18 SOC et de 14 CyberSOC répartis dans le monde entier, nous savons répondre efficacement aux problématiques globales et locales de nos clients. Nous les protégeons sur l'ensemble du cycle de vie des menaces dans plus de 160 pays.

A propos d'Orange
Orange est l'un des principaux opérateurs de télécommunications dans le monde, avec un chiffre d'affaires de 39,7 milliards d'euros en 2023 et 129 500 salariés au 31 mars 2024, dont 72 500 en France. Le Groupe servait 282 millions de clients au 31 mars 2024, dont 243 millions de clients mobile et 21 millions de clients haut débit fixe. Le Groupe est présent dans 26 pays (y compris les pays non consolidés). Orange est également l'un des leaders mondiaux des services de télécommunications aux entreprises multinationales sous la marque Orange Business. En février 2023, le Groupe a présenté son plan stratégique "Lead the Future", construit sur un nouveau modèle d'entreprise et guidé par la responsabilité et l'efficacité. "Lead the Future" capitalise sur l'excellence des réseaux afin de renforcer le leadership d'Orange dans la qualité de service.
Orange est coté sur Euronext Paris (symbole ORA) et sur le New York Stock Exchange (symbole ORAN).
Pour plus d'informations (sur le web et votre mobile) : www.orange.com, www.orange-business.com et l'app Orange News ou pour nous suivre sur X : @presseorange.
Orange et tout autre produit ou service d'Orange cités dans ce communiqué sont des marques détenues par Orange ou Orange Brand Services Limited.

Contact presse : Emmanuel Gauthier – emmanuel2.gauthier@orange.com – 06 76 74 14 54