Communiqué de presse
Paris, le 25 novembre 2022

Security Navigator 2023 d'Orange Cyberdefense : des menaces dominées par la cyber-extorsion, une augmentation des attaques en Europe et une exposition élevée des PME, de l'industrie et du secteur public.

Orange Cyberdefense, la filiale d'Orange et leader européen des services de cybersécurité, livre aujourd'hui les conclusions et analyses de son rapport **Security Navigator 2023 :**

- Toutes les entreprises sont confrontées à des attaques. Les logiciels malveillants représentant 40 % des incidents CyberSOC (Centres opérationnels de détection et réponse).
- Avec plus de 99 000 incidents traités cette année, le nombre recensé est en augmentation de 5 %. La moyenne est de 34 incidents par mois et par client, soit un incident par jour et par organisation.
- Un net déplacement de la localisation géographique des victimes des cyber-attaques est observé. De 2021 à 2022, la diminution du nombre de victimes basées en Amérique du Nord (-8 % aux États-Unis, -32 % au Canada) a été compensée par l'augmentation de celles en Europe (+18 %), au Royaume-Uni (+21 %), dans les pays nordiques (+138 %) et en Asie de l'Est (+44 %).
- Les petites entreprises[i] (49 %) ont spécifiquement fait l'objet d'attaques par logiciels malveillants. Le secteur industriel est le plus touché tandis que l'administration publique fait face au plus grand nombre d'incidents d'origine interne (66 %).
- Près de la moitié (47 %) de l'ensemble des incidents de sécurité détectés sont provoqués par des acteurs en interne, délibérément ou accidentellement.
- Pour la première fois, le Security Navigator Report inclut des données de près de 5 millions de mobiles, illustrant les différences de vulnérabilité entre Android et iOS.

Security Navigator 2023 – Malgré un ralentissement, les incidents augmentent de 5%

L'analyse porte sur 99 506 incidents potentiels ayant fait l'objet d'une investigation par nos CyberSOC, soit un nombre d'incidents en augmentation de 5 % par rapport à 2022. Ce rapport montre les signes encourageants d'un ralentissement du rythme des attaques, mais plusieurs facteurs restent préoccupants et les défis à relever sont nombreux.
Nos données montrent que les entreprises mettent encore 215 jours en moyenne pour corriger une vulnérabilité signalée. Dans le cas d'une vulnérabilité critique ou élevée, selon nos experts de Ethical Hacking, plus de six mois s'écoulent avant l'application d'un correctif. Si la cyber-extorsion touche des entreprises de toutes tailles dans le monde entier, les petites entreprises représentent 82 % du total des victimes.

Alors qu'au commencement de la guerre en Ukraine, nos équipes ont observé une nette diminution de la fréquence des cyber-attaques, celle-ci est rapidement repartie à la hausse.

La cyber-extorsion reste la forme d'attaque dominante, mais la localisation des victimes se déplace clairement de l'Amérique du Nord vers l'Europe, l'Asie et les marchés émergents

Les rançongiciels et les attaques de cyber-extorsion continuent de représenter une menace majeure pour les organisations du monde entier. Les mois de mars et d'avril ont été marqués par des pics notables d'activité de ransomwares, avec notamment Lapsus$, les fuites de données de Conti, ainsi que des préoccupations liées à la guerre en Ukraine. Simultanément, 40 % des incidents traités par nos CyberSOCs ont impliqué des logiciels malveillants.

Par ailleurs, un déplacement clair de la localisation des cibles est constaté, tel qu'illustré par le nombre de victimes de cyber-extorsion en diminution de 8 % en Amérique du Nord et de 32 % au Canada, mais en augmentation en Europe, en Asie et sur les marchés émergents. De 2021 à 2022, le nombre de victimes a augmenté de 18 % dans l'Union européenne, de 21 % au Royaume-Uni, de 138 % dans les pays nordiques, de 44 % en Asie de l'Est et de 21 % en Amérique latine.

Nous avons également constaté que des changements spectaculaires s'opéraient au niveau des groupes criminels les plus actifs. Il ne reste en effet dans ce « Top 20 » de 2022 que six groupes présents en 2021. Après la dissolution de Conti, Lockbit2 et Lockbit3 sont devenus les acteurs majeurs de la cyber-extorsion avec plus de 900 victimes à eux seuls.

Nous constatons également le caractère opportuniste des attaques. Près de 90 % de tous les acteurs malveillants que nous avons tracés ont revendiqué des victimes aux États-Unis, par exemple. Plus de 50 % ont attaqué le Royaume-Uni. Plus de 20 % ont même touché le Japon – un des pays de notre ensemble de données avec le plus petit nombre de victimes.

Les PME, le secteur industriel et le secteur public particulièrement vulnérables

Petites et moyennes entreprises

Les petites entreprises sont 4,5 fois plus nombreuses à être victimes de cyber-extorsion que les moyennes et grandes entreprises réunies. En proportion, cependant, les grandes entreprises restent beaucoup plus touchées. Les TPE et PME sont particulièrement sujettes aux malwares. 49 % d'incidents contre 35 % en 2021. Le coût moyen d'une fuite de données étant estimé à 1,9 million de dollars pour les entreprises de moins de 500 employés[ii], les vulnérabilités font courir un risque de faillite à de nombreuses PME.

Entreprises du secteur public

Le secteur public est à l'origine de la cinquième plus grande part d'incidents traités avec également le plus grand nombre liés à l'ingénierie sociale. Si dans la plupart des secteurs, la majorité sont déclenchés en interne, dans le secteur de la santé, 76 % sont attribuables à des acteurs externes tels que des cybercriminels et des groupes APT (groupes de cyberespionnage soutenus par des gouvernements).

Le secteur industriel reste le secteur le plus touché en nombre de victimes

Malgré le fait d'être l'un des secteurs les plus disposés à payer des rançons, l'industrie manufacturière reste le secteur le plus touché en nombre de victimes de cyber-extorsion (Cy-X). Les criminels compromettent souvent les systèmes informatiques « conventionnels »,

moins bien gérés, plutôt que les systèmes opérationnels (Operational Technology – OT) plus spécialisés. En effet, nos données montrent que les entreprises du secteur mettent en moyenne 232 jours pour corriger les vulnérabilités. À l'égard de cet indicateur, seules quatre autres industries se classent moins bien.

Des vulnérabilités critiques persistent et les délais dans l'application des correctifs menacent la sécurité

Nos chercheurs ont identifié la persistance inquiétante de vulnérabilités graves sur les systèmes informatiques des entreprises, avec 47 % identifiées comme d'une gravité « critique » ou « élevée ». Pour celles critiques, les organisations prennent souvent plus de six mois pour appliquer les correctifs… Les autres vulnérabilités peuvent donc persister beaucoup plus longtemps voire ne jamais être corrigées.
Dans les hôpitaux 491 jours sont en moyenne nécessaires pour corriger les failles. Dans les transports, les correctifs sont appliqués après 473 jours en moyenne. Par opposition, le temps moyen pris par nos hackers éthiques pour découvrir une vulnérabilité sérieuse est de 7,7 jours.

Le dilemme humain

En matière de cybersécurité, les employés forment la première ligne de défense d'une entreprise, mais ils peuvent aussi représenter son maillon le plus faible.
Dans l'administration publique, la plupart des incidents délibérés ou accidentels que nous avons traités sont attribuables à des sources internes. Pour le secteur industriel manufacturier, 58 % des incidents trouvent leur origine en interne. 64% pour le secteur du transport et de l'entreposage.
Notre rapport indique comment des niveaux plus élevés de surveillance améliorent l'efficacité des contrôles, mais génèrent également plus de faux positifs, entraînant potentiellement une plus grande pression sur les professionnels de la cybersécurité. Et ce, dans un secteur qui peine à pourvoir plus de 300 000 postes vacants, rien que dans la région EMEA[iii].

Sécurité mobile : iOS vs Android

Pour la première fois le Security Navigator Report 2023 inclut des données propriétaires sur les niveaux de mises à jour de sécurité de près de 5 millions d'appareils mobiles. Des recherches tierces suggèrent qu'en 2021, iOS et Android ont tous deux eu leur part de vulnérabilités : 547 pour Android et 357 pour iOS. 79 % des vulnérabilités Android ont été considérées comme peu complexes contre seulement 24 % pour iOS.

Dans le rapport Security Navigator, nous examinons les vulnérabilités graves d'Apple et d'Android afin de déterminer le temps nécessaire à l'écosystème pour déployer les correctifs requis. Dans un cas iOS, nous avons déterminé qu'il a fallu 224 jours pour que 90 % de l'écosystème Apple passe à la version corrigée. Pour Android comme pour iOS, il apparaît qu'environ 10 % de la base d'utilisateurs n'appliquera jamais les correctifs correctement.
Les résultats montrent qu'une plus grande proportion d'utilisateurs d'iPhone est menacée lors de la divulgation d'un problème de sécurité, ce qui s'explique par l'homogénéité du système. Les utilisateurs migrent néanmoins rapidement vers une nouvelle version, puisque 70 % d'entre eux appliquent un correctif dans les 51 jours suivant sa publication. La nature plus fragmentée de l'écosystème Android signifie que les appareils sont souvent laissés

exposés à un plus grand nombre d'anciennes vulnérabilités, tandis qu'un plus petit nombre d'appareils peut être compromis en utilisant des failles nouvelles.

« *Les derniers mois ont été particulièrement denses en termes d'évènements macro-environnementaux, néanmoins l'écosystème de la cybersécurité en ressort plus vigilant et uni. Les cyberattaques font la une des journaux, et la guerre en Ukraine nous rappelle catégoriquement que notre monde numérisé est aussi un champ de batailles* », a déclaré **Hugues Foulon, directeur général d'Orange Cyberdefense**.

« *L'encourageant ralentissement global du nombre d'incidents constaté pour nos clients les plus matures (+5% contre +13% l'année précédente) montre que nous sommes capables de remporter des batailles contre les acteurs malveillants. Ces succès ne doivent cependant en aucun cas ralentir nos efforts dans la lutte contre la cybercriminalité. Les résultats de cette année mettent en évidence les difficultés auxquelles les organisations de toutes tailles sont confrontées. Les menaces évoluent, se complexifient, proviennent de tous les horizons et soulignent l'importance du travail que nous continuerons de fournir pour nous adapter à la menace et accompagner nos clients dans cette lutte* », a-t-il conclu.

En ligne officiellement le 1er décembre, le Security Navigator Report 2023 est disponible à la presse sur demande : service.presse@orange.com

À propos d'Orange Cyberdefense

Orange Cyberdefense est l'entité du Groupe Orange dédiée à la cybersécurité. Elle compte 8 500 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 d'une expérience de 25 ans d'expérience dans le domaine de la sécurité de l'information, de plus de 2 700 experts, de 17 SOC et de 13 CyberSOC répartis dans le monde entier, nous savons adresser les problématiques globales et locales de nos clients. Nous les protégeons sur l'ensemble du cycle de vie des menaces dans plus de 160 pays.

À propos d'Orange

Orange est l'un des principaux opérateurs de télécommunications au monde, avec un chiffre d'affaires de 42,5 milliards d'euros en 2021 et 136 500 salariés au 30 septembre 2022, dont 75 000 en France. Le Groupe servait, au 30 septembre 2022, 286 millions de clients dans le monde entier, dont 240 millions de clients mobile et 24 millions de clients haut débit fixe. Le Groupe est présent dans 26 pays. Orange est également l'un des leaders mondiaux des services de télécommunications aux entreprises multinationales sous la marque Orange Business Services. En décembre 2019, le Groupe a présenté son nouveau plan stratégique intitulé « Engage 2025 ». Axé sur la responsabilité sociale et environnementale, ce plan vise à réinventer le modèle commercial du Groupe en tant qu'opérateur. Tout en intensifiant l'activité dans les domaines en croissance et en plaçant les données et l'IA au cœur de son modèle d'innovation, le Groupe entend se positionner comme un employeur attractif et responsable, en adéquation avec les métiers émergents.

Orange est coté sur le NYSE Euronext Paris (symbole ORA) et sur le New York Stock-Exchanges (symbole ORAN).
Pour plus d'informations sur Internet et votre mobile : rendez-vous sur www.orange.com, www.orange-business.com, consultez l'app Orange News ou suivez-nous sur Twitter : @orangegrouppr.

Contacts du service presse :
Emmanuel Gauthier : +33 6 76 74 14 54 ; emmanuel2.gauthier@orange.com

---

[i] Les petites entreprises, selon la définition d'Orange Cyberdefense, sont des entreprises de moins de 1000 salariés.
[ii] Étude Ponemon 2019 sur l'état mondial de la cybersécurité dans les PME – Ponemon Institute
[iii] Étude sur les effectifs dans le domaine de la cybersécurité en 2022 (ISC) https://www.isc2.org/-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx