Communiqué de presse
Paris, le 10 décembre 2020

Orange Cyberdefense, leader européen des services de cybersécurité, livre son décryptage de l'état de la menace en 2020 et dévoile sa vision pour 2021

- Toujours autant d'attaques même en temps de confinement COVID-19, avec une explosion des attaques ransomware liées à de nouveaux modèles économiques
- Une accélération de la transformation IT suite à la pandémie du COVID-19, introduisant de nouveaux risques et défis de sécurité : la cybersécurité est désormais au cœur de la plupart des entreprises, nécessitant une nouvelle approche
- Un écosystème cybercriminel qui se structure et se professionnalise davantage à cause de l'importance des potentiels gains

Orange Cyberdefense publie son rapport annuel, le Security Navigator, qui analyse l'évolution et les mutations des cybermenaces. Ces données recensées entre janvier et octobre 2020, émanent des 50 milliards d'événements de sécurité analysés par les 17 SOC et 11 CyberSOC mondiaux d'Orange Cyberdefense, du laboratoire d'épidémiologie et du centre de recherche interne, ainsi que de rapports d'experts et d'études de référence sur le sujet.

Cette édition 2021 du Security Navigator apporte une vision unique et d'ensemble de l'écosystème de la cybersécurité, dans une année 2020 où la crise sanitaire a touché de plein fouet l'ensemble des pays et des entreprises.

« *Avec le Security Navigator 2021, nos clients et partenaires ont accès à notre analyse de la menace cyber. Elle s'appuie sur des expertises reconnues en matière de Threat Intelligence et sur les données collectées à travers le monde via le réseau international du Groupe Orange* », précise **Hugues Foulon, Directeur Exécutif de la Stratégie et des activités de Cybersécurité du Groupe Orange**. Il ajoute « *Dans un contexte technique et avec des organisations bousculées par la crise du Covid-19, ce Security Navigator permet de disposer d'un état de la menace qui éclairera utilement les décideurs d'entreprise.* »

Jamais il n'aura été plus important de sortir de l'état de crise et de la réaction permanente, pour reprendre les commandes de son destin numérique et construire une société numérique plus sûre.

2020 : l'année du COVID-19

Le constat est simple : l'année 2020, malgré son lot de crises, n'a pas vu une explosion majeure des cyberattaques à l'exception des attaquants de ransomware qui ont changé de modèle économique.

Le ralentissement général de l'économie mondiale n'a pas eu d'impacts significatifs sur le comportement des attaquants. Les cybercriminels ont eu recours au thème du COVID-19 de manière opportuniste mais relativement vite ce subterfuge a été abandonné au profit des thèmes classiques. A titre d'illustration, les attaques utilisant le COVID-19 comme objet représentent vraisemblablement moins de 2% des attaques relevées durant le mois d'avril. Le comportement des attaquants n'a que superficiellement et temporairement été modifié pendant la crise (pages 42 à 54).
De plus, il n'y a pas eu d'explosion notoire en termes de volumétrie des alertes mais une tendance à des attaques ciblant davantage les utilisateurs, notamment via l'ingénierie sociale[1] (1% des attaques en 2019 vs 5% en 2020). Les incidents les plus fréquents sont : les anomalies du réseau et des applications (35%), les anomalies liées aux comptes utilisateurs (23%) et les malwares (20%) (pages 9 à 26).

Les ransomware, un business « data centric » qui prend de l'ampleur

Les ransomware étaient à l'origine des malwares relativement peu sophistiqués qui, après avoir pénétré le système IT de la victime chiffraient l'ensemble des données. La victime ne pouvait récupérer la clé de déchiffrement qu'en l'échange du paiement d'une rançon. Ce type d'attaque visait essentiellement les petites structures ou des particuliers, faciles à attaquer, ne disposant pas de sauvegardes et enclins à payer des rançons d'un montant modeste contre la récupération de leurs données. Le développement des cryptomonnaies, facilitant les transactions qui ne peuvent être facilement retracées jusqu'aux attaquants, a permis le développement rapide de ces attaques. Ce « business model » est clairement un modèle de masse altérant la disponibilité de la donnée de tous types de victimes (page 46).

En 2020, les groupes de ransomware ont fait évoluer leur « business model » en monétisant non seulement la disponibilité de la donnée mais aussi sa confidentialité : en plus de voir leurs données chiffrées, les entreprises victimes sont sous la menace de voir certaines divulguées publiquement. Une approche qui permet le « big game hunting », où la prise pour cible de grandes entreprises, dont les rançons se chiffrent en millions d'euros (pages18 et 19 ; page 46).

Des vulnérabilités en cascade

L'analyse des experts cyber d'Orange Cyberdefense montrent la découverte inhabituelle de nombreuses vulnérabilités dans les produits de sécurité, en particulier ceux essentiels à la vie en télétravail. Cette croissance peut s'expliquer en partie par un « effet domino » ou une « cascade » dans les recherches : la découverte d'une vulnérabilité en entraîne une autre. Il peut s'agir d'une vulnérabilité différente au sein du même logiciel ou bien de la même vulnérabilité au sein d'un autre outil. C'est donc un constat plus positif qu'il n'y paraît car cela permet in fine de renforcer la sécurité de ces solutions.
Un point de vigilance : les délais de patching (application des correctifs) demeurent longs. Dans une étude menée par nos équipes, sur 168 vulnérabilités au sein des produits de sécurité au cours des 12 derniers mois où un patch était disponible, moins de 19 % d'entre

[1] Pièges affectant les utilisateurs, notamment par recours au phishing et à l'usurpation d'identité

elles sont patchées sous 7 jours. De plus, 56,8 % de ces patchs disponibles prennent de 31 à 180 jours à être appliqués, et, plus préoccupant encore, 14 % n'étaient toujours pas appliqués six mois après avoir été notifiées (page 36). Ce délai peut être mis à profit par les attaquants qui exploitent chaque nouvelle vulnérabilité découverte.

2020 : un écosystème cyber plus mature

Les menaces d'aujourd'hui ne se substituent pas à celles d'hier, elles s'additionnent.

Une élévation du niveau de maturité général est constatée : les salariés sont plus attentifs aux sujets cyber. Ils ont pris conscience de la criticité du numérique dans leur travail et dans leur vie personnelle et font preuve de davantage de vigilance.

Cette maturité touche tous les acteurs du cyberespace, et donc la cybercriminalité aussi, qui se structure considérablement en 2020. Etre un cybercriminel est devenu un métier, du moins dans son organisation (page 62). Les cybercriminels s'allient pour former des groupes spécialisés, collaborer et constituer un réseau interconnecté. Ils s'organisent comme le font les entreprises qu'ils ciblent et font usage de pratiques connues : service client, assistance après-vente, Malware-as-a-Service, etc.

La démocratisation des nouvelles technologies et leur sécurisation

La pandémie aura mis les technologies d'accès distant à l'honneur. La demande globale de solutions VPN a augmenté de 41 % au cours de la seconde moitié du mois de mars, et reste de 22 % supérieure aux niveaux pré-pandémie (page 49). Une nouvelle manière de travailler qui implique une sécurisation plus accrue des endpoints (PC, tablettes, mobiles…). Depuis le début de la pandémie, les endpoints sont devenus des éléments essentiels. Nous avons d'ailleurs enregistrés +500% de demandes de nos clients pour la détection et la réponse des endpoints.

L'autre tendance notable, qui va de pair, est le boost de l'adoption du cloud qui offre réactivité, baisse des investissements et flexibilité aux entreprises. Cette migration vers le cloud nécessitera une protection spécifique des données et une vigilance importante sur l'identité des utilisateurs (IAM, authentification forte).

Les investissements des entreprises dans les produits de sécurité

En 2020, les entreprises semblent ainsi avoir adopté trois comportements type :

- Elles ont opté pour une position attentiste et limité leur action sur leur IT tant leur activité en dépendait,
- Elles ont revu leur architecture IT et les fondements de leur sécurité, notamment celles dont les activités étaient à l'arrêt (ex. secteur aéroportuaire),
- Elles se sont concentrées sur des actions ciblées, notamment sur la sécurisation des points critiques (les endpoints et les accès distants majoritairement).

En termes d'investissement, les prévisions 2021 des analystes semblent montrer un attrait marqué des entreprises pour les services managés (externaliser la sécurité, en tout ou partie, par un prestataire).

Le volume en fonction de la taille de l'entreprise
Nous avons enregistré environ 101 incidents confirmés (contre 63 en 2019) ciblant les petites entreprises. Pour les organisations de taille moyenne, le nombre moyen d'incidents est de 77 (266 en 2019) et de 278 pour les grandes entreprises (463 en 2019).

A noter : plus d'incidents ne veut pas dire moins de protection. Les petites entreprises ayant « rattrapé leur retard », et davantage investi dans des technologies de détection, elles voient de fait leur volume d'alertes augmenter (page 21).

2021 : quelles perspectives ?

La 5G, lancée cette année dans de nombreux pays, va apporter son lot de nouveaux usages et accélérer le développement des technologies et produits. Certains d'entre eux seront au cœur de l'industrie 4.0 et des smart cities. Aussi, nous anticipons un développement encore plus marqué des solutions de sécurisation pour l'IoT et des chaînes de production, avec le rapprochement nécessaire des équipes IT et OT (Systèmes Industriels). Orange Cyberdefense, notamment via son Demo Center de Lyon qui sera inauguré en 2021, s'engage à être pionnier dans la cybersécurité industrielle en pleine évolution.

La transformation de l'IT vers le cloud, mais aussi l'adoption de nouvelles formes de connectivité comme le SD-WAN, vont rester prioritaires pour les entreprises, apportant de nouveaux usages et de nouveaux risques à couvrir.

Dans un contexte où la cybermenace se veut de plus en plus structurée, il faut se préparer à ce que le nombre d'attaques continuent d'augmenter. La pandémie de COVID-19 a généré des bouleversements sans précédent sur la société et l'économie. Elle a fondamentalement transformé la façon dont nous travaillons et exerçons nos activités. Nous le voyons déjà, nombre de ces changements se transforment en améliorations durables et les états d'esprit évoluent. Une forte progression des demandes en matière de sécurité du Cloud, des réseaux et de visioconférence a été constatée — le télétravail est là pour durer.

Enfin, autre enseignement de la crise de COVID-19 : la valeur de la proximité. Bien que technologique, la cybersécurité reste, avant tout, imprégnée de la notion de confiance.

Pour télécharger le Security Navigator 2021 :
https://orangecyberdefense.com/fr/security-navigator/

A propos d'Orange

Orange est l'un des principaux opérateurs de télécommunication dans le monde, avec un chiffre d'affaires de 42 milliards d'euros en 2019 et 143 000 salariés au 30 septembre 2020, dont 83 000 en France. Le Groupe servait 257 millions de clients au 30 septembre 2020, dont 212 millions de clients mobile, 21 millions de clients haut débit fixe. Le Groupe est présent dans 26 pays. Orange est également l'un des leaders mondiaux des services de télécommunication aux entreprises multinationales sous la marque Orange Business Services. En décembre 2019, le Groupe a présenté son nouveau plan stratégique « Engage 2025 » qui, guidé par l'exemplarité sociale et environnementale, a pour but de réinventer son métier d'opérateur. Tout en accélérant sur les territoires et domaines porteurs de croissance et en plaçant la data et l'IA au cœur de son modèle d'innovation, le Groupe entend être un employeur attractif et responsable, adapté aux métiers émergents.

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 ou pour nous suivre sur Twitter : @presseorange.

Contacts presse :

Nathalie Chevrier, nathalie.chevrier@orange.com, 06 48 52 75 83
Caroline Cellier, caroline.cellier@orange.com, 06 07 25 00 06