Cyberdefense

Communiqué de presse
5 décembre 2024

L'Europe, première cible cyber des hacktivistes d'après le Security Navigator 2025

- Un groupe d'hacktivistes pro-russes a revendiqué plus de 6 600 attaques depuis mars 2022, dont 96 % visaient des pays européens.
- Près d'une attaque sophistiquée sur quatre des systèmes OT sont le fruit d'hacktivistes.
- Les PME ont enregistré une hausse annuelle de 53% des incidents de cyber-extorsions (Cy-X)
- L'avènement de l'IA générative permet d'accroitre les possibilités d'automatisation et détection des menaces mais représente également une aide en matière d'ingénierie sociale pour les cybercriminels. Par ailleurs, le déploiement massif de solutions à base d'IA générative au sein des entreprises sans considération parfois des aspects de protection des données et de vulnérabilité présente des risques cyber importants.

Security Navigator 2025 – Un tournant décisif pour le paysage de la cybersécurité en Europe

Orange Cyberdefense, l'entité dédiée à la cybersécurité d'Orange et leader des services de cybersécurité en Europe, publie aujourd'hui sa sixième enquête annuelle et internationale de référence en sécurité, le *Security Navigator 2025*. Après avoir analysé d'importants volumes de données, elle présente une vue détaillée d'un paysage de la cybersécurité modelé par des conflits géopolitiques et une sophistication accrue des techniques chez les acteurs malveillants. Dans un contexte d'évolution des menaces pesant sur les infrastructures critiques et la confiance du grand public, le rapport souligne l'urgence pour les organisations européennes de consolider leurs lignes de défense.

Le *Security Navigator 2025* révèle une intensification de la menace hacktiviste pro-russe en Europe – en particulier l'Ukraine, la République tchèque, l'Espagne, la Pologne et l'Italie – faisant de la région la première cible. Le rapport présente également l'Europe comme la deuxième région la plus impactée par la Cy-X, avec une hausse annuelle de 18 % du nombre de victimes. Les pays d'Europe les plus touchés sont l'Italie (19 %), l'Allemagne (19 %), la France (16 %), l'Espagne (13 %) et la Belgique (8 %).

Plus précisément, le rapport indique que l'un des groupes d'hacktivistes prorusses les plus actifs a mené 6 600 attaques depuis début 2022, visant dans 96% des cas des pays en Europe. Les groupes d'hacktivistes se tournent de plus en plus vers les attaques cognitives, provoquant non seulement des incidents techniques mais aussi des attaques informationnelles pour manipuler l'opinion publique, miner la confiance dans les institutions et déstabiliser la société. En attaquant des systèmes utilisés pour les élections et d'autres institutions symboliques, ces groupes cherchent à déstabiliser ou à attirer l'attention sur des questions politiques et économiques qu'ils jugent importantes, générant par la même occasion de la peur, de l'incertitude et des doutes. Cette évolution illustre à quel point les hacktivistes modernes peuvent cibler à la fois les esprits et les infrastructures. Il s'agit là d'un défi pour les organisations qui doivent protéger les actifs numériques et la confiance du public.

Malgré une forte présence en Europe, l'hacktivisme n'a pas épargné l'Amérique du Nord cette année. Dominée par les États-Unis, cette région a été la plus impactée par la Cy-X dans le monde, avec une augmentation de 25 % des cas par rapport à l'année dernière. Les États-Unis ont aussi enregistré la plus forte concentration d'attaques OT ciblées, soit 49 % du total des incidents.

Les hacktivistes ciblent désormais les systèmes d'information industriels

Autre crainte, les hacktivistes visent de plus en plus les systèmes d'information industriels. Ces derniers constituent des éléments assurant le fonctionnement d'activités essentielles dans les secteurs de l'énergie, des soins de santé et des transports. Selon le Security Navigator 2025, près d'une attaque sophistiquée sur quatre des systèmes OT sont le fruit des hacktivistes, alors qu'elles étaient plutôt associées aux acteurs étatiques auparavant.

En complément, le rapport indique que 46 % des cyberattaques OT ont permis de modifier un processus physique.

Pour Hugues Foulon, CEO d'Orange Cyberdefense, *« **Les cybermenaces sont le nouveau baromètre des tensions géopolitiques mondiales. Les rapports de nos experts offrent une perspective solide et nouvelle sur les perturbations internationales et leurs impacts opérationnels sur la société.** »*

« Il devient urgent de coordonner les stratégies de défense en Europe et dans le monde entier, notamment avec de meilleures mesures de réponse à incidents, le renforcement des protections appliquées aux OT et une surveillance proactive afin de contrer l'ensemble des techniques de cyber-extorsion, d'hacktivisme et de guerre cognitive auxquelles les organisations européennes sont confrontées », conclut-il.

Une cyber-extorsion en hausse dans les petites et moyennes entreprises

Le rapport souligne une hausse de la Cy-X dans les PME, avec une augmentation de 53 % des incidents dans les petites entreprises. Selon le Security Navigator 2025, les PME sont souvent limitées par de faibles ressources en cybersécurité et adoptent une approche de la gestion des vulnérabilités réactive plutôt que proactive. En outre, le phénomène de « re-victimisation », qui consiste à réutiliser des données volées dans plusieurs campagnes d'extorsion, amplifie encore davantage le tribut financier et psychologique payé par ces organisations. Les PME représentent aujourd'hui deux tiers des victimes.

Le *Security Navigator 2025* suggère également que le terme « gestion des vulnérabilités » ne correspond plus à la réalité des équipes restreintes des PME. En effet celles-ci font face à un grand volume de vulnérabilités et doivent dans le même temps identifier les plus critiques pour mieux lutter contre les attaques.

Enfin, la cybersécurité des PME peut également avoir un impact sur les grandes organisations en raison de leur intégration au sein de leur chaîne d'approvisionnement. Un incident chez un petit acteur peut ainsi entraîner une cascade de perturbations tout au long de la chaîne.

Des agressions plus fréquentes, notamment dans le secteur des soins de santé

La hausse constante de la Cy-X dans le monde cache également une dimension de plus en plus « cynique ». Les attaques ciblant le secteur de la santé et de l'aide sociale ont augmenté de 50 % cette année, le plaçant en 4e position des secteurs les plus touchés. Des sous-secteurs tels que les soins ambulatoires et les hôpitaux sont désormais la cible d'attaques, révélant une érosion des contraintes « morales » qui les protégeaient auparavant.

D'autres secteurs ont également enregistré une hausse marquée des attaques de Cy-X cette année. Les trois secteurs les plus touchés ont enregistré davantage d'attaques : +25 % dans l'industrie manufacturière, +20 % dans les services professionnels, scientifiques et techniques, et +65 % dans le commerce de gros.

IA générative : une nouvelle technologie à double tranchant pour le secteur de la cybersécurité

Pour le *Security Navigator 2025*, l'IA, et plus spécifiquement l'IA générative, est un outil à la fois puissant et complexe dont les applications défensives et offensives façonnent une nouvelle dynamique des menaces de cybersécurité.

L'IA générative élève la performance opérationnelle des attaquants et permet de produire relativement aisément du phishing ainsi que d'autres techniques d'ingénierie sociale. Des hacktivistes ainsi que des acteurs malveillants soutenus par des Etats tels que la Chine, la

Russie et l'Iran exploitent cette technologie afin de mener des attaques informationnelles, dites cognitives. Ces dernières visent la diffusion de fausses informations sur Internet et notamment les réseaux sociaux.

Côté défense, le rapport rappelle que l'IA est un atout pour détecter les menaces complexes à identifie et gagner en réactivité par l'automatisation des taches. L'IA peut ainsi permettre de détecter des anomalies dans des communications afin d'identifier des interactions entre un code malveillant et une infrastructure d'attaque (beaconing). Ce dispositif peut réduire de 30 % les délais de réponse à incidents lorsque l'IA est utilisée pour identifier et intercepter ces signaux avant tout dommage.

Enfin, le rapport souligne la nécessité de veiller à la sécurisation des solutions d'IA générative et de leur emploi. Il recommande notamment la mise en place des droits d'accès élevés aux données et systèmes sensibles, de garantir l'isolation entre les locataires et de sensibiliser au risque de fuites de données dans les prompts.

Vivien Mura, CTO d'Orange Cyberdefense, a déclaré : *« L'IA est depuis longtemps un atout majeur pour détecter, dans la masse de données de toutes natures, des anomalies signes de malveillances. L'IA générative apporte de nouvelles capacités d'automatisation des services de détection et de réponse pour une meilleure réactivité et un meilleur accès au renseignement d'intérêt cyber, sous condition de cibler les cas d'usage à véritable valeur ajoutée ».*

« Par ailleurs, l'enracinement progressif de solutions d'automatisation à base d'IA générative dans les usages et services numériques peut engendrer des vulnérabilités qui seront nécessairement exploitées par des attaquants pour déclencher des actions ou des accès illégitimes. Il est donc essentiel de ne pas accorder une confiance aveugle à ces nouveaux systèmes pour protéger la donnée et maitriser les accès », conclut-il

A propos du Security Navigator

Le Security Navigator est une enquête internationale et multisectorielle de référence et un support stratégique pour comprendre les évolutions de la menace cyber et partager des recommandations pour anticiper, répondre aux attaques et bâtir la résilience des sociétés.

Le Security Navigator s'appuie sur les capacités de renseignements d'Orange Cyberdefense et de sa Cyber Threat Intelligence : plus de 135 000 évènements de sécurité survenues dans 160 pays, plus d'1 300 000 failles de sécurité et 13 308 cas de cyber extorsions étudiés depuis 2020 dont 4200 sur les 12 derniers mois. En complément, il intègre les données provenant des 32 centres de sécurité opérationnels dans le monde et les travaux des chercheurs, dont une étude approfondie du groupe d'hacktiviste pro-russe le plus actif en matière de cybercriminalité.

Le Security Navigator plonge au cœur des attaques – du dark web aux opérations d'hacktivisme – et décrypte les mécanismes de la cybercriminalité. Il présente également des solutions concrètes pour améliorer la détection des menaces, l'analyse des risques et la continuité d'activité.

Le Security Navigator 2025 peut être téléchargé :
https://www.orangecyberdefense.com/fr/insights/livres-blancs-et-reportings/security-navigator-2025

À propos d'Orange Cyberdefense

Orange Cyberdefense est l'entité du Groupe Orange dédiée à la cybersécurité. Elle protège 9 000 grandes entreprises du début à la fin du cycle de vie des menaces dans plus de 160 pays. En tant que leader européen des services de cybersécurité, **nous souhaitons devenir le cyberpartenaire de confiance en proposant un espace numérique sûr, source de valeur pour tous.** 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 30 ans d'expérience dans le domaine de la sécurité de l'information, de 3 000 experts pluridisciplinaires et de 36 centres de détection répartis dans le monde entier, nous savons répondre efficacement aux problématiques mondiales et locales de nos clients. L'humain est au cœur de la cybersécurité, et au cœur de tout ce que nous faisons pour construire une société numérique plus sûre.

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.

Contacts presse :

Chris Thomas, Orange, chris.thomas@orange.com
Emmanuelle Nahmany, Orange Business, emmanuelle.nahmany@orange.com