Cyberdefense

Communiqué de presse
Paris, le 29 novembre 2023

Orange Cyberdefense Security Navigator 2024 : Nombre record de victimes de cyber-extorsion dans le monde, en hausse de 46 %

- Les 129 395 incidents détectés par les équipes d'Orange Cyberdéfense révèlent une hausse de 30 % d'une année sur l'autre, pour un total de 25 076 incidents de sécurité confirmés.
- Qu'ils soient volontaires ou accidentels, 37,45 % des incidents sont imputables à des acteurs internes.
- Les cas de « Hacking »[1] conserve sa première position, avec près d'un tiers des incidents confirmés (30,32 %).
- Les grandes entreprises (40 %) sont les plus impactées par la cyber-extorsion, suivies des petites (25 %) et des moyennes (23 %) entreprises.
- Les nouvelles recherches confirment une évolution de la conflictualité où les champs physiques et cyber se combinent davantage.
- L'analyse de 2,5 millions de vulnérabilités uniques révèle une majorité (50,4 %) de vulnérabilités critiques ou élevées.

Security Navigator 2024 – Les incidents de sécurité sont en hausse

Orange Cyberdefense, la branche dédiée à la cybersécurité d'Orange, publiera demain à 10h00 CET son rapport de recherche en sécurité annuel, le « Security Navigator 2024 ». Le rapport, qui rassemble, recoupe et analyse des données de sources variées*, dresse un tableau vaste et complexe de l'univers de la cybersécurité cette année, amplifié par des facteurs technologiques, géopolitiques, économiques et sociaux. Dans un contexte d'instabilité et d'imprévisibilité croissantes, les organisations doivent absolument réduire leur exposition au risque à travers la compréhension du paysage des menaces et de ses potentielles répercussions.

Le Security Navigator 2024 révèle que les équipes chargées de la détection des menaces ont traité 30 % d'événements supplémentaires sur la période, soit un total de 129 395, dont 25 076 (19 %) incidents confirmés. La catégorie « Hacking » reste prédominante, avec près d'un tiers des incidents confirmés (30,32 %), suivie par les catégories « Utilisation abusive » (16,61 %) et « Malware », en 3e position (12,98 %).

Malgré un volume d'incidents plus élevé, le nombre réel d'incidents de sécurité confirmés par nos équipes auprès des clients que nous soutenons a diminué de 14% d'une année sur l'autre. Le secteur de l'Industrie manufacturière (32,43 %) est de loin le plus touché en termes d'incidents confirmés, conformément aux tendances des années passées. La Vente au détail et le commerce (21,73 %) et les Services professionnels, scientifiques et technologiques (9,84 %) complètent le Top 3, qui représente à lui seul plus des deux tiers des incidents confirmés que nous signalons à nos clients.

[1] Pirater, désactiver ou endommager les appareils informatiques ou les infrastructures d'une organisation

Outre l'appât du gain, de plus en plus d'acteurs malveillants sont animés par des causes politiques ou idéologiques, mêlant dans leurs attaques des techniques d'espionnage, de sabotage, de désinformation et d'extorsion. L'augmentation record cette année du nombre de victimes de cyber-extorsion (ransomware) est mondiale et s'accompagne d'une hausse considérable de l'hacktivisme, en lien avec la guerre contre l'Ukraine. Les événements géopolitiques actuels ont également politisé certains acteurs de la cyber-extorsion.

Un nombre record de victimes de cyber-extorsion enregistré en 2023

Le paysage des menaces de cyber-extorsion, mode d'action consistant à extorquer de l'argent à une victime par le biais d'une action cyber (chiffrement des données, divulgation de données confidentielles, blocage des accès,…) continue à évoluer rapidement. Ces 12 derniers mois, une hausse mondiale record de 46 % des victimes de cyber-extorsion a été enregistrée. Les grandes entreprises ont essuyé la majorité des attaques (40 %), avec une hausse régulière pour celles qui emploient plus de 10 000 personnes. Cette tendance a été exacerbée par l'acteur malveillant Cl0p, qui a exploité deux vulnérabilités majeures en 2023. Les petites entreprises représentent un quart (25 %) des victimes et sont suivies de près par les moyennes entreprises avec 23 %.

Les grandes économies anglophones continuent d'enregistrer le plus grand nombre de victimes. Plus de la moitié d'entre elles (53 %) ont leur siège aux États-Unis, au Royaume-Uni (2e, 6 %) et au Canada (3e, 5 %). Cependant, nous constatons peu à peu une latéralisation de la répartition géographique, illustrée par des hausses considérables du nombre de victimes en Inde (+97 %), en Océanie (+73 %) et en Afrique (+70 %) d'une année sur l'autre.

En 2023, 25 groupes de cyber-extorsion ont disparu, 23 groupes ont survécu d'une année à l'autre et 31 nouveaux groupes ont émergé. Parmi les groupes de cyber-extorsion existants, plus de la moitié (54 %) ont survécu 6 mois maximum, 21 % ont survécu pendant 7 à 12 mois et 10 % ont survécu pendant 13 à 18 mois. Ce constat rappelle les difficultés auxquelles se heurtent ceux qui tentent de lutter contre les acteurs de cyber-extorsion.

Combinaison des champs de confrontation : l'hacktivisme, mode d'action des conflits actuels.

Ces deux dernières années, nous avons constaté une augmentation de l'activité dans la sphère de l'hacktivisme, utilisé pour défendre des causes de nature politique ou sociale. Les attaques de groupes d'hacktivistes engagés aux côtés de la Russie ou de l'Ukraine ont atteint des niveaux record. L'Ukraine, la Pologne et la Suède ont été les pays les plus touchés par les hacktivistes prorusses que nous surveillons. Cette tendance à la hausse est exacerbée par d'autres événements géopolitiques à l'origine de l'émergence de nouveaux groupes, notamment au regard de la situation actuelle au Proche Orient.

L'Europe a essuyé 85 % des attaques d'hacktivistes en 2023, suivie par l'Amérique du Nord (7 %) et le Moyen-Orient (3 %). Nous constatons que la plupart des pays qui subissent des attaques d'envergure sont géographiquement proches de la guerre contre l'Ukraine.

Nos recherches ont révélé un phénomène d'évolution continue vers des attaques « cognitives », qui cherchent à façonner les perceptions. Les perturbations causées (par l'attaque en elle-même ou la valeur des données ou systèmes touchés) sont finalement moins importantes que les répercussions de ces attaques sur la perception sociétale. Plus globalement, nous observons des événements physiques suscitant une cyberréponse directe des acteurs malveillants, et entraînant une escalade des tensions géopolitiques en question.

La plupart des attaques d'hacktivisme observées sont des dénis de service distribués (DDoS). Certains groupes d'hacktivistes ont développé de solides compétences DDoS, tandis que d'autres mettent en avant leurs capacités et leur impact, employant un langage et une narration disproportionnés par rapport à leurs actions (et répercussions) concrètes.

La catégorie « Hacking » occupe toujours le haut du classement, avec près d'un tiers des incidents détectés dans nos CyberSOC

Sur la base du cadre VERIS[2], l'action malveillante « Hacking » reste le type d'incident de sécurité le plus détecté, puisqu'elle représente près d'un tiers des incidents confirmés, soit 30,32 %. Cela représente une hausse significative par rapport aux 25 % de l'année dernière. La catégorie « Malware » a toujours fait partie des deux types d'incidents vrais positifs les plus détectés. Pourtant, elle se retrouve en 3e position cette année, avec 12,98 %. La catégorie « Utilisation abusive » est la 2e action malveillante la plus souvent détectée avec 16,61 %, un chiffre conforme à celui de l'an dernier. Les incidents de la catégorie « Erreur de système » (7,33 %) occupent à nouveau la 4e position et l'Ingénierie sociale (7,15 %) complète le top 5.

Les données indiquent que 37,45 % des incidents détectés dans les organisations proviennent d'acteurs internes, même si la majorité d'entre eux sont dus à des acteurs externes (43,6 %). Les actifs les plus touchés par ces incidents étaient les appareils des utilisateurs finaux (27,7 %), suivis par les serveurs (27,34 %).

Le niveau de qualification des menaces cyber en augmentation

Nous démontrons également que si la quantité d'incidents signalés à nos clients a diminué proportionnellement au fil des années, leur niveau de qualification a augmenté. Ce constat se vérifie à travers le nombre « d'événements inconnus » qui passe de 15,33 % pour les clients intégrés depuis 1 à 10 mois à seulement 4,10 % pour les clients intégrés depuis 41 à 50 mois. Ce résultat découle selon nous de l'ajustement de la détection, d'une analyse plus rigoureuse et d'autres améliorations du service. Par ailleurs, plus nos clients gagnent en maturité au sein du service, plus ils sont en mesure d'agir face aux événements que nous signalons et d'affiner leur processus pour nous fournir des retours. La qualité des retours nous permet de procéder à un ajustement précis et d'améliorer l'efficience de la détection, cycle après cycle.

Un partenariat de confiance pour l'élaboration et la mise en œuvre de stratégies de cybersécurité adaptées aux besoins des organisations

« Cette année, le rapport met en évidence l'environnement imprévisible auquel nous sommes confrontés comme en témoigne l'activité sans précédent de nos équipes qui font face à une croissance du nombre d'incidents détectés (+30% d'une année sur l'autre). Concernant les cibles, si nous constatons une augmentation du nombre de grandes entreprises touchées par la cyber-extorsion (40%), les petites et moyennes entreprises représentent tout de même près de la moitié des victimes (48%) », a déclaré Hugues Foulon, CEO d'Orange Cyberdefense

« Avec nos clients, nos équipes et l'ensemble de nos partenaires, nous poursuivons nos actions de sensibilisation au risque cyber dans la perspective de bâtir une société numérique plus sûre. Nous nous adaptons aux nouvelles technologies et nous nous préparons aux nouveaux acteurs de la menace en continuant d'anticiper, de détecter et de contenir les attaques lorsqu'elles émergent", conclut Hugues Foulon

Retrouvez l'ensemble du rapport le 30 novembre à 10h via ce lien : Security Navigator 2023 (orangecyberdefense.com)

[2] Actions (verisframework.org)

*Annexe : Ensembles de données clés

Le rapport Security Navigator exploite la visibilité et les analyses d'Orange Cyberdefense sur le paysage actuel de la cybersécurité obtenues grâce au travail de 3 000 experts, 18 SOC et 14 CyberSOC dans le monde entier. Il prend en compte notamment la France, la Belgique, les Pays-Bas, le Danemark, l'Allemagne, la Norvège, la Suède, le Royaume-Uni et l'Afrique du Sud sur une période allant d'octobre 2022 à septembre 2023. Il tire parti de sources de données propriétaires (CyberSOC, Vulnerability Operations Center, tests d'intrusion, données World Watch, leak sites de données de cyber-extorsion, journaux de conversation Telegram) et de sources tierces de données externes. Pour en savoir plus :

Analyse des CyberSOC

Un large ensemble de données est collecté auprès de toutes les équipes opérationnelles d'Orange Cyberdefense, notamment 14 CyberSOC chargés de soutenir les clients dans le monde entier. Il inclut les données des services de Managed Threat Detection entre le 1er octobre 2022 et le 30 septembre 2023, sur la base du cadre VERIS pour la classification des incidents.

Cyber-extorsion

Depuis 2020, nous avons enregistré 8 948 victimes de cyber-extorsion publiquement répertoriées sur un « leak site » du dark Web. Il ne s'agit que d'un aperçu partiel du défi posé par la cyber-extorsion, car nous répertorions les victimes qui ont été exposées sur les leak sites dédiés, ce qui signifie qu'elles ont déjà atteint la fin de la chaîne d'attaque de cyber-extorsion, et que les acteurs malveillants ont déterminé qu'il était intéressant de rendre publique la prétendue compromission. Nous sommes tout à fait conscients de ne méconnaissance d'un grand nombre de victimes.

Tests d'intrusion

Cette année, l'ensemble de données des tests d'intrusion inclut les analyses de deux équipes qui ont examiné 296 rapports de tests d'intrusion anonymisés entre octobre 2022 et septembre 2023. Les évaluations sont généralement axées sur des exigences et des portées spécifiques des clients, dans les limites de certains types de projets : Interne, Externe, Application Web, Sécurité des applications mobiles, Red Team, évaluation des API, Examens de configuration et autres. Leur complexité et le temps passé varient, mais elles peuvent nécessiter l'intervention de plusieurs hackers éthiques. Dans la plupart des cas, le client détermine la portée et l'étendue des tests requis.

Analyse des vulnérabilités

Grâce au Vulnerability Operations Center, les clients d'Orange Cyberdefense peuvent entrer en contact avec des experts qui, en évaluant les risques et l'exposition de l'environnement client face aux menaces pertinentes du moment, les aideront à mieux se protéger. Cet ensemble de données est représentatif d'un sous-ensemble de clients ayant souscrit à nos services d'analyse de vulnérabilité. Les actifs analysés comprennent les actifs accessibles via Internet, ainsi que les actifs présents sur les réseaux internes. Les données comprennent les équipements réseau, les ordinateurs de bureau, les serveurs Web, les serveurs de base de données, et même les périphériques occasionnels de type imprimante ou scanner.

Analyse des renseignements World Watch

Notre service World Watch a publié 491 avis pour la période allant d'octobre 2022 à septembre 2023, avec une moyenne de plus de 40 avis par mois – combinant nouveautés et mises à jour de sujets déjà couverts. World Watch couvre les vulnérabilités et les menaces avec un niveau de détail élevé.

Cyberattaques signalées sur les technologies industrielles

Nous avons ensuite analysé les cyberattaques OT répertoriées sur une période de 35 ans puis, pour ajouter davantage de contexte, leur pertinence par rapport aux types et catégories initialement proposés. Nos conclusions soulèvent des questionnements sur le futur des cyberattaques OT et

l'évolution potentielle des types ou catégories à moyen et long termes. Nous terminons par un exemple illustrant notre point de vue sur l'évolution des cyberattaques OT.

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.

À propos d'Orange

Orange est l'un des principaux opérateurs de télécommunications au monde, avec un chiffre d'affaires de 43,5 milliards d'euros en 2022 et 137 000 salariés au 30 septembre 2023, dont 73 000 en France. Le Groupe servait, au 30 septembre 2023, 296 millions de clients dans le monde entier, dont 251 millions de clients mobile et 25 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. 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 cotée 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.

Press contacts:

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