Orange
Cyberdefense

Security Navigator 2020

La Recherche au service d'une société numérique plus sûre.

Hugues Foulon
Executive Director
of Strategy and
Cybersecurity activities
Orange

Michel Van Den Berghe
Chief Executive Officer
Orange Cyberdefense

En 2019, grâce à nos 16 CyberSOCs, nous avons analysé plus de 50 milliards d'évènements de sécurité par jour, résolu plus de 35 000 incidents de sécurité et mené plus de 170 missions de réponse à incidents.
Nos experts internationaux ont intégré ces informations et proposent, dans ce rapport, une synthèse de leurs principaux constats, à destination de nos clients et de la communauté cybersécurité dans son ensemble.

Nous sommes heureux de publier aujourd'hui la toute première édition du rapport Orange Cyberdefense, Security Navigator. En tant qu'opérateur mondial des télécoms avec Orange, et leader européen en matière de cybersécurité avec Orange Cyberdefense, notre connaissance de la menace est unique.

La pandémie de COVID-19 a provoqué un bouleversement sans précédent affectant la société et l'économie, tant d'un point de vue physique que numérique. Elle a fondamentalement changé notre manière de travailler et de mener nos activités. Nombre de ces changements persisteront au-delà de la crise. Demandes accrues de services Cloud sécurisés, de connexions réseau distantes fiables par SSL, sans oublier le recours à la visioconférence – le nouveau monde du télétravail est là pour rester.

Cette crise prouve aussi que la liberté numérique n'est pas acquise. Elle est remise en question tous les jours par des acteurs malveillants qui font de nos espaces de connexion et de progrès, des fenêtres d'attaques pour nous nuire. Chacun peut en être victime, individuellement et collectivement, et la confiance que nous plaçons dans les acteurs du numérique peut alors en pâtir. Chez Orange Cyberdefense, nous voulons que ce monde numérique reste un moyen fiable de se divertir, d'accéder à des opportunités professionnelles, à des services qui améliorent notre quotidien, le rendent plus prospère et plus épanouissant.

C'est pourquoi nous nous attachons à créer les lignes de défense qui protègeront la liberté de tous dans l'espace numérique, non seulement en temps de crise, mais aussi pour demain. Notre mission : construire une société numérique plus sûre.

En 2019, grâce à nos 16 CyberSOC, nous avons analysé plus de 50 milliards d'évènements de sécurité par jour, résolu plus de 35 000 incidents de sécurité et mené plus de 170 missions de réponse à incidents.

Nos experts ont analysé l'ensemble de ces informations et proposent, dans ce rapport, une synthèse de leurs principales conclusions, à destination de nos clients et de la communauté cyber dans son ensemble.

Pas un jour ne passe sans que nous soyons reconnaissants de la confiance que nos clients nous accordent pour sécuriser leurs actifs les plus critiques, et fiers des expertises les plus pointues et des technologies les plus avancées que nous déployons dans tous les domaines, pour protéger leurs entreprises.

Merci de votre confiance !

Hugues Foulon
Michel Van Den Berghe

Table des matières

COVID-19 et cybersécurité

Alors que la pandémie de COVID-19 gagne du terrain à l'international, les cybercriminels tentent de capitaliser sur cette crise sanitaire globale en concevant des malwares ou en lançant des attaques exploitant ce thème. Néanmoins, ces comportements opportunistes au sein de l'écosystème cybercriminel ne constituent qu'une partie d'un plus vaste tableau. Orange Cyberdefense publie une note d'information afin d'attirer l'attention sur une variété de faits qui se doivent désormais d'être pris en compte.

Téléchargez le rapport complet
https://orangecyberdefense.com/global/covid-19/

Méthodologie et menaces cyber : cinq changements induits par la pandémie de COVID-19 :

- Vos employés sont plus vulnérables aux techniques d'ingénierie sociale et autres escroqueries
- Vous avez moins de contrôle et de visibilité sur les systèmes informatiques que vous protégez.
- Vos utilisateurs peuvent se connecter depuis des systèmes et environnements non sécurisés ou mal configurés.
- Vous vous êtes peut-être empressés de mettre en œuvre des outils d'accès distants sans disposer de temps pour les planifier et les déployer aussi bien que vous l'auriez souhaité.
- Vos équipes, vos fournisseurs et vous-même fonctionnez peut-être en mode dégradé.

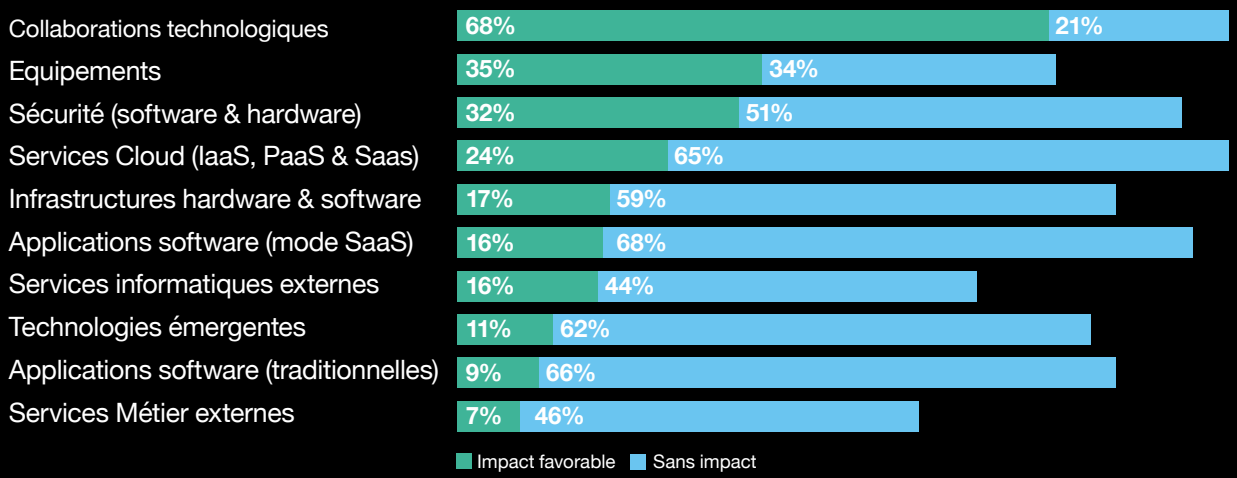
Des effets sur le monde numérique

Quelques-unes des tendances que nous avons observées durant la phase de confinement :

1. Malware et campagnes de phishing ayant recours au COVID-19 comme prétexte
2. Campagnes globales de désinformation et de « fake news »
3. Certains groupes spécialisés dans les attaques par ransomware appelant à un cessez-le-feu
4. Attaques ciblées à l'encontre d'établissements de santé et d'organismes de recherche
5. Augmentation des tensions géopolitiques susceptibles d'accroitre les risques de cyberguerre
6. Attaques ciblant les technologies d'accès distant et passerelles VPN
7. Visibilité réduite depuis les SIEM
8. Activité informatique largement déplacée vers le Cloud
9. Accélération du recours au e-commerce
10. Pression accrue sur les infrastructures Internet pouvant conduire à une

L'impact du COVID-19 sur la technologie

Une étude IDC a enquêté auprès de 180 organisations dans toute l'Europe pour mesurer l'impact de la crise sur leurs investissements technologiques.



https://www.idc.com/getdoc.jsp?containerId=EUR146175020

Le leurre parfait

La seule journée du 24 mars, notre CERT en France a identifié 23 e-mails de phishing liés au COVID-19 et sur une période de 24 heures. Notre équipe a aussi constaté que, durant la même semaine, les clients ont remonté plus de 600 e-mails potentiellement frauduleux, dont 10 % se sont avérés malveillants.

E-mails de phishing suspects notifiés par les clients

Le nombre d'e-mails frauduleux confirmé était 4 fois supérieur à la semaine précédente

Les recommandations en résumé

Durant une crise telle que celle liée au COVID-19 nous vous conseillons de vous concentrer sur les réponses suivantes, par ordre de priorité :

- Établir des procédures et systèmes de réponse d'urgence.
- Mettre en place un support sécurité (hotline) et se préparer à renforcer l'équipe chargée de fournir ce support.
- Passer en revue les sauvegardes ainsi que le plan de reprise d'activité post-sinistre (Disaster Recovery Plan).
- Doter vos utilisateurs des informations nécessaires pour garantir des décisions de sécurité éclairées.
- Fournir un accès distant sécurisé.
- Garantir la visibilité des équipements distants (Endpoints).

COVID-19 : les enseignements

Les conseils n'ont que peu de poids en temps de crise. Chaque métier est différent et nous ne prétendons pas savoir comment chaque société devrait répondre aux cybermenaces qui les affectent particulièrement. Nous partageons des recommandations avec celles qui mesurent le risque cyber et envisagent d'y apporter une réponse en période de crise :

1. Comprendre que si le niveau de la menace est élevé il augmente pourtant faiblement notre vulnérabilité. La menace est hors de notre contrôle, mais nous gardons la main sur le niveau de vulnérabilité. Concentrons-nous sur ce point.
2. Comprendre ce qui a changé et ce qui n'a pas changé. Votre modèle de réponse aux menaces peut être très différent aujourd'hui que celui d'hier, mais il peut aussi demeurer inchangé. Si ce modèle est resté le même, votre stratégie et vos opérations n'ont pas non plus besoin d'être modifiées.
3. Instaurer des partenariats afin d'éviter les foules. Vos fournisseurs, prestataires, voire aussi vos concurrents, voguent – plus que jamais – sur le même bateau. Ils ne disposent peut-être pas non plus de toutes les réponses, c'est peut-être le bon moment pour engager le dialogue et trouver des partenaires dont le point de vue est mesuré, rationnel, tout en évitant les communautés propageant battage médiatique et hystérie.
4. Maintenir le contexte. L'informatique et Internet ont survécu vingt ans durant malgré de multiples échecs en sécurité. Il ne fait aucun doute que la situation de crise est préoccupante et que le risque d'une crise cyber est réel et ne doit être ignoré. Quand bien même, cette fois, la crise est médicale et humaine. Ne laissez pas le battage médiatique autour de la cybersécurité vous éloigner de cette réalité.
5. Travailler de façon intelligente. Vous ne mènerez à bien que peu de projets si vous travaillez en mode dégradé. Exploitez votre temps et votre énergie de façon à définir vos priorités : concentrez-vous sur ces points.

Charl van der Walt
Head of Security Research
Orange Cyberdefense

Introduction

L'état de la menace

« Les dépenses mal orientées sont excessives. La peur et les problématiques de conformité ont contribué à concevoir et vendre des stratégies de cybersécurité sur des menaces perçues plutôt que réelles. »

Art Coviello, Former CEO, RSA Security (2017)

Une guerre d'usure

La cybersécurité est une question de ressources. Les attaquants comme les défenseurs ont accès à des ressources limitées en termes de temps, de budget ou de compétence. Ils y recourent de façon stratégique pour atteindre leurs objectifs.

Dans ce paysage complexe et évolutif, il n'est pas aisé de différencier menaces « perçues » et « réelles ». Comme l'indique Art Coviello, ce manque de certitudes a installé le doute et engendré un excès d'achats motivés par la peur. Quelles sont alors les véritables menaces ? Comment les identifier et les suivre dans un environnement qui ne cesse d'évoluer ?

Nous vous proposons d'exploiter la vaste quantité de données à notre disposition ainsi que la connaissance fine et l'expertise de nos spécialistes pour vous aider à tirer des enseignements du passé et, quand cela est possible, vous préparer au futur.

L'état de la menace peut être analysé au prisme de trois composantes : les forces structurelles, les facteurs inflationnistes et les évolutions technologiques

Les forces structurelles

Les forces structurelles se composent d'éléments systémiques à l'origine de catalyseurs et de contraintes qui façonnent la menace et notre capacité à y répondre. Ces facteurs sont ancrés dans nos contextes et environnements ; leur impact sur la forme que prendra la menace et sur notre capacité de réponse est fondamental.

L'innovation criminelle en est un exemple : ce qui évolue dans la « cyber-criminalité », ce n'est pas tant l'aspect « cyber », que la « criminalité ». De nouvelles façons de monétiser certaines méthodes d'attaque existantes – par le biais du crypto-mining et de ransomware, par exemple – altèrent rapidement la nature de la menace, faisant continuellement bouger les lignes de nos modèles de menaces.

« Tendances clés de marché affectant les RSSI:

- Réglementations et lois en matière de cybersécurité ;
- Responsabilité de la direction vs Manque de visibilité ;
- Pénurie sur le marché (accroissement des besoins vs Demande accrue de compétences). »

Nadav Shatz /
Director of Advisery and Architecture,
Orange Cyberdefense

Autre exemple, la cyberdéfense est devenue une fonction essentielle, les dirigeants et les comités exécutifs sont bien plus au fait des questions « cyber » qu'auparavant. Toutefois, ils sont prioritairement préoccupés par des questions d'ordre réglementaire, par le souci de conformité et par leur responsabilité financière. Ils font désormais pression sur les RSSI pour les inciter à modifier leurs modes de travail. De ce fait, les RSSI sont détournés du vrai sujet, s'employant à comprendre et à répondre, non pas à la menace, mais bien aux exigences du comité exécutif.

Les facteurs inflationnistes

Comme précédemment indiqué, le paysage de la menace auquel nous faisons face aujourd'hui se dessine d'abord et surtout dans un contexte marqué par de puissantes forces structurelles. Ces forces, soient-elles militaires, politiques, économiques, sociales ou légales, trouvent leur origine au niveau national ou international.

Une fois la forme de la menace définie, les défis auxquels nous sommes confrontés sont amplifiés par des « facteurs inflationnistes », également puissants et moins contrôlables encore. Ces facteurs sont comparables à l'effet produit lorsque l'on souffle dans un ballon.

Une majeure partie des facteurs inflationnistes provient de l'ambivalence des gouvernements face à la résolution des problèmes de sécurité, et la poursuite de leurs investissements dans la construction et l'utilisation d'outils et techniques avancés de piratage pour mener à bien leurs objectifs politiques. Nous estimons que l'investissement des forces militaires dans le piratage informatique est le facteur majeur dans ce domaine.

Alors que les conflits entre États-nations dans le cyberespace prennent de l'ampleur et augmentent en intensité, il est important de noter que ces conflits se déroulent sur Internet : espace que nous partageons tous. Leur impact ne peut se limiter qu'aux cibles « gouvernementales » : nous sommes inévitablement touchés, d'une manière ou d'une autre. Il faut le voir comme un dommage collatéral.

Enfin, les technologies, la formation, les compétences et l'expérience gouvernementale finiront par se retrouver dans la sphère civile où leur impact peut s'avérer hautement disruptif, comme l'ont clairement illustrées, WannaCry et notPetya. La portée et l'ampleur des initiatives gouvernementales sont capables de bouleverser entièrement tout ce que nous jugeons « vrai » sur nos marchés.

Du point de vue de la cyberdéfense, ces puissantes forces géopolitiques font la pluie et le beau temps. Leur impact sur nos réalités quotidiennes est énorme. Nous pouvons observer ces forces, voire même tenter de les prédire, mais nous n'avons pas de moyen sûr de les contrôler. Seul choix possible : tâcher de les appréhender et d'orienter nos stratégies en conséquence.

« De nos jours, pas une opération militaire ne se déroule sans impliquer des services de cyberdéfense, soient-elles de l'ordre du renseignement, des opérations psychologiques, du ciblage, de la destruction ou de l'évaluation post-frappe. »

Laurent Célérier / Executive VP Technology & Marketing,
Orange Cyberdefense
Former senior officer, French Ministry Of Defense

L'évolution technologique

La logique veut que l'évolution technologique, autant que les nouveaux modèles de gestion et les dernières procédures qu'ils sous-tendent, affecte amplement l'état de la menace. Attaquants et défenseurs sont impactés par tout changement, même infime, apporté aux systèmes et outils dont ils se servent.

Des principes cohérents décrivent comment l'évolution technologique affecte l'état de la menace.

L'un d'eux est que pour la plupart des entreprises, les nouvelles technologies remplacent rarement totalement les anciennes. Plus simplement, elles s'y ajoutent. Ainsi, au fil du temps, l'entreprise s'alourdit d'une « dette » sécurité dont elle ne se départira jamais, et qui a plutôt tendance à augmenter. Nous pouvons affirmer avec assurance que les défis de cybersécurité auxquels nous avons été confrontés hier continueront de nous défier demain et que les nouvelles technologies ne réduiront probablement pas le risque. Elles ajouteront de nouvelles menaces.

L'introduction de la 5G est, ici, un exemple évident. Cette nouvelle technologie est indubitablement plus sûre que les précédentes. Elle promet d'être un puissant facilitateur tant pour les technologies nouvelle-génération que pour les opportunités commerciales. Néanmoins, elle décuplera sans doute la dette sécurité que l'industrie technologique continue d'accumuler dans sa course au développement, à la commercialisation et à la vente de nouvelles technologies. L'Internet des Objets (IoT) est clairement sujet aux mêmes problèmes de sécurité que ceux qui caractérisent les PC depuis des décennies, mais il implique aussi ses propres défis (e.g. : application à distance de correctifs firmware à grande échelle). Ces problèmes sont amplifiés par l'augmentation des déploiements IoT.

Du point de vue de la cyberdéfense, cependant, il est possible d'exercer un contrôle sur la technologie. Nous sommes en mesure de choisir de ne pas adopter une nouvelle technologie, quand et comment en déployer d'autres pour remédier à des menaces émergentes.

Ces actions étant entièrement à notre main, il est tout à fait logique pour nous de recourir aux meilleures pratiques pour nous en charger.

> « L'impact des nouvelles technologies est toujours surestimé à court terme, et sous-estimé à long terme.
>
> Nous ne savons pas ce qui changera, mais nous pouvons assurément prévoir ce qui restera inchangé. »
>
> Etienne Greeff / CTO, Orange Cyberdefense

Evaluer nos options

À la lumière des trois facteurs clés constitutifs de la menace émergente, nous nous demandons comment, nous – experts en cyberdéfense – pouvons contrôler ou influencer ces forces à notre avantage.

Nous ne sommes véritablement capables de contrôler qu'un seul élément constitutif de la menace: la technologie. Elle doit donc s'imposer comme une préoccupation immédiate et à court terme. Pour cela il faut penser intelligemment son déploiement, celui des talents et des pratiques de sécurité visant à contrer les menaces et réduire les risques.

Bien que nos efforts en matière de technologie soient évidemment nécessaires, les trois facteurs clés précédemment décrits n'ont, malheureusement, pas un impact égal sur l'état de la menace émergente.

Celle-ci est davantage influencée par des facteurs sur lesquels nous n'avons pas de contrôle, que par ceux que nous contrôlons. Ceci suggère que, certes, il est impératif de continuer d'améliorer nos technologies, nos équipes et nos méthodes, mais nous devons aussi accepter et anticiper que ces efforts seuls ne suffiront pas à atteindre le niveau de résilience que nous souhaitons face aux menaces actuelles « réelles ».

Forces structurelles
Les forces systémiques créent des catalyseurs et des contraintes qui façonnent la menace et notre capacité d'y répondre.

Influence
Nous ne pouvons contrôler ces facteurs, mais nous sommes en mesure de les influencer. Influencer l'environnement est le moyen le plus efficace d répondre à la menace sur le long terme.

Forces inflationnistes
La menace nait d'un contexte politique, économique, social, légal et réglementaire.

Observer et orienter
Ces facteurs font la pluie et le beau temps : leur impact est considérable, mais nous ne pouvons les maitriser. Notre seul choix : les appréhender et orienter nos stratégies en conséquence.

Évolution technologique
Les technologies changent et les menaces avec elles.

Contrôler
Nous pouvons limiter notre surface d'attaque, trouver et atténuer les vulnérabilités. Ces travaux sont sous notre contrôle, il est donc logique de s'en charger.

« Les individus mal intentionnés continueront d'innover. Nous devons accepter qu'il y ait des failles et nous concentrer sur la détection et la réponse. »

Stefan Lager / Senior VP Global Service Lines, Orange Cyberdefense

Une crise de compromis

Certains diront que le rôle de la cybersécurité au cœur des technologies est de créer et de garantir la confiance. Les trois piliers de la « Triade CIA » – Confidentialité, Intégrité et Disponibilité – définissent selon nous la façon de procéder : en veillant à la fiabilité des données et systèmes que nous utilisons pour garder des secrets, nous garantissons leur intégrité et et leur disponibilité quand nous en avons besoin. Si la sécurité échoue, la confiance est compromise. Une fois la confiance perdue, elle est difficile à rétablir. De fait, la confiance est si cruciale pour des systèmes dont nos métiers, sociétés, et même nos vies, dépendent, que la sacrifier pour des technologies clés ne reviendrait à rien de moins qu'à une crise.

L'enseignement à propos de la technologie est simple et clair : nos partenaires doivent pouvoir faire confiance aux systèmes et données qui sont sous notre responsabilité.

Quand des attaques, fuites et autres compromissions surviennent, cette confiance est mise à mal, les conséquences vont loin. Dans un système complexe, sujet à de multiples facteurs hors de notre contrôle, nous ne pouvons empêcher l'émergence de crises. Nous pouvons cependant les tuer dans l'œuf et, pour ce faire, il nous faut de la visibilité, une détection précoce et des capacités claires et sûres de réponse. Plus encore que de préserver la confiance, il nous faut œuvrer à la restaurer lorsque des évènements adverses se produisent. La détection, la réponse et la remédiation jouent des rôles centraux.

Équilibrer la balance – détecter, répondre, remédier

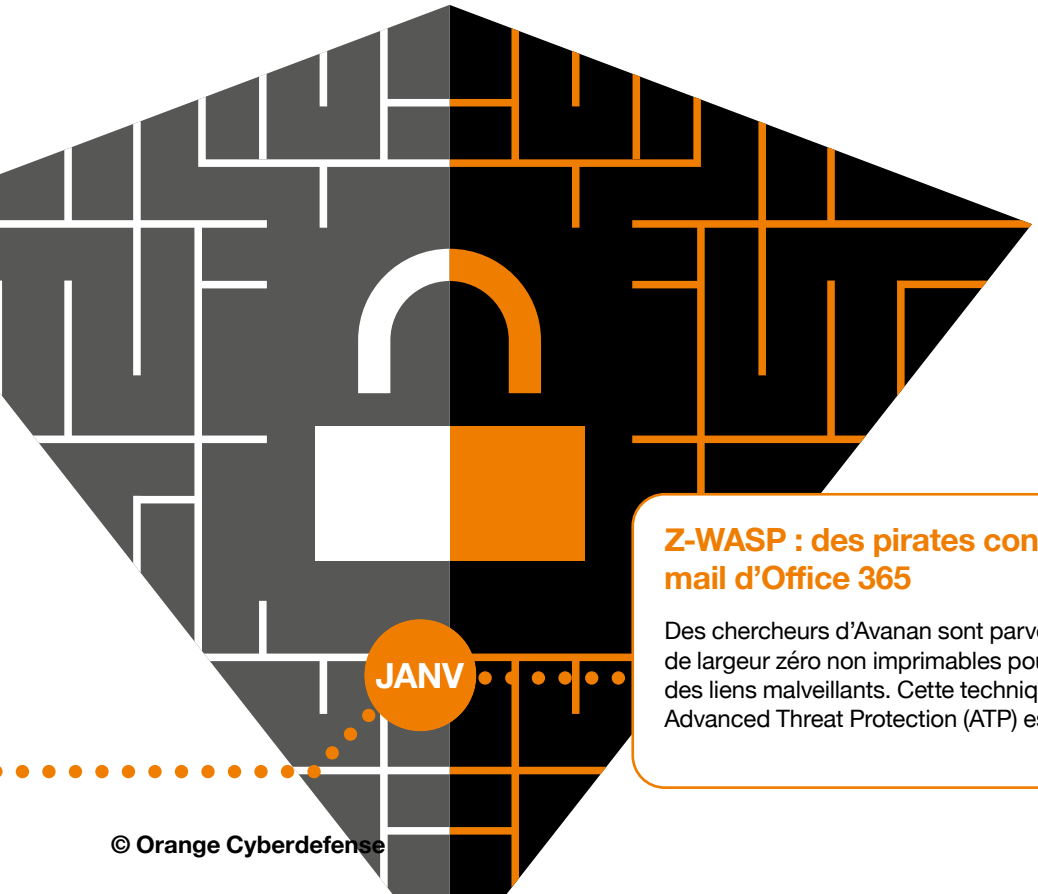
Nos paradigmes doivent changer. Dominic White (CTO en charge de l'unité d'élite Orange Cyberdefense spécialisée dans les attaques et tests d'intrusion) nous livre des clés pour nous orienter.

« S'ils nous détectent, ils nous « crament », et il y a des conséquences. Les attaquants aussi ont un boss et un budget. »

Dominic White / CEO, SensePost

Ici le point de vue d'une équipe d'attaquants chevronnés montre que si les différents contrôles préventifs que nous mettons en œuvre peuvent imposer un coût à l'attaquant, la détection et une réponse efficace par une unité d'élite spécialisée dans les attaques et tests d'intrusion ont pour effet de les repousser véritablement. De cet enseignement naît notre conviction de l'intérêt de la « mobilisation » : l'adversaire ne peut plus être retenu aux portes.

Nous devons prévoir que les adversaires peuvent être actifs au-delà de nos périmètres et sur nos systèmes. Nous devons donc les y trouver et les contrer, souvent système par système, jusqu'à ce qu'ils soient poussés vers la sortie. Comme les autres doctrines de sécurité avant elle, « Détecter, Analyser & Réagir » ne relève pas du miracle. Elle ne peut être déployée isolément et elle ne surmontera pas les forces structurelles et inflationnistes systémiques auxquelles nous sommes confrontés. Il s'agit toutefois d'une réponse tactique nécessaire dans la réalité contemporaine qui favorise toujours largement l'attaquant.



Z-WASP : des pirates contournent les protections mail d'Office 365

Des chercheurs d'Avanan sont parvenus à utiliser caractères HTML de largeur zéro non imprimables pour empêcher Office365 d'identifier des liens malveillants. Cette technique fonctionne même lorsque MS-Advanced Threat Protection (ATP) est activé. [t1]

Conclusion

Ce qui ressort clairement de l'examen de la menace émergente, est que les entreprises, grandes comme petites, vont se trouver dans un état de conflit permanent avec des adversaires soutenus par de grands facteurs et forces systémiques sur lesquels nous n'avons que très peu de contrôle. Collectivement, ces facteurs et forces l'emportent sur toutes les ressources que nous – défenseurs – pouvons espérer mettre en œuvre.

Le confinement lié au COVID-19 et son impact sur les marchés mondiaux sont un parfait exemple d'un tel facteur dit « incontrôlable ». Il est évident qu'ils affectent les modes d'attaque des acteurs de la menace, tant positivement (certains groupes ont déclaré un cessez-le-feu) que négativement (pression accrue sur les établissements de santé et tentatives massives de profiter du thème du COVID pour alimenter les campagnes de phishing et la fraude).

Sans négliger les bonnes pratiques de sécurité de base, nécessaires pour contrebalancer ces menaces (et sans lesquelles elles nous submergeraient purement et simplement), nous devons reconnaître que les attaques, compromissions et fuites de données sont inévitables. Nous devons nous préparer à affronter notre adversaire, activement et de manière continue, au-delà des périmètres traditionnels de nos environnements.

À la lumière des menaces contemporaines, des capacités de détection et de réponse matures et efficaces sont non seulement une exigence essentielle, mais des programmes de détection et de réaction nous aident aussi à contrecarrer certains des facteurs qui donnent à nos adversaires un avantage systémique. Par exemple: minimiser l'élément de surprise, influer sur les coûts réels et conséquences de leurs erreurs, prolonger le temps qui leur est nécessaire pour apprendre et s'améliorer, et, parallèlement, réduire pour nous le temps d'en faire de même.

Un « Hacktiviste » condamné à 10 ans de prison après une attaque DDoS contre un centre hospitalier

En 2014, Martin Gottesfeld s'en est pris au Boston Children's Hospital ainsi qu'à un autre établissement via un botnet de 40 000 routeurs, prétendument pour protester contre des traitements abusifs à l'encontre de Justina Pelletier. [t2]

La Fondation du Patrimoine et l'incendie de Notre-Dame de Paris

Après que les toits de la Cathédrale Notre-Dame ont brûlé le 15 avril 2019, la Fondation du Patrimoine a dû faire face à une autre crise. Habilitée par l'état à récolter les fonds de solidarité pour la reconstruction de l'édifice, cette entité a rapidement été submergée par un problème qu'elle n'avait pas anticipé : la prolifération de campagnes de collecte frauduleuses et le dépôt de de noms de domaine parasites.

« De nombreux sites tentaient de se faire passer pour des collectes légitimes et le site de la Fondation du Patrimoine est resté hors ligne deux heures durant [...].

Grâce à Orange Cyberdefense nous avons pu réagir immédiatement, surveiller les activités frauduleuses et engager des poursuites judiciaires avec efficacité. »

Jean-Michel Livowski, DPO, Fondation du Patrimoine

Gestion de crise, chiffres clés :

- 50 jours de surveillance
- 20 000 informations remontées à la cellule de crise
- 400 cagnottes parallèles identifiées et notifiées aux autorités
- Plus de 20 noms de domaines sous surveillance

Préoccupée par la situation et la possible intensification des attaques à l'aube du week-end de Pâques, la presse a contacté Orange Cyberdefense le soir du 19 avril, veille d'un long week-end susceptible d'aider les malfaiteurs. L'équipe de réponse à incidents d'Orange Cyberdefense (CSIRT) et son CERT décident alors de déployer sans tarder un système de gestion de crise.

Gestion de crise en en temps record

Alors que les dons affluent, les premières actions sont prises par la Fondation, notamment la création d'une page Web officielle dédiée aux dons et soutenue par une campagne de communication reprise par différents médias et réseaux sociaux. Celle-ci, tout comme les sites Internet de Notre-Dame de Paris et de la Fondation du Patrimoine sont placés sous observation par les analystes d'Orange Cyberdefense. A ce premier dispositif de sécurité, s'ajoute une surveillance:

- des noms de domaine
- des applications mobiles
- des profils sur les réseaux sociaux
- des cagnottes sur les plates-formes spécialisées

Une cellule de crise remonte les alertes en temps réel aux responsables, aux avocats et aux autorités judiciaires via un Extranet.

« La collecte lancée par la Fondation du Patrimoine a été un très grand succès populaire avec plus de 220 000 donateurs individuels. Cette mobilisation historique, réalisée dans l'urgence et en un temps record, n'aurait pas pu réussir sans la collaboration et le travail des équipes d'Orange Cyberdefense »

Guillaume Poitrinal, Président de la Fondation du Patrimoine

Sara Puigvert
Executive VP Global Operations
Orange Cyberdefense

Franz Häertl
Head of Global Content Marketing
Orange Cyberdefense

Les Statistiques de nos CyberSOC

Ce qu'il s'est passé

Notre préoccupation quotidienne est la protection des actifs, des systèmes et des infrastructures informatiques afin de permettre aux entreprises de fonctionner. Lorsque nous surveillons pour nos clients leurs dispositifs de sécurité, leurs postes et terminaux, leurs applications Cloud, leurs environnements technologiques d'exploitation (OT) et leurs réseaux dans le monde entier, nous voyons de nos propres yeux beaucoup de ce qui finit par être médiatisé.

Un flux continu de données passe par nos 10 CyberSOC et 16 SOC. Comme nous l'avons fait dans nos précédents rapports de sécurité annuels, nous avons choisi d'examiner ces données et d'extrapoler les chiffres pour mieux appréhender l'évolution du paysage de la menace.

Ainsi, dans le cadre de ce nouveau Security Navigator, nous pouvons à nouveau partager avec vous une image réaliste et actualisée des évènements et tendances de l'année passée.

Ces données ont été recueillies avant que le COVID-19 n'affecte à la fois les marchés et le paysage de la menace. À ce titre, elles pourront servir de base pour une comparaison avec de futures données.

À propos des données

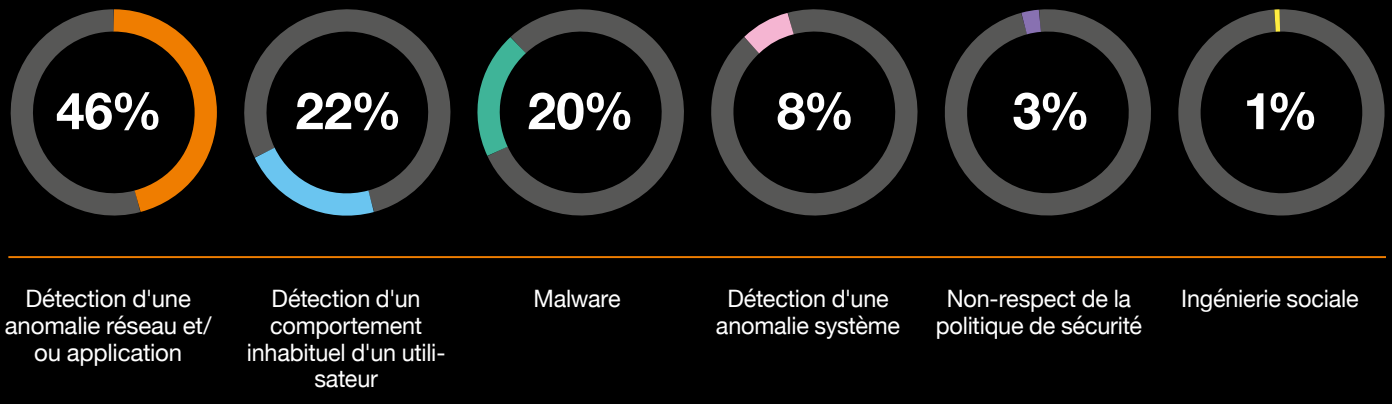
- **Total des évènements analysés : 263 109**
- **Dont 11,17 % (29 391) considérés comme des incidents de sécurité selon la classification de données Orange Cyberdefense*.**
- **Période analysée : l'intégralité des données pour toute l'année 2019.**
- **Source des données : réseau, systèmes, postes de travail, utilisateurs, applications, systèmes de détection d'intrusion (IDS) et tout évènement de sécurité collecté par un SIEM (Security Event Information Management).**

*Les alertes issues de notre périmètre opérationnel incluses pour cette édition spéciale

Tri et qualification des alertes

263 109
Alertes • Évènements

29 391
11,17 % Incidents de Sécurité



Les typologies d'incidents

En 2019, nous avons détecté les typologies d'incidents suivantes :

Réseau et applications : tunnel, alertes IDS/IPS et autres attaques qui perturberaient le trafic réseau ou les applications.

Comptes utilisateurs : attaque par force brute, usurpation d'identité , mouvements latéraux, élévation de privilèges ou incidents similaires.

Malware : logiciels malveillants tels que les ransomwares

Systèmes : évènements qui concernent le système d'exploitation et les périphériques (pilotes cessant de fonctionner ou une interruption de services).

Transgression des politiques de sécurité : installation de logiciels non pris en charge ou connexion de périphériques non autorisés sur le réseau.

Non-respect de la politique de sécurité : installation de logiciels non pris en charge ou connexion de périphériques non autorisés sur le réseau.

En somme

En comparant les précédents rapports, nous constatons une augmentation du nombre d'alertes. Nous avons observé davantage de souscriptions cette année ; cet écart était donc attendu. Ceci dit, il est important de noter que le nombre d'évènements identifiés comme incidents de sécurité a progressé plus que prévu.

Pour un total de 263 109 évènements, 11,17 % (29 391) sont des incidents de sécurité avérés. L'année précédente, ce taux était de 8,31 %, soit une progression de 38 %.

Ceci est assez significatif puisque que le nombre total d'alertes a augmenté de moins de 3 %.

La collaboration avec nos clients pour l'optimisation de notre plateforme et la réduction du nombre de faux positifs explique en partie ce ratio. Quand bien même, il est clair que le nombre d'incidents de sécurité a considérablement augmenté. Les attaquants saisissent chaque opportunité d'exploiter des faiblesses.

Have you been pwned?

Autre tendance majeure selon nous : l'augmentation du nombre d'anomalies sur les comptes utilisateurs.
Dans le rapport précédent, 15 % des incidents tombaient dans cette catégorie, qui se plaçait en troisième position. Cette année, elle atteint la seconde place, avec 22 %. Pourquoi ?

Une explication possible : la fréquence anormale et l'ampleur même des fuites de données cette année. La chronologie 2019 en fait état. Ce sont littéralement des centaines de millions de comptes et identifiants qui ont été volés et vendus sur le Darknet. Si nous ajoutons à cela que les utilisateurs tendent à réutiliser leurs mots de passe – en particulier quand ils doivent être réinitialisés tous les 100 jours, il devient évident que nous multiplions les risques.

Le sujet clé ici est le « credential stuffing » (pratique automatisée consistant à exploiter des informations volées, dont des identifiants et mots de passe associés pour accéder à des comptes utilisateurs). L'augmentation de cette méthode pourrait n'être que le sommet de l'iceberg : même les criminels ont besoin de temps pour traiter et exploiter des données à cette échelle. Vous trouverez davantage d'informations sur les fuites de données, leurs causes et leurs impacts dans le chapitre « L'essor des fuites de données».

L'ingénierie sociale toujours difficilement décelable

Pour le cas de l'ingénierie sociale, les statistiques sont plus délicates. L'ingénierie sociale englobe toutes sortes d'activités précédant habituellement l'attaque. Le processus commence par une recherche ciblée sur différents médias sociaux (tels que LinkedIn ou Facebook) de propriétaires de comptes ou des collaborateurs d'une entreprise ayant des postes clés. Par exemple, les cibles peuvent être manipulées pour divulguer des détails sur les systèmes d'exploitation, les configurations réseaux, voire même des identifiants via des appels téléphoniques frauduleux émis par de faux employés.

Tout ceci peut se dérouler hors du périmètre de l'entreprise et échapper à nos capacités de surveillance habituelles. Nos outils de Threat Intellligence peuvent dans certains cas contribuer à identifier ces occurrences bien qu'en général nous en constations seulement les conséquences.

Les dommages causés par l'ingénierie sociale pourraient, toutefois, être évités, en fonction de la nature et de la sophistication de l'attaque réelle. Les incidents de sécurité qui en découlent sont susceptibles d'être comptabilisés dans les catégories de détection des anomalies sur les comptes utilisateurs ou Malware, bien qu'ils résultent directement de campagnes d'ingénierie sociale.

Une vulnérabilité critique dans la plate-forme de réservation en ligne « Amadeus » corrigée : près de la moitié de toutes les compagnies aériennes au monde affectées
En injectant de simples commandes dans le navigateur, il était possible d'accéder aux dossiers passagers, puis à leurs informations de vol, leurs noms ainsi qu'à d'autres données personnelles. [t3]

Une protection des endpoints active

Un autre changement notable que nous avons observé : le nombre d'incidents liés aux logiciels malveillants a diminué de manière significative. Précédemment, Nous avions classé 45 % des incidents comme étant liés à des malwares. En 2019, ce chiffre a chuté à 22 %. Au cours de la même période, les détections d'anomalies réseau et applications ont quant à elles, progressé de 36 % à 46 %, classant cette catégorie d'incidents au premier rang en 2019.

Faut-il comprendre que les malwares ne sont plus des menaces ? De manière générale non, ils restent des menaces, mais ces données montrent que prévenir la protection des endpoints contribue considérablement à réduire les risques. Ce que nous constatons ici est vraisemblablement le résultat immédiat de systèmes de protection nouvelle-génération appliqués aux endpoints.

Alors que les solutions reposant sur l'IA existent depuis un moment maintenant, leur déploiement a pris un certain temps. Désormais, un nombre croissant de clients a commencé à investir dans des systèmes de protection des endpoints. Le résultat est assez probant : les malwares s'y « cassent les dents », tombant ainsi à la troisième place du classement, juste après la détection d'anomalies au niveau sur les comptes utilisateurs.

Des malwares sophistiqués et menaces persistantes avancées (APT) utilisés dans le cadre d'attaques ciblées s'imposent néanmoins toujours comme de sérieuses menaces. Mais, bonne nouvelle, le niveau du cybercriminel moyen ne correspond plus au niveau des systèmes de protection à jour.

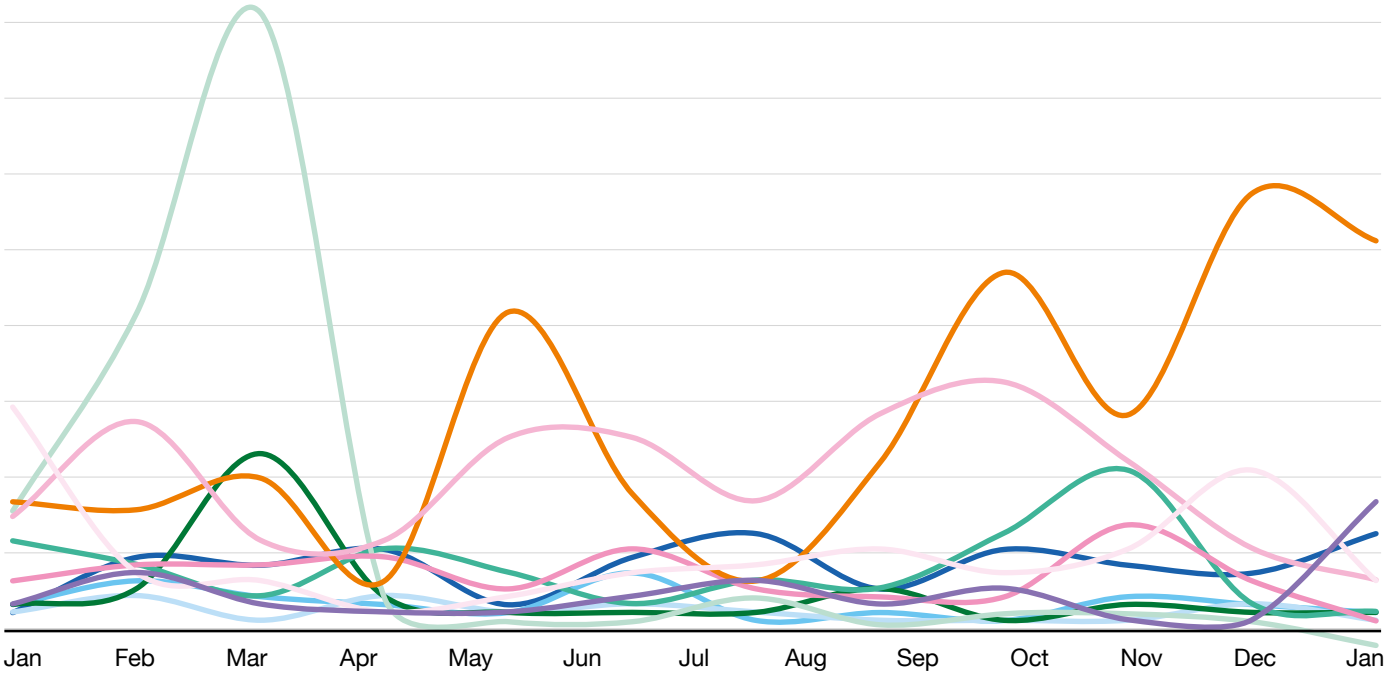
Malwares : analyse des tendances

En observant les tendances globales en matière de logiciels malveillants, nous identifions certains modèles très marqués.

Les deux premières tendances notables sont : la chute du nombre d'attaques début avril, mi-juillet et début décembre. Cette situation est potentiellement liée à une tendance déjà observée les années précédentes : les cybercriminels se professionnalisent et adoptent des horaires de bureau, le « 9h-18h ». Aussi étrange que cela puisse paraître, les pirates prennent désormais régulièrement des vacances « comme tout le monde ». Cela pourrait expliquer la baisse enregistrée en avril, le rythme des attaques ralentissant au moment des vacances de Pâques. La tendance se vérifie sur les périodes des vacances d'été et de Noël en fin d'année.

Les attaques par ransomware ont connu des hauts et des bas, mais restent populaires. Le cas diffère pour les attaques de cryptojacking. Bien que ces deux types d'attaques aient progressé en début d'année, les attaques de cryptojacking ont reculé et leur nombre est resté bas à partir d'avril. Les ransomware ont aussi reculé en avril, mais ont atteint de nouveaux sommets en mai, en octobre et en décembre. Nous avons par ailleurs remarqué que les cours du Monero [2.1], de l'Ethereum [2.2], du Litecoin [2.3] et du Bitcoin [2.4] ont atteint un nouveau pic au début de l'été, sans pour autant augmenter la fréquence des attaques de cryptojacking alors que nous avions précédemment observé une corrélation entre la valeur marchande des cryptomonnaies et la fréquence des attaques. Ceci tend à montrer que le Cryptojacking en tant que menace a cessé d'exister et ne s'imposera plus dans des campagnes à grande échelle.

Vue d'ensemble



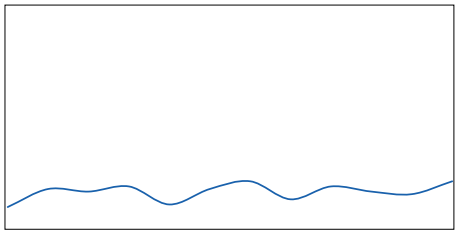
« Collection #1 » : 773 millions d'enregistrements sur le Darknet

Le chercheur australien Troy Hunt a découvert sur le Darknet l'enregistrement d'une collection entière d'informations confidentielles (e-mails et mots de passe) issues de diverses fuites de données. [t4]

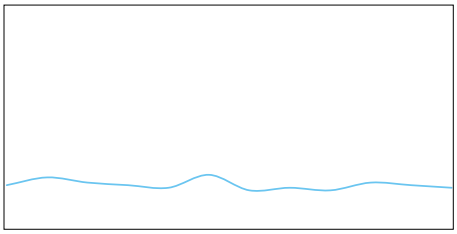
Altran Technologies frappé par une cyberattaque, ses opérations affectées dans plusieurs pays européens

Le leader mondial de services d'ingénierie a, semble-t-il, été frappé par une campagne ciblée qui a affecté ses opérations dans plusieurs pays européens.

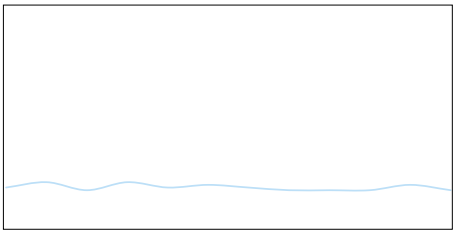
Backdoor/RAT



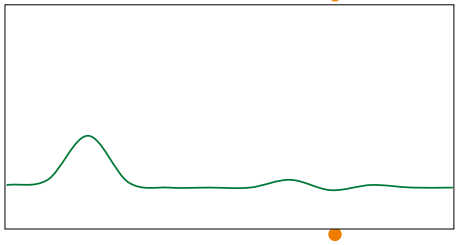
Banker



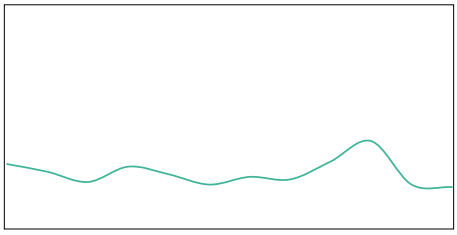
Bot



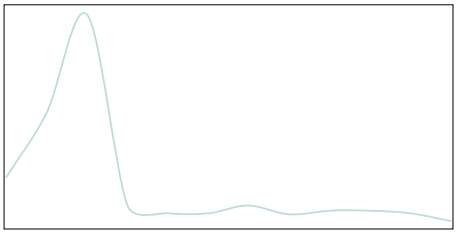
Piratage de cryptomonnaie



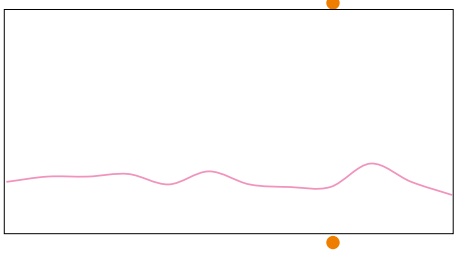
Downloader/Dropper



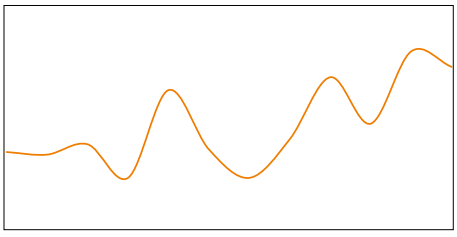
Kit d'exploitation



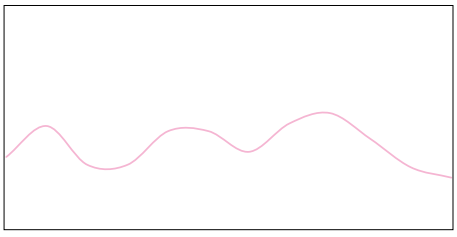
Information Stealer



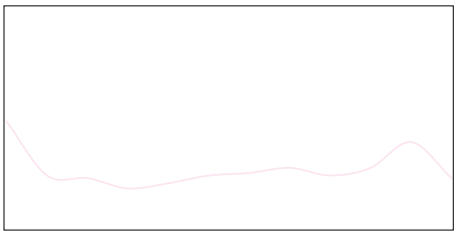
Ransomware



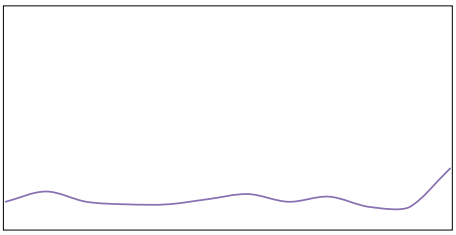
Cheval de Troie



Virus



Ver



GandCrab/Ursnif

Méfiez-vous des Macros sous Word : Ursnif est un cheval de Troie visant à exfiltrer des données critiques et GandCrab est un ransomware classique. Ils se propagent tous deux par le biais d'e-mails de phishing au moyen de pièces jointes malveillantes sous Word. [t6]

La multinationale européenne Airbus attaquée

Airbus et ses fournisseurs ont été frappés par une série d'attaques visant à accéder et dérober leur propriété intellectuelle. [t7]

FÉVR

145 millions de dollars s'évaporent, un PDG emporte dans sa tombe le seul mot de passe

QuadrigaCX, la plus grande plate-forme d'échange de Bitcoins au Canada, dit avoir perdu l'accès à ses portefeuilles de stockage hors-ligne. La seule personne disposant d'un accès à ceux-ci était leur PDG et fondateur, Gerry Cotton, subitement décédé en décembre.[t8]

Contournement de mots de passe E-Scooter : des piratages qui mettent des vies en danger

Les trottinettes électriques Xiaomi M365 sont livrées avec une application Bluetooth apparemment vulnérable. La trottinette ne validant pas de mot de passe, les attaquants peuvent freiner, accélérer ou même l'éteindre à 100 mètres de distance.[t9]

Le fournisseur de services de messagerie sécurisée VFEmail.net balayé

A partir d'une faille de sécurité, des pirates ont entièrement détruit les données des serveurs de fichiers et de sauvegarde de VFEmail, réduisant à néant l'infrastructure : Serveur de messagerie, machines virtuelles et la base de données (cluster SQL Server). Cette attaque ayant pour seule finalité la destruction, aucune demande de rançon n'a été formulée [t10]

Un pirate vend 839 millions de comptes sur le Darknet

Le pirate « Gnosticplayers » a publié sur Dream Market trois lots de données utilisateurs provenant d'une douzaine de sites et services piratés soit un ensemble de 839 millions d'informations personnelles. Beaucoup de ces sites ignoraient même avoir été piratés. [t11]

La taille de l'organisation

La situation a changé. Au regard des précédents chiffres, le changement le moins significatif concerne les petites entreprises. Le précédent rapport montrait que 8% des incidents de sécurité concernaient les petites structures. Aujourd'hui nous constatons une augmentation mineure, celles-ci étant ciblées dans 9,72% des cas.

En revanche, nous avons observé un changement substantiel dans le cas des moyennes et grandes entreprises. L'an dernier, nous avons constaté que les gros acteurs étaient de loin les plus touchés. D'une manière générale, la majorité des incidents se déroulent au sein d'entreprises comptant plus de 10 000 employés.

Mais, cette fois-ci, nous avons aussi vu une augmentation radicale des attaques à l'encontre des organisations de taille moyenne. En 2019, 31 % d'entre elles étaient la cible de cyberattaque, soit une nette progression par rapport aux 19 % des années précédentes. Dans le même temps, les incidents touchant les grandes organisations ont régressé de 73 % à 58,8%.

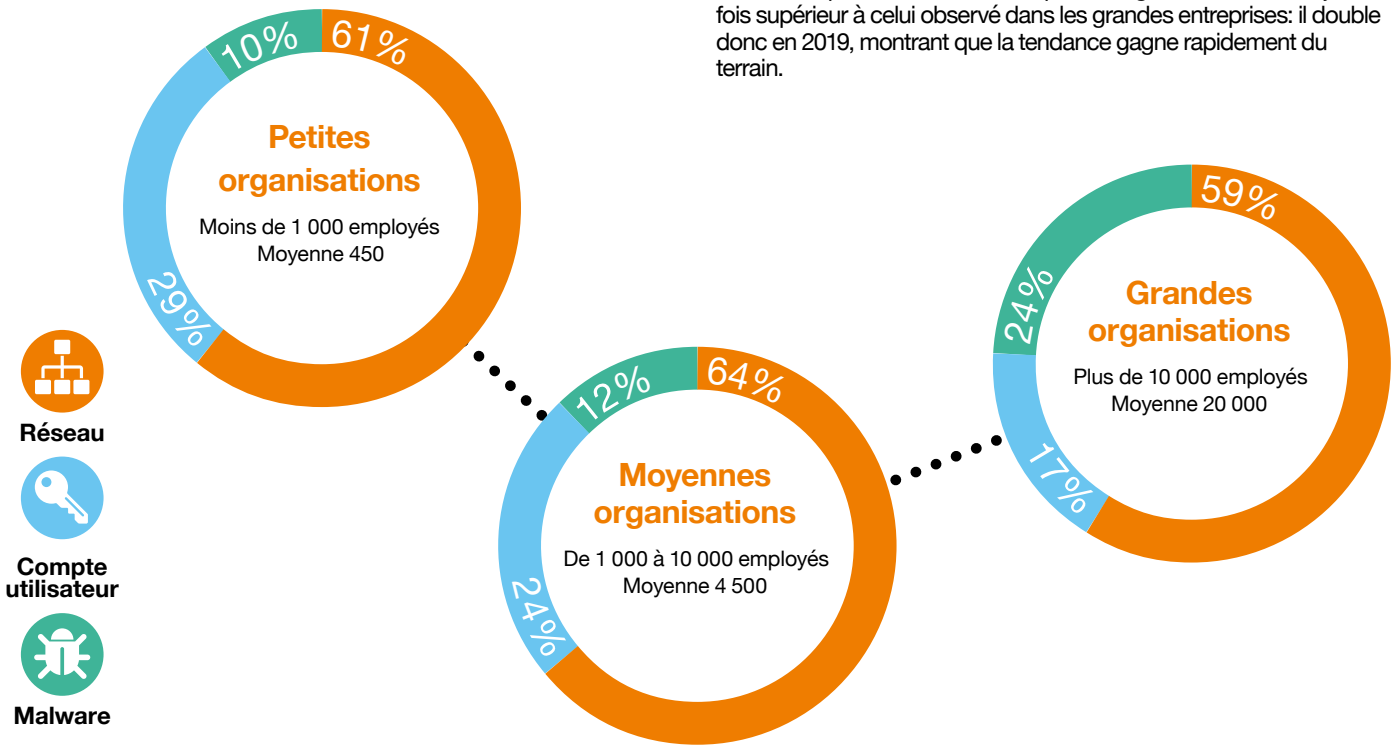
Il semble que les acteurs malveillants ont partiellement changé de centre d'intérêt, ciblant plus qu'auparavant les groupes de taille moyenne, comptant de 1 000 à 10 000 employés.

Les types d'incidents versus la taille des organisations

Le constat que nous faisons ici est cohérent avec les typologies d'incidents analysées dans notre tableau « tri des alertes » en page 18. La même tendance se dessine. Si l'année dernière, les grandes entreprises étaient significativement ciblées par des malwares : cette année, ce sont toutes les tailles d'entreprises qui ont été touchées et qui ont dû faire face notamment à des détections d'anomalies réseau et applications, venant prendre la première place des incidents devant les malwares.

Deux inflexions se détachent cependant : les petites structures souffrent davantage de détection d'anomalies sur les comptes utilisateurs (29 %, contre 24 % pour les organisations moyennes et 17 % pour les grandes) et les grandes structures doivent toujours repousser plus du double des attaques par malware comparativement aux petites entreprises.

En moyenne, le nombre d'incidents par individu dans les petites entreprises est environ quatorze fois supérieur à celui observé dans les grandes organisations. Cela confirme une tendance déjà constatée dans nos précédents rapports dans lesquels le nombre d'incidents par individus dans les petites organisations était déjà six fois supérieur à celui observé dans les grandes entreprises: il double donc en 2019, montrant que la tendance gagne rapidement du terrain.



Incidents
Pour 100 employés

Pour les organisations comptant moins de 1 000 employés, nous remarquons à nouveau une augmentation importante de la proportion d'incidents. En moyenne, le nombre d'incidents par personne est quatorze fois supérieur comparativement aux grandes organisations.

Près d'une personne sur trois travaillant dans une organisation de plus petite taille est désormais ciblée directement par une cybermenace.

Petite Organisation	Moyennes Organisations	Grandes Organisations
29.5	6.4	2.1

Criticité

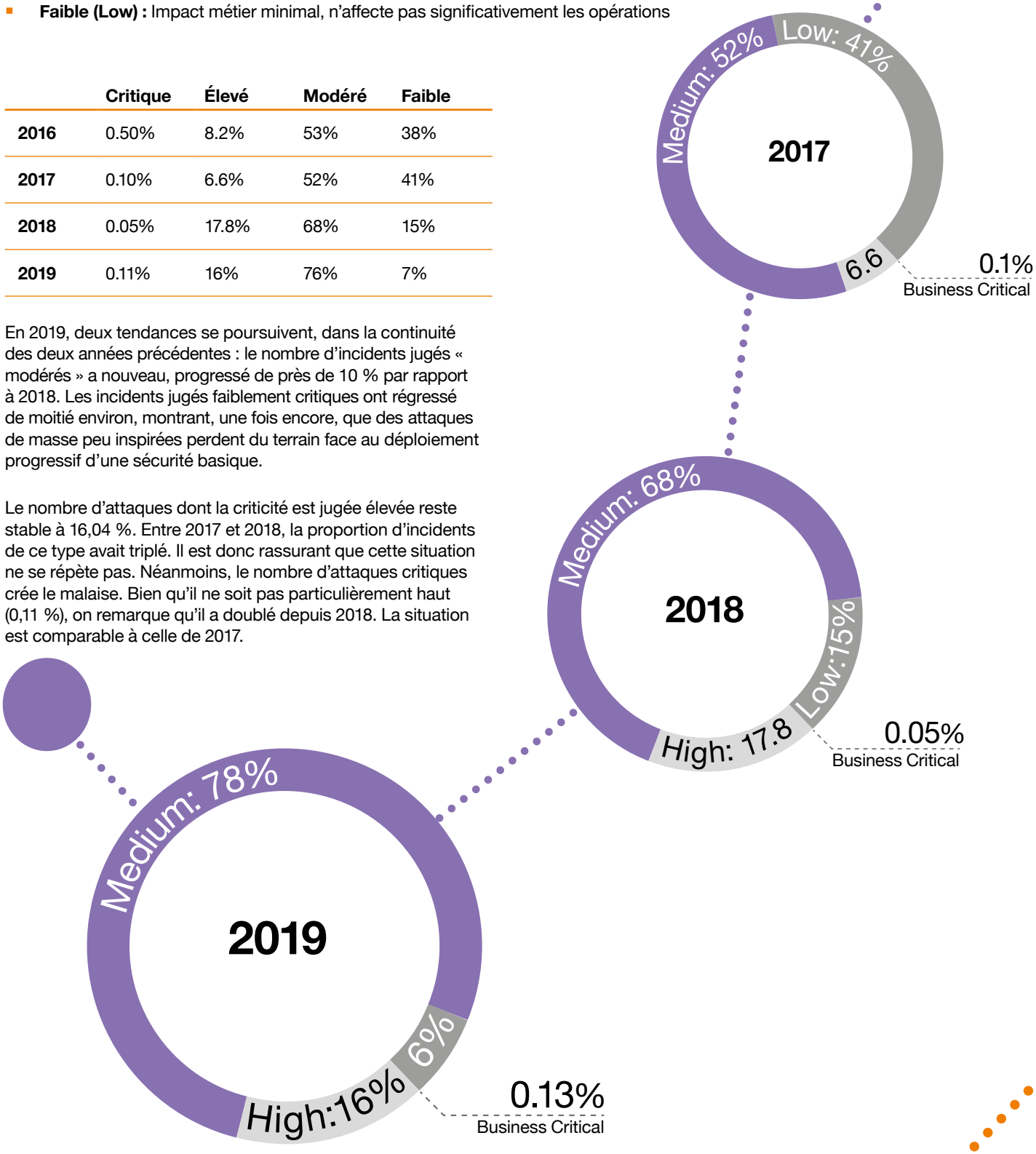
La criticité des incidents est inégale. Chez Orange Cyberdefense, quatre niveaux ont été définis :

- **Critique:** Impact critique sur l'entreprise, processus métiers poussés à l'arrêt
- **Élevé (High) :** Impact métier significatif, incident devant être géré immédiatement
- **Modéré (Medium) :** Impact métier limité, des solutions de contournement acceptables peuvent exister
- **Faible (Low) :** Impact métier minimal, n'affecte pas significativement les opérations

	Critique	Élevé	Modéré	Faible
2016	0.50%	8.2%	53%	38%
2017	0.10%	6.6%	52%	41%
2018	0.05%	17.8%	68%	15%
2019	0.11%	16%	76%	7%

En 2019, deux tendances se poursuivent, dans la continuité des deux années précédentes : le nombre d'incidents jugés « modérés » a nouveau, progressé de près de 10 % par rapport à 2018. Les incidents jugés faiblement critiques ont régressé de moitié environ, montrant, une fois encore, que des attaques de masse peu inspirées perdent du terrain face au déploiement progressif d'une sécurité basique.

Le nombre d'attaques dont la criticité est jugée élevée reste stable à 16,04 %. Entre 2017 et 2018, la proportion d'incidents de ce type avait triplé. Il est donc rassurant que cette situation ne se répète pas. Néanmoins, le nombre d'attaques critiques crée le malaise. Bien qu'il ne soit pas particulièrement haut (0,11 %), on remarque qu'il a doublé depuis 2018. La situation est comparable à celle de 2017.



MARS

L'opération Sharpshooter liée à la Corée du Nord

La campagne de cyber espionnage mondial ciblait les infrastructures critiques d'institutions gouvernementales, de centrales électriques et d'organisations financières. Des leurres ont rendu l'attribution difficile mais aujourd'hui des chercheurs travaillant pour Mc Afee ont officiellement établi le lien avec le groupe Lazarus et la Corée du Nord. [t12]

Mozilla présente Firefox Send, un service gratuit et chiffré de transfert de fichiers

Ce service permet aux utilisateurs de charger des fichiers pouvant aller jusqu'à 1 Go (et 2,5 Go pour les utilisateurs inscrits) et de partager le lien de téléchargement. [t13]

Round 4 — Un pirate met26 millions de nouveaux comptes en vente sur le Dark Web

« Gnosticplayers » récidive : 26 millions de données personnelles sont proposées à la vente. [t14]

Le retour de Mirai

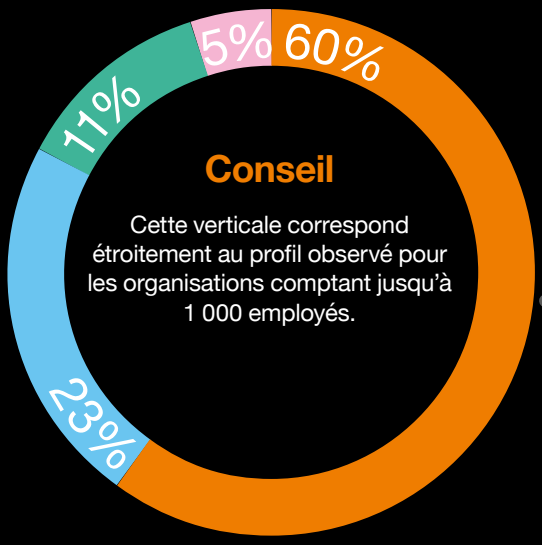
Le botnet IoT Mirai refait surface sous une version « Enterprise Edition », visant désormais spécifiquement à détourner du matériel d'entreprise intelligent – comme les systèmes de présentation sans fil et les routeurs – en bots pour lancer des campagnes de DDoS. [t15]

Répartition des incidents par secteur d'activité

Comment sont distribués les incidents au sein de différentes verticales business ? Nous avons analysé sept industries et avons été surpris des différences que nous avons identifiées.

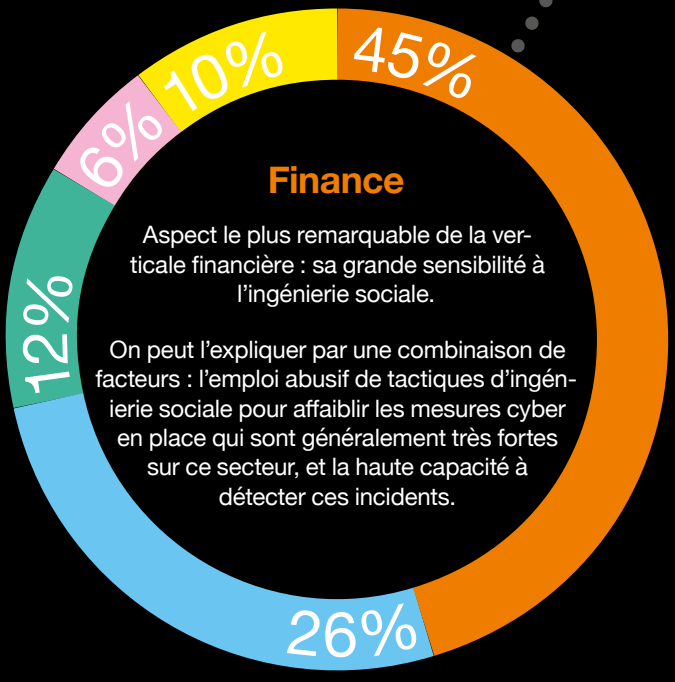
Les pourcentages les plus élevés dans ces graphiques ne veulent pas forcément dire que les incidents surviennent plus fréquemment et que le secteur en question est plus « vulnérable ». Ils peuvent, en effet, démontrer l'inverse. La capacité des entreprises à identifier un incident peut indiquer une plus grande maturité en matière de cybersécurité. Par exemple, dans la finance, les volumes d'ingénierie sociale à des fins frauduleuses sont conséquents, car ces organisations sont plus aguerries dans la gestion de ces incidents. Elles sont en mesure d'en détecter et d'en remonter davantage.

	Réseau	Compte	Malware	Système	Pol. Sécurité	Social
Conseil	59.93%	22.68%	10.85%	5.50%	0.94%	0.10%
Finance	45.06%	26.48%	11.76%	6.19%	0.11%	10.41%
Industrie manufacturière	44.38%	32.63%	16.94%	4.39%	1.63%	0.03%
Industrie agroalimentaire	12.13%	27.62%	43.51%	16.32%	0.00%	0.42%
Service public	49.17%	41.72%	5.30%	1.16%	2.65%	0.00%
Santé	83.19%	5.75%	9.02%	1.84%	0.03%	0.19%
Éducation	39.25%	57.01%	0.47%	0.00%	2.80%	0.47%
Biotechnologies	42.37%	49.57%	4.76%	3.30%	0.00%	0.00%
Retail	34.33%	18.49%	27.84%	12.11%	5.77%	1.46%



Conseil

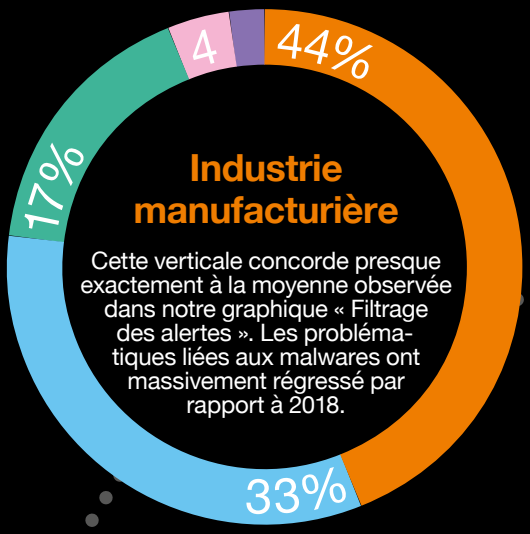
Cette verticale correspond étroitement au profil observé pour les organisations comptant jusqu'à 1 000 employés.



Finance

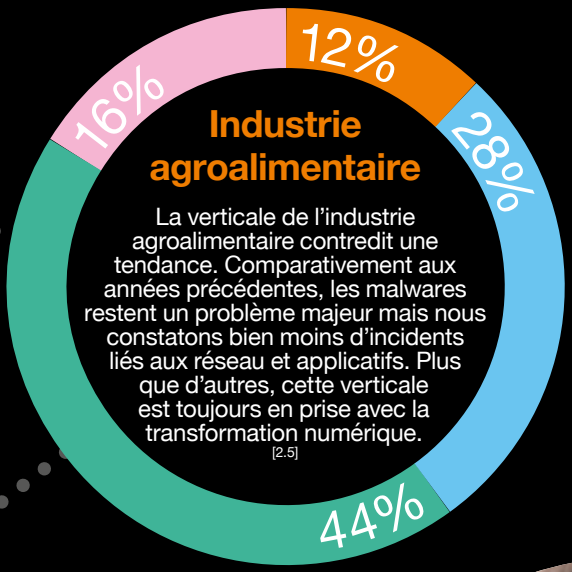
Aspect le plus remarquable de la verticale financière : sa grande sensibilité à l'ingénierie sociale.

On peut l'expliquer par une combinaison de facteurs : l'emploi abusif de tactiques d'ingénierie sociale pour affaiblir les mesures cyber en place qui sont généralement très fortes sur ce secteur, et la haute capacité à détecter ces incidents.



Industrie manufacturière

Cette verticale concorde presque exactement à la moyenne observée dans notre graphique « Filtrage des alertes ». Les problématiques liées aux malwares ont massivement régressé par rapport à 2018.

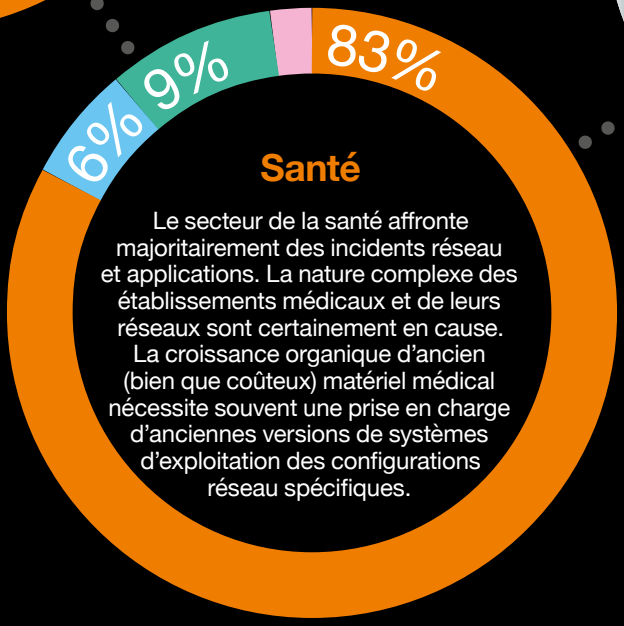


Industrie agroalimentaire

La verticale de l'industrie agroalimentaire contredit une tendance. Comparativement aux années précédentes, les malwares restent un problème majeur mais nous constatons bien moins d'incidents liés aux réseau et applicatifs. Plus que d'autres, cette verticale est toujours en prise avec la transformation numérique. [2.5]

Service Public

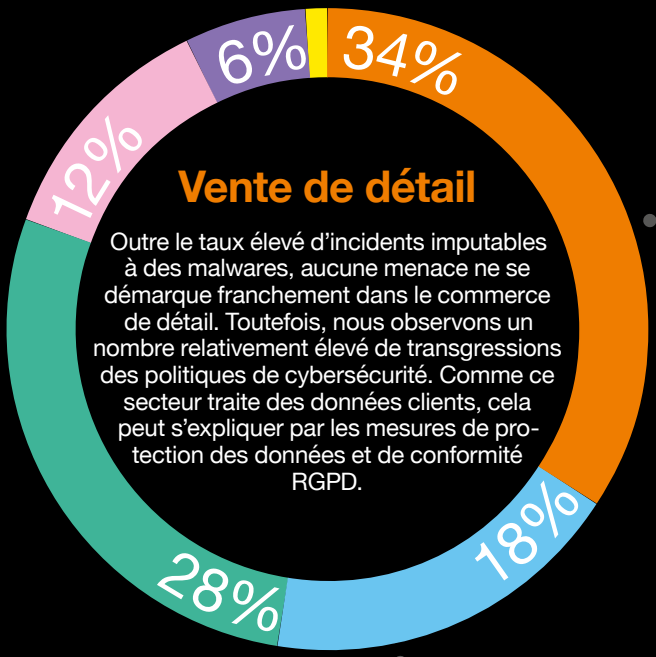
On note ici que les établissements gouvernementaux et institutions publiques font face, plus que tout autre verticale, à des problématiques liées aux comptes utilisateurs. Naturellement, ce secteur en gère un volume très important, cette situation n'est donc pas surprenante. Les taux de détection élevés montrent aussi une forte sensibilisation à la sécurité de ces derniers.



Santé

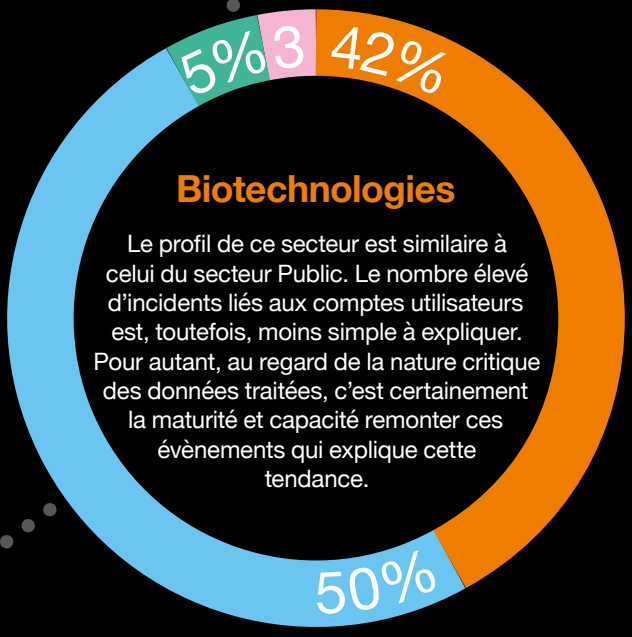
Le secteur de la santé affronte majoritairement des incidents réseau et applications. La nature complexe des établissements médicaux et de leurs réseaux sont certainement en cause. La croissance organique d'ancien (bien que coûteux) matériel médical nécessite souvent une prise en charge d'anciennes versions de systèmes d'exploitation des configurations réseau spécifiques.

Vente de détail



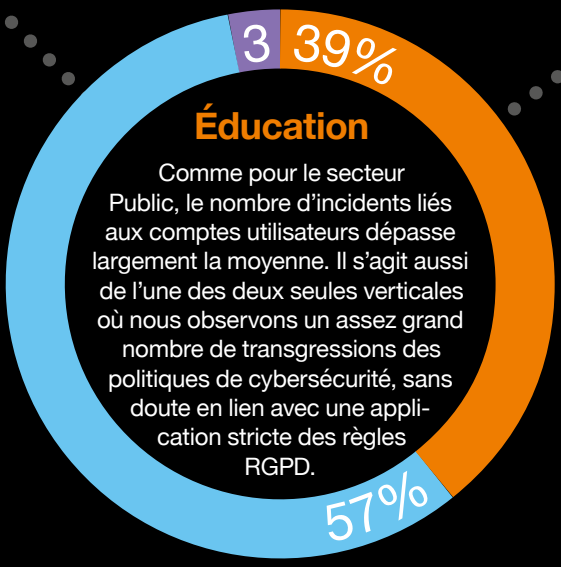
Outre le taux élevé d'incidents imputables à des malwares, aucune menace ne se démarque franchement dans le commerce de détail. Toutefois, nous observons un nombre relativement élevé de transgressions des politiques de cybersécurité. Comme ce secteur traite des données clients, cela peut s'expliquer par les mesures de protection des données et de conformité RGPD.

Biotechnologies



Le profil de ce secteur est similaire à celui du secteur Public. Le nombre élevé d'incidents liés aux comptes utilisateurs est, toutefois, moins simple à expliquer. Pour autant, au regard de la nature critique des données traitées, c'est certainement la maturité et capacité remonter ces évènements qui explique cette tendance.

Éducation



Comme pour le secteur Public, le nombre d'incidents liés aux comptes utilisateurs dépasse largement la moyenne. Il s'agit aussi de l'une des deux seules verticales où nous observons un assez grand nombre de transgressions des politiques de cybersécurité, sans doute en lien avec une application stricte des règles RGPD.

Conclusion

La tension monte. Le taux croissant de remontée d'alertes et d'incidents nous le prouve. Bien entendu, il s'explique aussi par l'effort investi dans le paramétrage fin de ces événements de sécurité (éliminant les faux-positifs), mais il nous dit aussi que la cybermenace nous talonne toujours.

Dans le rapport précédent, les malwares s'imposaient comme source principale d'incidents, représentant près de la moitié des attaques détectées par nos CyberSOC. Cette année, ce sont les incidents liés au réseau qui l'emportent.

La réduction du nombre d'incidents liés aux malwares a été rendue possible grâce à la mise en œuvre par nombre de nos clients de systèmes modernes de protection du endpoint.

Cependant, les anomalies détectées sur les comptes utilisateurs et les malwares ne doivent pas être sous-estimées. Elles demeurent des menaces réelles, et ont des impacts majeurs sur leurs victimes lorsqu'elles frappent. La détection et la réponse appliquées aux endpoints contribuent à limiter le facteur de risque à certains égards, la détection est plus efficace (et plus rentable) qu'un seul investissement massif dans la prévention. En outre, les solutions de détection et de réponse des menaces cachées dans le trafic réseau complètent bien les systèmes de détection appliqués aux endpoints et ceux opérés par les SIEM.

Une évolution considérable des attaques ciblant les petites et moyennes entreprises démontre que ces organisations de moindre envergure ont encore du chemin à faire sur le plan de leur maturité et de leur sensibilisation à la menace cyber.

L'investissement ne se limite pas aux technologies : l'accès à des experts disposant de compétences appropriées est crucial. Et sur un marché sur lequel la cyber expertise est rare (jusqu'à 2,9 millions de postes à pourvoir aujourd'hui selon l'organisation à but non lucratif ISC2), les services managés de détection et de réponse deviennent des solutions d'autant plus pertinentes. Les grandes entreprises et multinationales les ont très vite adoptées. Nous espérons pour les structures de taille moyenne qu'elles s'y intéressent rapidement.

Il sera intéressant de revenir sur ces chiffres et sur leur évolution pour mesurer l'impact majeur de la crise du COVID-19 dans notre prochain Security Navigator en décembre. Sur cette période, le passage au télétravail et la transformation des schémas d'attaques au sein de la communauté cybercriminelle pourraient avoir de lourdes conséquences.

Norsk Hydro stoppe l'intégralité de son réseau après une attaque par ransomware

Plusieurs usines implantées dans différents pays ont dû être fermées ou ont dû fonctionner en urgence en mode manuel suite à une infection par LockerGoga se propageant depuis ses sites américains. [t16]

AVR

Des défibrillateurs vulnérables aux attaques

Les appareils fabriqués par Medtronic fonctionnent sur un protocole de connexion radio propriétaire, dont le déploiement est fondamentalement défectueux. Il n'embarque aucun chiffrement, aucune vérification d'authentification, ni aucune validation des données. [t17]

Bithumb (encore) piraté : 19 millions de dollars volés

Trois millions d'EOS et 20 millions d'XRP ont été dérobés de portefeuilles compromis. L'an dernier, Bithumb avait déjà perdu l'équivalent de 32 millions de dollars d'EOS, volés à plusieurs millions de ses utilisateurs. [t18]

540 millions de lignes de données utilisateurs Facebook trouvés sur des serveurs Amazon non protégés

La société de médias mexicaine Cultura Colectiva avait rassemblé 146 Go de données dont les commentaires, les mentions « j'aime », les noms de comptes et identifiants d'utilisateurs Facebook, et les avait laissées en accès public sur les serveurs AWS. Facebook semble déjà avoir perdu le contrôle sur les données de millions d'utilisateurs ; données dont des tiers se sont emparés. [t19]

TajMahal : découverte d'une nouvelle menace persistante avancée

TajMahal est une boite à outils dit « toolkit » comportant un ensemble de 80 modules aux possibilités « jamais vues ». Il existe apparemment depuis au moins cinq ans, mais n'avait jusqu'alors pas été détecté. [t21]

Le site Aéroports de Lyon visé par une cyberattaque

Les clients – réservant notamment des places de stationnement et des accès aux lounges se sont retrouvés dirigés depuis la page d'accueil vers un site de phishing qui essayait de dérober leurs identifiants et leurs données. [t28]

La ville de Baltimore mise à l'arrêt par un ransomware

Bien que les lignes d'urgence, dont le 911, n'aient pas été affectées, la plupart des services civils tels que les services des travaux publics, des finances et des transports ont vu leurs services de messagerie et leurs lignes téléphoniques être totalement interrompus. [t27]

Europol ferme Wall Street Market et Silkkitie (dit Valhalla)

Les forces de l'ordre internationales ont démantelé deux tristement célèbres places de marché sur le Darknet. Wall Street Market, deuxième plus grande marketplace au monde avec quelques 5 400 vendeurs et des millions d'utilisateurs, permettait d'échanger drogues, données volées, services de piratage et codes malveillants. [t26]

Fleury Michon interrompt sa production pendant cinq jours suite à un virus informatique

Onze sites de production ainsi que l'unité de logistique ont été fermés. La direction explique que le coût de cette interruption est pris en charge par une assurance cyber. [t24]

MAI

Découverte d'une mystérieuse base de données contenant les informations personnelles de 80 millions de citoyens américains

Des Hacktivistes réputés, Noam Rotem et Ran Locar, ont découvert une base de données non protégée contenant des informations sur près de 65 % des ménages américains, et hébergée sur un serveur Cloud Microsoft. L'identité du propriétaire de cette base et l'objectif de celle-ci restent inconnus.[t25]

L'infection d'Electrum Wallet se propage à grands pas, 4,6 millions de dollars volés

L'attaque a pour origine un groupe de serveurs piratés prétendant appartenir au réseau Electrum. Ils répondaient par un faux message d'erreur à des requêtes légitimes, piégeant ainsi l'application Electrum Wallet en lui faisant télécharger une mise à jour malveillante. Ce téléchargement permettait de dérober les fonds présents sur les wallets et contenait un botnet utilisé ensuite pour mener des attaques par DDoS sur les serveurs Electrum légitimes. [t23]

La messagerie instantanée du gouvernement français « Tchap » piratée

Suite à une validation incorrecte des e-mails autorisés, le chercheur en cybersécurité Elliot Alderson a pu se connecter à l'application qui devait être réservée aux fonctionnaires gouvernementaux. [t22]

Paul van der Haas
Lead Engineer Operations SLI
Orange Cyberdefense

Thomas Eeles
CSIRT Manager
Orange Cyberdefense

Récits du Pentest et du CSIRT

Les contes de la « cave »

Il était une fois, un test d'intrusion

Au fil du temps, les pentesters ont acquis une certaine réputation ainsi qu'un arsenal de compétences hautement spécifiques. Ces compétences ne diffèrent pas beaucoup de celles qu'ont les pirates que les entreprises cherchent désespérément à tenir éloignés, Et même si dans notre cas, vous nous faites confiance pour divulguer nos rapports de manière responsable. Il n'empêche qu'on boit aussi du café, en quantité, et que nous aimons les donuts. Ceux avec des pépites !

La réputation n'a d'égale que la confiance. Nos clients apprennent à nous connaître, ils s'émerveillent de notre savoir-faire et choisissent de se fier à nous. Ils nous invitent alors à identifier pour eux des vulnérabilités, voire, à les exploiter. Quel meilleur moyen pour démontrer la menace se loge ?

Notre réputation nous précède. Souvent, nos équipes commerciales vantent nos mérites, s'enorgueillissant du peu de temps qu'il nous faudrait pour prendre la main sur le compte d'un administrateur de domaine. Tout ça avant même que le premier café ne soit fini… et que le client ne revienne avec des donuts saupoudrés.

Les temps changent, de pareils contes sont voués l'histoire cyber Les fables les relayeront et les histoires que nous lirons à nos enfants pour s'endormir rendront populaires ces pentesters de l'ancien temps.

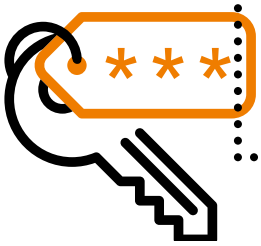
Alors, n'oubliez pas vos marshmallows et suivez le guide au sous-sol de la cybersécurité !

1er récit : Le défaut du défaut de sécurité

Une nouvelle mission nous est parvenue de l'un de nos clients ; mission dont les objectifs étaient clairement précisés : identifier les vulnérabilités du réseau interne, les exploiter et tester plus en profondeur ce réseau. Une tâche assez conventionnelle, certes, mais nous avions permission d'exploiter et d'explorer : choses que nous faisons bien. Café et donuts étaient livrés, et nous nous lancions à la découverte du réseau au moyen d'un logiciel de scan.

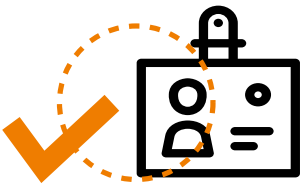
1 Scanner

Le café était encore chaud, les scans toujours en cours, quand un membre de notre équipe déclarait déjà avoir découvert une application Web qui ressemblait à un panneau d'administration pour l'Active Directory du client. Se remémorer le passé… il ne serait sûrement pas possible de se connecter avec « admin/admin », n'est-ce pas ?



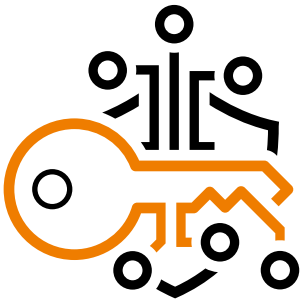
2 Se connecter avec des identifiants par défaut

A peine le café fini, le portable rangé, il y a un nouvel administrateur de domaine dans la maison !



3 Obtenir un accès privilégié

Comme vous l'aurez sans doute deviné, il a été possible de se connecter avec ces identifiants. L'application utilisait un compte doté de droits d'accès privilégiés à l'Active Directory du client dans le but de rendre l'administration du domaine plus aisée et permettre aux administrateurs du support de gérer les comptes clients.



4 Camoufler n'est pas sécuriser

Sans mauvaises intentions, le client avait configuré le compte d'administration de domaine pour atteindre ce but. L'application dissimulait le mot de passe du compte par simple camouflage, mais uniquement côté client.

JUIN

GoldBrute cible 1,5 million de serveurs RDP

Cette attaque par force brute orchestrée par le botnet GoldBrute cible les accès aux serveurs Windows RDP accessibles sur Internet. Pour éviter la détection, chaque bot n'envoie qu'un couple identifiant/mot de passe à plusieurs serveurs différents, chaque requête provenant ainsi toujours d'une IP différente. [t29]

5 Exploiter la faille

En exploitant l'erreur du client, il a été possible de modifier le champ du mot de passe pour l'afficher en clair et révéler aux pentesters les identifiants de l'administrateur de domaine.

6 Aboutir à une compromission complète

Encore un peu plus de la moitié d'un donut restant à manger, et nous avions dévoilé le compte dont les droits sont les plus élevés en informatique. Le drapeau du camp adverse capturé, la ligne d'arrivée franchie, ce que le client pensait en sécurité était désormais compromis.

Enseignements

Bien que ce chapitre sur les tests d'intrusion ne constitue qu'une fraction de l'histoire informatique du client, plusieurs enseignements sont à tirer.
Qu'est ce qui n'a pas fonctionné ? Les identifiants par défaut ou l'application échouant à protéger suffisamment les identifiants de l'administrateur de domaine ?

Il nous faut remonter dans le temps pour comprendre. La sécurité de l'information a pour coutume d'admettre que les contrôles de sécurité échouent, aussi, se baser sur un seul contrôle est tout bonnement inefficace. En lisant cette histoire depuis le début, vous remarquerez que les contrôles sont faibles, et même absents, à commencer par :

- **Les contrôles d'accès au réseau – (NAC) () :** Les pentesters ont pu se connecter au réseau sans avoir à surmonter de quelconques obstacles. Les NAC auraient pu leur donner du fil à retordre pour simplement se connecter au réseau et à ses services.
- **Principe de moindre privilège :** des identifiants bien trop permissifs. Le compte de l'administrateur de domaine a un but : gérer le domaine (via le contrôleur de domaine). L'accès à ce compte devrait être extrêmement limité.
- **Segmentation et filtrage :** L'application découverte était utilisée pour gérer des comptes utilisateurs. Il n'y avait aucune raison pour qu'un matériel non administratif puisse accéder à l'application. Une segmentation fonctionnelle aurait dû être mise en place et filtrer les accès autorisés à l'application. Gardez toujours à l'esprit le principe de moindre privilège !
- **Identifiants par défaut :** changez toujours les identifiants par défaut des systèmes et applications. Ces identifiants sont délibérément faibles et généralement publiquement connus. Des politiques et procédures devraient être établies pour exiger le changement des identifiants par défaut.

Les récits du CSIRT

Cette année, le CSIRT Orange Cyberdefense a eu à gérer des incidents de sécurité sans précédent. Un flux continu d'e-mails Microsoft Office 365 piratés a servi à des attaques par ransomware de grande ampleur. Ces attaques n'étaient pas imputables à des États et, pour la plus grande partie, n'étaient pas extrêmement sophistiquées selon nos critères. Cependant, elles ont toutes causé de sérieux dommages avant que nous ne soyons appelés pour y remédier. Cette section s'intéresse à une infime sélection de quelques erreurs constatées en 2019 ainsi qu'aux pertes occasionnées.

2ème récit : La brèche à un million sur un réseau à plat

C'est l'histoire d'un cauchemar informatique et une fable aussi vieille que ce domaine : « Personne ne va nous pirater. Il n'y a rien qui vaille la peine d'être volé chez nous ». Pourquoi alors s'embarrasser des bonnes pratiques, même les plus élémentaires ? C'est exactement ce que nous avons trouvé : Un réseau à plat, sans sauvegardes, plus de 30 comptes d'administrateurs de domaine, et pas de connexion centralisée…

1 L'enfer des macros Word

Ce réseau à plat sous-entendait que lorsque quelqu'un ouvrait un fichier Word porteur de macros, personne ne s'apercevait que leur antivirus prévenait (mais sans le bloquer) le téléchargement d'Emotet. Aussi, personne ne voyait que, peu après, un compte d'administrateur local était utilisé pour installer des outils de cartographie réseau.

2 Pas d'alerte

Un SOC (Security Operations Centers) efficace aurait pu émettre une alerte précoce informant tous les utilisateurs de ces incidents. Ils auraient alors été résolus rapidement et les utilisateurs auraient bénéficié, dans la foulée, d'une formation les aidant à prévenir d'éventuels incidents ce type. Mais, ça ne s'est pas passé comme ça.

3 Jackpot pour les pirates

Les attaquants ont eu de la chance : la protection du compte admin local sur le poste auquel ils ont accédé était très faible, pour rester poli.

La situation passe alors de préoccupante à épouvantable, car le mot de passe d'administration local était identique pour l'ensemble des endpoints du réseau, dont les serveurs et les hyperviseurs.

Les attaquants ont ainsi obtenu un accès total à l'intégralité du réseau…

Le ransomware GandCrab neutralisé

Un outil gratuit de déchiffrement a été publié, il y a quelques mois, pour aider les victimes du GandCrab à récupérer leurs données. [t30]

5 Diffuser un ransomware

L'attaque s'est ensuite avérée dévastatrice quand Ryuk, ransomware très populaire, a été installé dans un dossier de partage sur le serveur de contrôle du domaine, accompagné d'une liste de plus de 4 000 terminaux Microsoft Windows dans un simple fichier ".txt", d'un fichier ".bat" et d'une copie du fichier binaire Windows "PsExec" légitime.

En un clic, le fichier .bat libérait Ryuk sur le réseau, chiffrant tous les fichiers utilisables et forçant l'entreprise à un arrêt total.

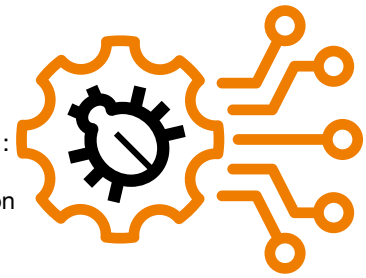
6 Remédiation

Au total, le CSIRT Orange Cyberdefense a travaillé quatre semaines pour restaurer le réseau et le rendre à nouveau opérationnel.

Contre les conseils d'Orange Cyberdefense, le client a réglé un demi-million d'euros aux attaquants pour récupérer les clés de déchiffrement. Par-dessus le marché, il leur a fallu payer des centaines de milliers d'euros de frais à un cabinet d'avocats en charge de gérer le paiement aux pirates Enfin, plus d'un demi-million a été investi pour restaurer le réseau et modifier leurs politiques de sécurité jusqu'à ce que le réseau soit nettoyé et de confiance.

4 Mouvements latéraux et destruction

Les attaquants ont donc poursuivi : suppression des sauvegardes, désactivation des antivirus, création de comptes d'administration de domaine, recours à BloodHound pour cartographier tout le réseau et ouverture des pare-feux à des connexions RDP externes.



Enseignements

Que retenir de ce terrifiant récit ?

Il aurait été possible de remédier à la majorité des failles dans ce réseau : segmenter le réseau est probablement la mesure sécuritaire la plus basique, autant que la mise en œuvre de politiques fortes pour le choix des mots de passe et la restriction des droits utilisateurs. Ces mesures ont quelques impacts sur la façon dont les équipes informatiques travaillent, mais ne sont pas particulièrement coûteuses à déployer. Certes, la remise à niveau d'un SOC est un projet lourd, c'est pour cette raison qu'il faut s'assurer que le réseau met en œuvre les bonnes pratiques de sécurité dès sa création.

Le plus terrible dans cette histoire : nous avons volontairement édulcoré par souci de confidentialité.

3ème récit : une délicate affaire d'email

Cette attaque n'a pas affecté le directeur financier de l'entreprise autant que dans la première histoire mais elle a causé des insomnies aux responsables des relations publiques durant de longues semaines. Sans surprise, un nombre croissant d'organisations se fient désormais au Cloud, en particulier, lorsqu'il s'agit de leurs e-mails et de partages de fichiers. Microsoft Office 365 (O365) tenant la première place des fournisseurs d'hébergement d'e-mails pour les grands groupes.
Comme souvent dans l'informatique, ce changement de pratique a vu naître quelques mauvais génies de la sécurité.

1 Un spam haut placé

Début 2019, un client nous contacte pour enquêter sur un sujet « sensible » en lien avec le piratage d'un compte mail O365.

Afin de maintenir le niveau d'accord parental acceptable de ce rapport, nous nous contenterons de dire que des spams « pour adultes » avaient été envoyés à des centaines de milliers de comptes par un cadre haut placé de l'organisation.

2 Une mauvaise réputation mais pas que…

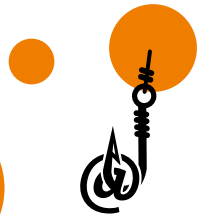
Cet incident confronta notre client à deux problèmes : d'une part, évidemment, un cauchemar en matière de réputation et communication puisqu'un membre du Comité exécutif avait spammé un grand nombre de personnes en leur envoyant des insanités ; et, d'autre part, quelqu'un avait accès à des e-mails hautement sensibles dans l'environnement client O365.

Avaient-ils alors transféré ou copié une partie de ces emails ? Il a rapidement été évident que l'utilisateur en question avait fait l'objet d'une attaque par bourrage d'identifiants.

3 Le bourrage d'informations d'identification

L'attaque s'est avérée bien plus conséquente qu'initialement anticipé.

Des milliers de combinaisons identifiants/mots de passe pointaient vers l'infrastructure O365 de l'organisation. Grâce aux logs fournis par Microsoft, nous avons réussi à déterminer que la liste utilisée était une base de données de mots de passe LinkedIn datant de 2016. L'utilisateur du premier compte piraté utilisait le même couple e-mail/mot de passe pour LinkedIn et son compte mail professionnel.



4 Bannir les mots de passe non sécurisés

Nous avons constaté que bien plus d'une centaine de comptes avaient été visités depuis quatre adresses IP suspectes, que nous pouvions associer à d'autres campagnes de spam obscènes.

À cette étape, le client aurait pu mettre en œuvre des protections pour limiter les risques face à ce type d'attaques. Il n'est pas simple, mais tout de même possible, d'empêcher les utilisateurs de réutiliser les mêmes mots de passe. Les mots de passe piratés peuvent être bloqués sur les réseaux d'entreprise. Par ailleurs, des services comme « Have I Been Pwned » permettent d'associer des hashs de mots de passe à des listes divulguées connues. Vous pouvez donc disposer d'une liste extensive de mots de passe à bannir.

Facebook présente Libra, sa cryptomonnaie

Le plus puissant des réseaux sociaux annonce le lancement de sa propre cryptomonnaie basée sur la Blockchain dès 2020. Cette annonce a été suivie d'une myriade de réactions pour le moins mitigées. [t31]

5 Retracer l'attaque

Une fois satisfaits d'avoir identifié tous les comptes qui avaient été impactés pendant l'attaque, nous en avons cartographié le déroulement et déterminé les datas auxquelles les attaquants avaient pu avoir accès.

6 Hack automatisé, mais pas de fuite de données

L'horodatage nous montra que l'attaque était automatisée. Le délai entre l'accès et l'envoi des premiers e-mails n'était que de quelques secondes. Aussi, le volume d'envois en un laps de temps si court concordait avec d'autres campagnes dont il a été prouvé qu'elles étaient automatisées.

Nous n'avons pas non plus trouvé de signes de synchronisation ou de téléchargement des mails, ni même des règles de transfert sur les comptes affectés.

7 Remédiation

Nous pouvions simplement constater l'accès à des centaines de comptes de messagerie, puis l'envoi de millions d'e-mails habilement supprimés : ce qui plut au DPO, mais pas aux équipes des relations publiques ou du marketing.

Enseignements

Comme dans le cas du premier récit, quelques changements simples auraient pu être configurés pour stopper l'incident dès son origine. Les utilisateurs ont tendance à accéder à leurs e-mails depuis les mêmes appareils et adresses IP (tout du moins le même bloc d'IP pays). Les alertes notifiant les accès mail depuis des IP anormales constituent un outil de détection précoce.
En particulier si elles sont corrélées à d'autres tentatives d'authentification.

Néanmoins, la mesure principale reste l'authentification à double facteurs (2FA). En 2019, toutes les organisations disposant d'une infrastructure/de services Internet sans double authentification s'exposaient à des risques. Ce procédé arrête la majorité des attaques opportunistes à l'origine de tant de dommages. S'il est aisé et gratuit de scanner des IP, l'authentification 2FA elle peut être plus délicate. Mais, vous en voyez déjà les avantages après une ou deux semaines d'efforts seulement pour la mettre en place. Il ne fait pas de doute que tous devraient appliquer l'authentification 2FA.

Voilà donc, trois récits qui – depuis les « tranchées » du Pentest et du CSIRT – témoignent de la façon dont vous pouvez mettre un terme à des désastres financiers et liés à votre réputation. En s'en tenant seulement aux meilleures pratiques du secteur, beaucoup de clients pourraient réduire drastiquement la menace induite par ces attaques. Une fois la sécurité de base couverte, vous pouvez envisager de mettre un terme à ce type de piratage autrement plus « sexy », ou à des attaques sophistiquées orchestrées par des États.

Laurent Célérier
Executive VP Technology & Marketing,
Orange Cyberdefense
Former senior officer,
French Ministry Of Defense

L'essor des fuites de données

Où sont passées les données ?

L'histoire nous a montré que 2017 aura été l'année des ransomwares. Nos malheureux confrères du département informatique (et, plus encore, ceux de notre CSIRT !) gardent un souvenir anxieux des campagnes dévastatrices de WannaCry, Petya et NotPetya.

L'extorsion en ligne n'avait rien d'une nouveauté, mais le succès des campagnes par ransomware en 2017 a été matière à médiatisation. À cette attention sans précédent des médias s'ajoutent des entreprises meurtries : c'est une année que nous ne sommes pas prêts d'oublier.

2018 a porté son lot de misère, certes pas d'envergure « biblique », mais le cryptojacking a sans doute causé préjudice à beaucoup de portefeuilles numériques (et aux factures d'électricité). Lourdement dépendant de la valeur marchande de Bitcoin et d'autres cryptomonnaies, l'usage de ces logiciels escrocs a progressé au cours du premier semestre donnant lieu à des attaques réussies d'un nouveau genre. Globalement, les botnets se sont vus attribuer une nouvelle mission, leur puissance de calcul évoluant des campagnes de spams traditionnelles et d'attaques par DDoS vers la génération de revenus numériques.

Alors en 2019, quelle aura été l'évolution la plus marquante ? Elle pourrait ne pas être considérée comme olympique, mais elle restera dans les mémoires comme une année record en matière de violation de données.

Le temps : un facteur crucial

Le temps, et le manque de temps, sont toujours des facteurs centraux dans la gestion des fuites de données. Un bon nombre d'entre elles ne sont découvertes que plusieurs années après être survenues. Certaines fois aussi, elles se poursuivent des mois, voire des années, avant d'être détectées. Souvent, les organisations en sont informées par les autorités ou des chercheurs en sécurité qui découvrent des données les concernant dans de sombres recoins du Web. Il est alors bien trop tard pour éviter aux individus d'être touchés et aux organisations d'être décontenancées. Il est souvent difficile de remonter à la source et de définir comment et quand les données ont pu fuir.

Un impact en milliards, non en millions

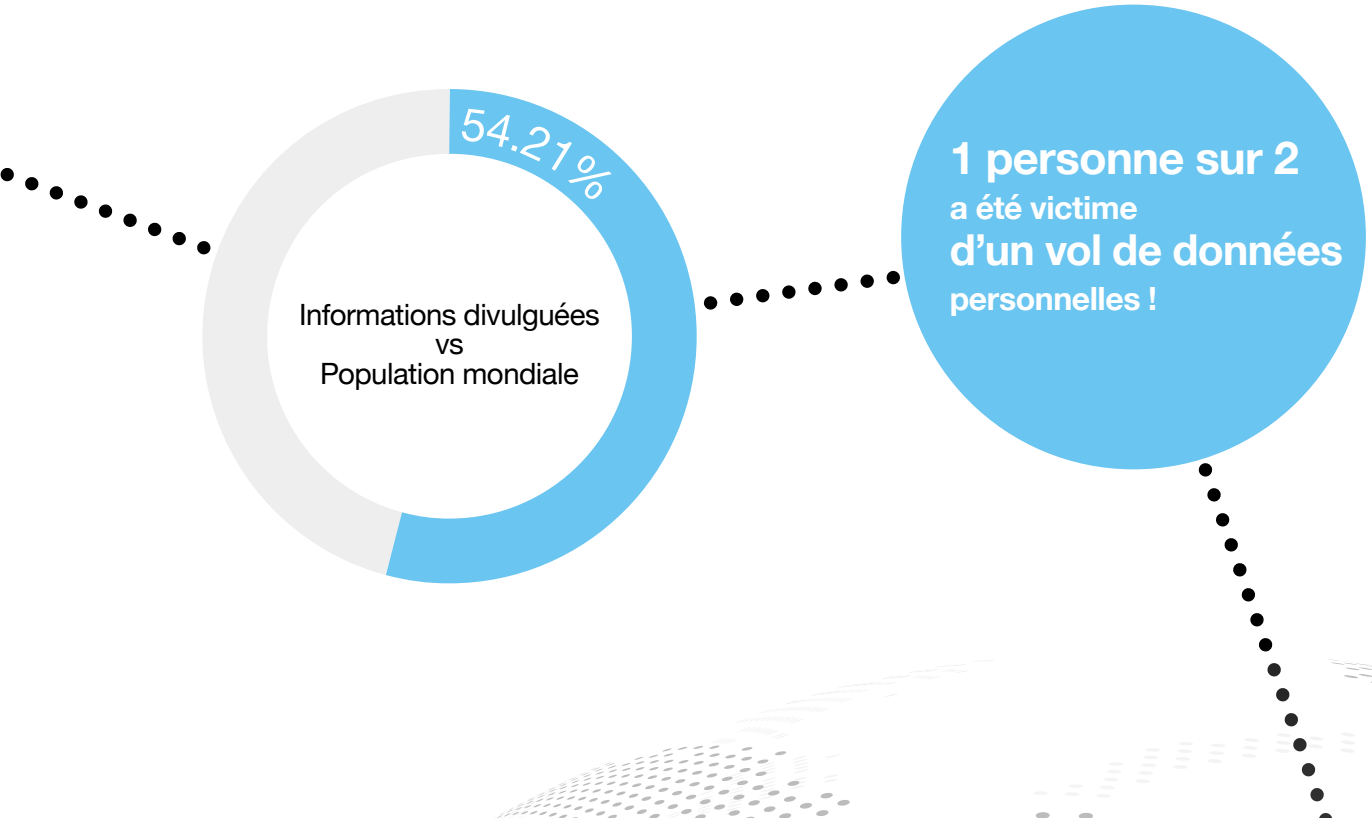
Un triste volume de 4 174 339 740 de données pillées a été découvert en 2019. En avril de cette même année, la population mondiale était estimée à 7,7 milliards d'individus [4.29], ce qui revient à dire qu'une personne sur deux peut donc avoir été victime d'un vol d'informations personnelles. Ce chiffre est alarmant, et pas uniquement pour les fans de protection des données et de RGPD. D'autant qu'il ne s'agit là que des fuites dont nous avons eu connaissance.

Les entreprises assiégées

Selon le Midyear Data Breach Report [4.30], 3 813 fuites de données ont été signalées au premier semestre 2019, soit plus de 54 % par rapport à la même période en 2018. Au cours de la même période, huit infractions ont été identifiées comme exposant plus de 100 millions de données.

Avec 84,6 %, la vaste majorité de ces cas provient des entreprises. Il n'est pas surprenant que les criminels cherchent en premier lieu des adresses mail (trouvées dans 70,5 % des cas) et des mots de passe (64,2 %) [4.30]. Évidemment, les identifiants peuvent être détournés de diverses manières.

Les méthodes employées par les attaquants pour obtenir de grandes quantités de données ne sont pas nouvelles : des tactiques telles que le phishing et le skimming (piratage des terminaux de paiement ou des distributeurs de billets) sont toujours populaires.



Il n'y a pas de petit profit

Les médias ont, à juste titre, saisi cette occasion pour faire sensation avec les fuites d'informations dont ont été victimes les grandes organisations. Cette couverture épargne les petites et moyennes structures, mais elle peut aussi induire un faux sentiment de sécurité, en particulier pour les organisations de moindre envergure. Au regard des chiffres, cette idée est dangereusement trompeuse : plus de deux tiers des informations ont étés exposées en petite quantité de 1 000 données ou moins. Pour les criminels, peu importe la taille des entreprises : un sou est un sou.

Une fuite de données en agrège très vite une autre. Cet enrichissement crée de nouvelles opportunités pour les criminels, leur garantissant un modèle économique durable, ainsi que des données qualitatives et fiables pour ceux qui souhaitent les monétiser.

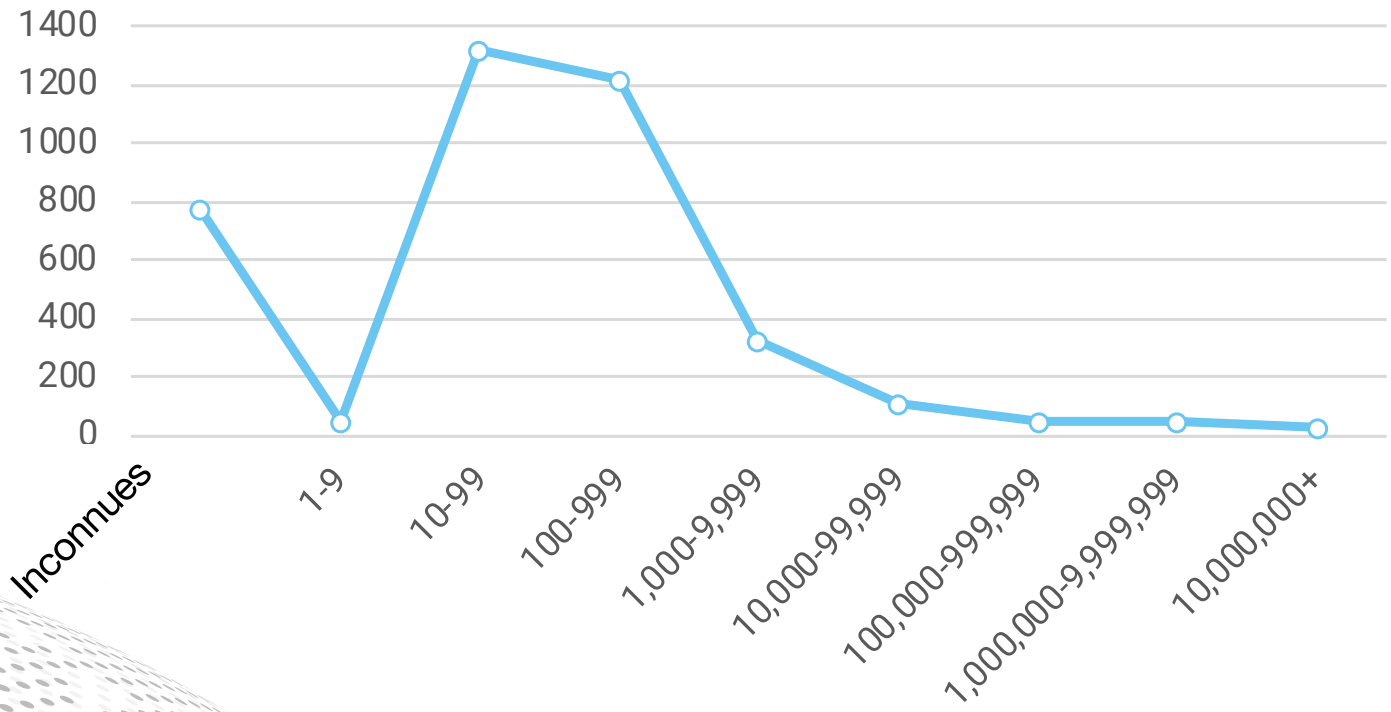
De là, les informations mises en vente proviennent souvent de milliers de petites entreprises ayant fait l'objet de fuites de données, souvent sans en avoir conscience.

Pourquoi grimper aux arbres…

… quand on peut ramasser les fruits par terre ?

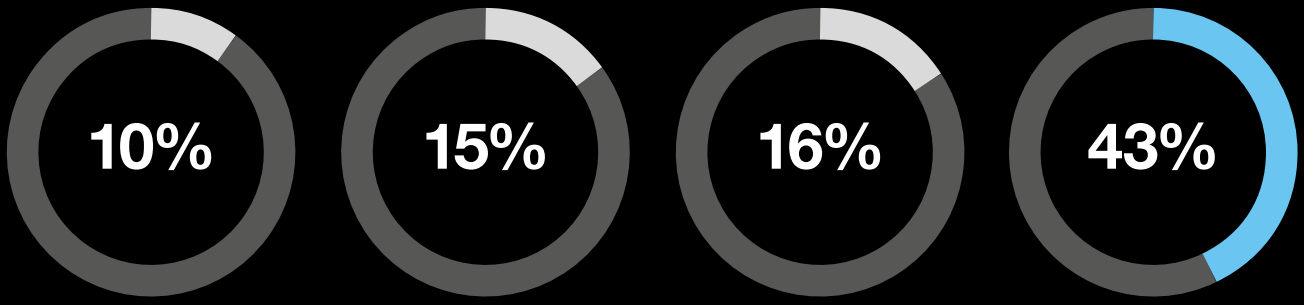
Certes, les fruits tombés sont généralement jugés non-comestibles, mais les données n'ont pas de bactérie. La majorité des incidents sont liés à du piratage (82 %), mais pas le plus gros volume de données fuitées. Les nombres sont dans ce cas trompeurs. En leur portant davantage attention, nous observons que dans 79 % des cas la violation d'informations confidentielles a requis peu d'efforts, voire aucun effort, aux attaquants et sont liés à des bases de données mal configurées, des services Web, applications et stockages Cloud mal sécurisés accessibles en ligne). Les menaces internes, malveillantes comme accidentelles, sont une autre source majeure de collecte d'informations.

Volume de données exposées par rapport au nombre de fuite de données



Victimes de fuites de données

Source : Verizon data breach report 2019



Fuites de données notables en 2019

Fuite	Date	Nombre de données	Methode	Source
Collection 1	Jan 17	773,000,000	Piratage	[4.1]
Universiti Teknologi MARA	Jan 25	1,164,540	Piratage	[4.2]
Ministry of Health (Singapore)	Jan 28	14,200	Défaut de sécurité / Malveillance interne	[4.3]
GnosticPlayers, Round 1	Feb 11	617,000,000	Piratage	[4.4]
GnosticPlayers, Round 2	Feb 15	127,000,000	Piratage	[4.5]
GnosticPlayers, Round 3	Feb 18	92,000,000	Piratage	[4.6]
Health Sciences Authority (Singapore)	Mar 15	808,000	Défaut de sécurité / Malveillance interne	[4.7]
GnosticPlayers, Round 4	Mar 17	26,000,000	Piratage	[4.8]
Facebook	Apr 04	540,000,000	Défaut de sécurité / Malveillance interne	[4.9]
Facebook	Apr 18	1,500,000	Exposition accidentelle	[4.10]
Justdial	Apr 18	100,000,000	API non protégée	[4.11]
Mystery Database	Apr 30	80,000,000	Défaut de protection	[4.12]
Truecaller	May 22	299,055,000	Inconnu	[4.13]
First American Corporation	May 24	885,000,000	Défaut de sécurité / Malveillance interne	[4.14]
Canva	May 28	140,000,000	Piratage	[4.15]
Westpac	Jun 03	98,000	Piratage	[4.16]
Australian National University	Jun 04	200,000	Piratage	[4.17]
Quest Diagnostics	Jun 05	11,900,000	Défaut de sécurité / Malveillance interne	[4.18]
Desjardins	Jun 20	2,900,000	iMalveillance interne	[4.19]
2019 Bulgarian revenue agency hack	Jul 16	5,000,000	Piratage	[4.20]
Capital One	Jul 29	106,000,000	Piratage	[4.21]
StockX	Aug 03	6,800,000	Piratage	[4.22]
Health Care Image Leak	Sep 17	16,000,000	Défaut de protection	[4.23]
Novaestrat	Sep 18	20,000,000	Défaut de protection	[4.24]
Mobile TeleSystems (MTS)	Sep 20	100,000,000	Mauvaise configuration / Défaut de sécurité	[4.25]
Amazon Japan G.K.	Sep 26	unknown	Publication accidentelle	[4.26]
DoorDash	Sep 26	4,900,000	Piratage	[4.27]

Total: **4,174,339,740**

Conclusion

En dépit de nouvelles réglementations, de technologies de pointe et d'une plus ample compréhension des cyber risques, 2019 a connu un nombre incroyable de fuites de données très médiatisées. Au vu de la quantité exceptionnelle d'informations mise à disposition sur les places de marché criminelles, la protection des données est une problématique phare à laquelle la majorité des organisations sont confrontées.

Environ 80 % des fuites de données sont involontaires ou accidentelles. Les entreprises doivent donc porter une grande attention au traitement des données pour en identifier les causes principales. Former et sensibiliser les employés à ces problèmes, suivre et analyser en interne les menaces sont des mesures de prévention primordiales.

Les cas hautement médiatisés – parmi lesquels Marriott, British Airlines et Facebook – changent les repères pour ces organisations. Non seulement leur réputation est atteinte mais les autorités réglementaires réagissent fermement et infligent des amendes faramineuses. Ces évènements se répercutent aussi sur beaucoup d'individus pour qui les dommages sont réels. Ils sont contraints de regagner le contrôle sur leurs identités numériques.

Le confinement lié à la crise du COVID-19 a poussé nombre d'industries vers le télétravail. D'où l'importance de sécuriser les transferts de données, le stockage Cloud et les accès hors des périmètres habituels. Il était urgent d'agir, mais il est vital que les entreprises adaptent leur sécurité à cette nouvelle situation dans les délais les plus brefs et éviter ainsi d'étendre la surface d'attaque. C'est l'occasion de repenser la protection des données dans son ensemble.

Les organisations encourent des risques considérables en s'appuyant sur des plateformes et places de marché en ligne. Les meilleurs tireront avantageusement parti de la situation et demeureront résilients en cas de mer agitée. Ceux qui échoueront à identifier des garde-fous pertinents subiront rapidement d'importantes et fréquentes perturbations.

Charl van der Walt
Head of Security Research
Orange Cyberdefense

Revue technologique

Les VPN sont-ils sûrs ?

Les VPN (Virtual Private Networks) sont vus comme un moyen sûr de communication et de transfert des données, en particulier par les entreprises. Nous nous sommes penchés sur cette question, à la recherche de possibles faiblesses.

Les entreprises équipent leurs salariés d'équipements mobiles, dont ordinateurs portables et smartphones, de façon à ce qu'ils puissent accomplir leurs tâches au quotidien. La « main d'œuvre » devient ainsi bien plus mobile, mais elle est aussi affublée d'une charge implicite : s'assurer de toujours être en ligne. La sécurité est gérée par leur système d'exploitation et les solutions de support, comme les VPN. La technologie du VPN existe depuis au moins 1996. Mais elle a récemment atteint un pic d'exploitation : des millions d'employés dans le monde entier ayant dû accéder à distance à des réseaux d'entreprise du fait du confinement.

Les VPN, en particulier du niveau de ceux des entreprises, peuvent s'avérer complexes et leurs diverses options de configuration peuvent nécessiter beaucoup de méthode. Fournir un support à distance aux utilisateurs rencontrant des difficultés techniques engendre des coûts lorsqu'il s'agit de régler des problèmes causés par des solutions mal configurées.

Cette section présente les résultats de nos recherches sur l'efficacité des VPN du marché au regard des usages mobiles contemporains, des technologies habituellement rencontrées sur les postes de travail et des modèles de menaces.

Ces VPN fonctionnent-ils effectivement ?

Ce qu'un VPN est censé faire

Un VPN doit garantir confidentialité et intégrité des connexions réseau, prémunir les utilisateurs contre d'éventuels vols et altérations des données. Dans l'entreprise, l'authentification et le contrôle d'accès sont ajoutés pour s'assurer que seuls les utilisateurs légitimes accèdent aux ressources. En ce sens, les VPN d'entreprise modernes remplissent au moins deux cas d'usage distincts.

Les mots « privé virtuel » et « réseau » traduisent littéralement leur fonction. « Virtuel » renvoie au fait que sa construction se comporte comme un équivalent physique. Le terme « privé » revendique, quant à lui, la confidentialité et la fiabilité.

Nous pouvons donc déduire qu'un VPN est une extension logique d'un réseau privé vers un autre lieu, faisant en sorte que l'expérience d'utilisation à distance d'outils informatiques réside sur le segment réseau local. Cette extension réseau peut s'étendre à l'ensemble de l'Internet public.

Un VPN n'est pas simple

En vérité, les solutions VPN sont rarement déployées simplement considérant le trafic transitant depuis le VPN vers l'entreprise. Par exemple, la plupart des déploiements permettent qu'une certaine partie du trafic soit dirigée vers le VPN tandis qu'une autre partie conserve un accès direct à Internet. Cette solution est appelée split tunneling (ou tunneling fractionné) et prévaut de plus en plus à mesure que la vitesse d'Internet augmente.

Un autre exemple complexe est celui des salariés à distance se connectant à des hotspots Internet gratuits généralement proposés par les cafés, aéroports, hôtels, etc. Ces hotspots sont des points d'accès Wi-Fi offrant de la bande passante gratuite. Aujourd'hui, la plupart d'entre eux sont des portails captifs nécessitant un mot de passe, un code ou une forme quelconque d'accord avant d'autoriser les ordinateurs connectés à accéder à Internet.

La mise en œuvre d'un VPN robuste ne devrait pas permettre aux utilisateurs d'interagir avec des ressources réseau qui contournent le tunnel VPN. Cependant, dans la plupart des déploiements modernes, ceci conduit à une impasse : l'utilisateur doit d'abord se connecter au hotspot Wi-Fi, puis envoyer la requête au portail, avant que le VPN puisse se connecter au serveur et établir le tunnel.

Que se passe-t-il chronologiquement entre le moment de la connexion au hotspot Wi-Fi et l'activation du VPN, quand l'utilisateur est face au portail captif ?

À ce state, l'utilisateur est-il vulnérable ? Le hotspot Wi-Fi isole les invités de façon sécurisée et le pare-feu local sur le portable protège l'utilisateur contre d'éventuels attaquants. Ce principe fonctionne-t-il quand le hotspot est entièrement contrôlé par l'attaquant ? Regardons de plus près

VPN et sécurité

Dans le cadre de cette étude, il est important de comprendre les menaces qui guettent un utilisateur type. Menaces susceptibles d'affecter la confidentialité, l'intégrité, le contrôle d'accès et qui sont censées être prévenues par le VPN. Nous nous sommes concentrés sur la liste suivante :

Man in the middle ou usurpation d'identité

L'attaquant trouve un moyen de donner de fausses réponses aux requêtes DNS légitimes du client. Il contrôle ainsi le point d'atterrissage de la connexion. C'est ici la première étape du déploiement d'une attaque qui va suivre comme celle des faux sites visant à collecter des identifiants ou d'attaques « Responder » (voir plus bas).

Récupération d'identifiants via de faux sites

Une fois que les attaquants contrôlent le DNS et le routage (comme ils le feraient avec un point d'accès malveillant), ils peuvent afficher une fausse page d'identification pour accéder à des ressources telles qu'O365 afin de collecter les identifiants de connexion.

Extraction des hashs de mots de passe Windows

Les attaques dites « Responder » consistent à piéger les systèmes Windows pour qu'ils se connectent à un faux service Windows qui demande à son tour une authentification puis capture les hashs des mots de passe envoyés. Ce mécanisme permet ensuite des attaques contre les ressources de l'Active Directory comme la connexion à la passerelle VPN qui utilise généralement l'Active Directory pour les processus d'authentification.

Utilisation du navigateur comme proxy

En contrôlant le DNS et le routage (comme ils le feraient avec un point d'accès malveillant), les attaquants peuvent injecter du code JavaScript dans d'autres sites légitimes pour exercer un contrôle distant sur l'ordinateur de la victime, s'en servant, par exemple, comme pivot pour accéder au réseau de l'entreprise.

Utilisation d'IPv6 pour interagir avec l'hôte

La plupart des technologies VPN d'entreprise sont conçues pour protéger du trafic IPv4, mais plusieurs endpoints supportent maintenant aussi des paquets IPv6 qui peuvent être utilisés pour communiquer sur le LAN (réseau local) et sur Internet. Si le VPN ne gère pas IPv6, l'attaquant dispose d'un canal ouvert pour communiquer avec l'ordinateur.

Toutes ces attaques sont réalisables lorsqu'un ordinateur professionnel se connecte à un point d'accès Wi-Fi public contrôlé par un pirate. Les entreprises dépendent donc largement des VPN pour protéger leurs postes nomades. Etant donné l'état d'ambiguïté dans laquelle les portails captifs placent les endpoints, nous voulons savoir jusqu'à quel point les VPN assurent la protection que nous attendons.

JUIL

Double peine : des amendes infligées à des établissements après des fuites de données

British Airways a été contrainte de verser 183 millions de livres au titre de la RGPD pour la fuite de données qu'elle a subi en 2018 [t32]. Equifax doit payer 700 millions de dollars pour la fuite de 2017 [t33] et Marriott reçoit une amende de 123 millions de dollars après l'affaire Starwood.[t34]

Présentation des portails captifs

Les portails captifs sont généralement utilisés par des fournisseurs d'accès Wi-Fi comme les hôtels, les aéroports et les cafés. Un équipement nécessitant un accès à Internet pourra se connecter au réseau Wi-Fi, mais n'aura habituellement pas accès à Internet tant que les exigences de ce portail ne seront pas remplies (paiement, données personnelles ou consentement).

Une fois connecté à un point d'accès Wi-Fi, le système d'exploitation testera l'accès du périphérique à Internet avec une requête HTTP vers une URL de son choix. Si la réponse HTTP concorde avec ses attentes, le système d'exploitation considère qu'il est connecté à Internet.

Toutefois, si le portail captif constitue le point d'atterrissage, le système d'exploitation invitera l'utilisateur, le plus souvent depuis une interface de navigateur web, en affichant un message du portail sous la forme d'un formulaire. Dans les cas d'Android et d'iOS, l'utilisateur est informé qu'un portail captif est présent ; il lui est demandé s'il souhaite interagir avec celui-ci.

Android et iOS intègrent des navigateurs web spéciaux, des mini-navigateurs pour portails captifs. Ils se distinguent des applications de navigations Web à part entière. MacOS présente un concept similaire sous forme d'un assistant de réseau captif.

Windows et Linux quant à eux s'appuient sur les navigateurs par défaut pour interagir avec le portail captif. Windows peut démarrer le navigateur par défaut automatiquement lorsqu'il détecte le portail captif. Linux reste silencieux et se base sur l'utilisateur pour lancer un navigateur (ex : Firefox) capable de détecter un portail captif.

Dans tous les cas, l'utilisation d'un portail captif sur un réseau Wi-Fi gratuit crée un créneau durant lequel le périphérique est connecté au point d'accès Wi-Fi et voit ses configurations réseau contrôlées par le point d'accès, mais ne peut se connecter à Internet et, par conséquent, ne peut établir le VPN.

Présentation du split tunnelling

Autre exemple de configuration VPN courant – mais pas obligatoire – utilisée par les entreprises : le split tunneling. Dans ce cas, une fois le VPN configuré et connecté, il achemine des requêtes réseau spécifiques via le tunnel VPN, alors qu'une autre partie du trafic suit les règles de routages réseau par défaut. Cette configuration fait en sorte que seul le trafic destiné au réseau d'entreprise est chiffré et assujetti à des contrôles d'accès. Le trafic réseau normal ou lié à Internet passe directement en clair. L'objectif est évident : permettre l'accès aux ressources de l'entreprise et améliorer les performances lors d'accès à des sites et services publics sur Internet.

Les implications de ce choix de configuration pourraient, cependant, ne pas être très claires parce que si un ordinateur est « capturé » par un réseau Wi-Fi malveillant, il pourrait être forcé à se connecter ou envoyer du trafic via des routes non chiffrées et non protégées.

Au cours de notre étude du déploiement par défaut d deux grands produits VPN d'entreprise, une fois le VPN établi, opérait le split tunneling. Il s'agit du modèle que nous avons retenu pour nos tests et que nous décrivons ci-dessous.

Test A : Mode standard

Comme prévu, avec ce mode les machines Windows sont vulnérables à tous les vecteurs de menace décrits plus haut, et ce pour les deux produits VPN d'entreprise que nous avons testés. Plus préoccupant encore, utilisés en mode split tunneling, ces produits demeurent vulnérables aux attaques même une fois le VPN complètement déployé. (✓ = protégé, ✗ = sans protection)

Attaque	Capturé		En ligne	
	VPN1	VPN2	VPN1	VPN2
DNS « Man in the middle » ou usurpation de sites	✗	✗	✗	✗
Récupération d'identifiants via de faux sites	✗	✗	✓	✓
Capture des hashs Windows via Responder	✗	✗	✗	✗
Utilisation du navigateur comme proxy	✗	✗	✓	✓
Utilisation d'IPv6 pour interagir avec l'hôte	✗	✗	✗	✗

Ces résultats représentent une version simplifiée de nos tests. Il peut y avoir des cas, tant pour les tests réussis que pour les échecs, où les résultats diffèrent au gré d'autres circonstances qui dépassent le cadre de ce test.

Améliorations apportées aux VPN – Mode Lockdown

Les VPN modernes répondent au défi des portails captifs, tels que décrits plus haut, en introduisant un ensemble de fonctionnalités connues sous le mode « lockdown » afin de garantir une meilleure protection dans certains environnements non sécurisés.

Le mode Lockdown peut être considéré comme un ensemble de fonctionnalités VPN conçues pour limiter la quantité de trafic quittant le poste alors qu'il se trouve sur le réseau local sans fil (WLAN) qui gère le portail captif.

Les spécificités de ces fonctionnalités varient d'un produit à l'autre, mais se résument en général à :

- protéger le navigateur qui se connecte au portail et
- limiter la quantité de trafic autorisée à quitter l'ordinateur.

Nous avons donc testé les deux produits VPN qui proposent ces fonctionnalités en activant toutes leurs capacités. Nous tâchions de déterminer l'efficacité de leur protection.

Test B : Mode Lockdown

En résumé, notre test montre que même en mode Lockdown les capacités fournies par les VPN pour réduire les risques induits par les portails captifs sont peu efficaces contre l menaces actuelles. (✓ = protége, ✗ = sans protection)

Attaque	Capturé		En ligne	
	VPN1	VPN2	VPN1	VPN2
DNS « Man in the middle » ou usurpation de sites	✗	✗	✗	✗
Récupération d'identifiants via de faux sites	✗	✗	✓	✓
Capture des hashs Windows via Responder	✗	✓	✗	✗
Utilisation du navigateur comme proxy	✓	✗	✓	✓
Utilisation d'IPv6 pour interagir avec l'hôte	✗	✗	✗	✗

Ces résultats représentent une version simplifiée de nos tests. Il peut y avoir des cas, tant pour les tests réussis que pour les échecs, où les résultats diffèrent au gré d'autres circonstances qui dépassent le cadre de ce test.

Les résultats en résumé

En résumé, nos tests montrent que notre intuition première quant à l'échec des VPN à protéger les machines au sein des portails captifs est justifiée. Cela ne signifie pas que ces VPN ne fonctionnent pas, ni qu'ils présentent des bugs, mais plutôt que les portails captifs sont un cas d'usage pour lequel les VPN n'ont simplement pas été conçus à l'origine.

Dans l'hypothèse où tout Wi-Fi gratuit devrait raisonnablement être considérés comme malveillant et au vu des vecteurs et outils d'attaque contemporains, cette incapacité à gérer un cas d'usage si important représente une limitation considérable. Elle nous force à dépendre de mécanismes secondaires comme le certificat SSL/TLS, les firewalls, et la protection du poste pour défendre le terminal mobile.

Nous étions d'autant plus déçus de découvrir qu'une fois pleinement établi, un VPN configuré négligemment ne réussit guère mieux à limiter ces menaces réelles.

En réponse aux défis liés aux portails captifs, les VPN d'entreprises ont mis en place un ensemble de fonctionnalités de verrouillage pour limiter les problèmes. Ces fonctionnalités traitent, en effet, certaines de ces problématiques, mais malheureusement ne permettent pas de mettre un terme à l'ensemble des menaces que nous avons testées.

Alors que le comportement de certaines de ces fonctionnalités nous a parfois laissés perplexes, nous devons préciser qu'il s'agit d'une des fonctions fondamentales dans la manière dont les portails captifs fonctionnent, plutôt qu'un problème lié aux produits eux-mêmes

Les menaces prises en compte pendant nos tests ne sont, certes, pas catastrophiques. Plusieurs facteurs doivent coïncider pour que les faiblesses soient exploitées et plusieurs facteurs externes peuvent empêcher ces attaques d'aboutir.

Néanmoins, nous maintenons qu'il existe un ensemble réaliste de conditions sous lesquelles les VPN modernes sont fondamentalement incapables de remplir leur objectif de sécurisation : garantir la confidentialité, l'intégrité et la fiabilité des contrôles d'accès.

Notre expérience nous aura montré que les conditions requises pour exploiter malicieusement cette faiblesse des VPN peuvent être remplies dans des circonstances réelles et sont probablement bien plus courantes que nous ne le pensons.

Nous maintenons que la menace est suffisamment sérieuse et réelle pour justifier une réponse dédiée de la part des équipes informatiques des entreprises.

Recommandations

Nous estimons que les vulnérabilités et menaces décrites par ces tests sont suffisamment graves pour justifier une réponse urgente, sans que cette réponse soit pour autant particulièrement coûteuse ou disruptive.

Nos recommandations techniques peuvent être résumées comme suit :

Changements de configuration :

- Éviter la configuration VPN en split tunneling. Faites passer les employés par le réseau de l'entreprise où ils peuvent être filtrés, « surveillés » ou se voir appliquer d'autres protections offertes par le réseau interne.
- Configurer votre VPN pour utiliser des domaines DNS personnalisés dont vous avez le contrôle.. Les produits VPN d'entreprise que nous avons testés proposaient tous deux cette fonctionnalité. Nous supposons que d'autres produits sérieux en font de même.
- Comprendre et implémenter toutes les fonctionnalités du mode lockdown offertes par votre VPN. Il ne s'agira pas d'un changement simple : il nécessitera des tests et un déploiement minutieux.

Autres contrôles techniques :

- S'assurer que tous les systèmes Windows internes auxquels vos utilisateurs accèdent ont des noms d'hôtes qualifiés. Par exemple, toujours utiliser « ocd-src-server.ocd.local », et pas simplement « ocd-src-server ».
- Mettre en œuvre les pare-feux des hôtes locaux et des programmes de détection et de protection avancés pour les postes de travail. Utilisés convenablement, ils constituent des défenses sérieuses contre les attaques décrites plus haut.

Raisonnement stratégique :

Si c'est gratuit, c'est que vous êtes le produit : une expression utilisée fréquemment de nos jours

Nous pensons que cela vaut également pour les services Wi-Fi dits gratuits. Le coût de la confidentialité et de la sécurité de ces accès Internet pour les utilisateurs nomades est trop élevé pour les entreprises qui doivent prendre au sérieux ces deux composantes. Nous conseillons donc aux entreprises d'équiper leurs collaborateurs nomades de technologies de données mobiles et de bande passante suffisante pour se connecter de manière relativement fiable, visible et transparente à un fournisseur de réseau mobile, plutôt que de les exposer à un assortiment anarchique de fournisseurs d'accès gratuits. Nous ne pouvons garantir leur intégrité et leurs motivations sont inconnues.

Considérer le Zero Trust

Le Zero Trust est un concept stratégique émergent, au sein duquel tous les réseaux sont considérés comme égaux et auxquels aucune confiance ne leur est accordée. Ce modèle brise la frontière entre espace interne et espace externe, la sécurité doit donc être garantie au niveau des endpoints et du serveur sans nécessiter un VPN. Le Zero Trust est une nouvelle façon de penser la sécurité conçue pour l'Internet moderne et adoptée par des groupes de pointe comme Google pour leur propre stratégie de sécurité. Nous recommandons à nos clients de s'engager sérieusement sur la voie du Zero Trust et d'opter pour les nouvelles technologies et approches qu'elle implique. Ils pourraient ainsi garantir que le niveau de sécurité reste adéquat quand il faudra affronter les changements de technologies et les menaces émergents des cinq à dix années à venir.

Conclusion

Des technologies de cybersécurité voient le jour en réponse à un ensemble spécifique de menaces.

Le besoin client et le paysage technologique évoluent, les produits de sécurité se doivent d'en faire de même. Garantir un alignement entre menaces émergentes et technologies exploitées pour les limiter demande une vigilance de tous les instants.

Le confinement lié au COVID-19 a prouvé combien nous dépendons des technologies de communication sécurisées. Les VPN ont ainsi été au centre de l'attention des attaquants autant que des responsables sécurité.

Notre enquête sur l'efficacité des VPN prenant en compte les configurations Internet actuelles soulève d'importantes préoccupations. Le problème est toutefois plus vaste si l'on considère les efforts constants requis pour appréhender la menace, la difficulté à comprendre comment nos outils de sécurité concordent avec celle-ci et, enfin, le besoin de garantir une utilisation optimale de ces outils. Aucune technologie, prise individuellement, ne saurait faire disparaître un problème.

Ceci relève de notre responsabilité et les choses sont loin d'être plus simples aujourd'hui.

Le ransomware eCh0raix/QNAPCrypt vise les stockages réseau

Le malware vise les serveurs NAS produits par QNAP Systems, soit en attaquant par force brute des identifiants SSH faibles, soit en exploitant des vulnérabilités connues. [t35]

Le Kazakhstan pourrait lancer des attaques « Man in the Middle » contre tous les citoyens

Les FAI Kazakhs sont contraints d'exiger de leurs clients qu'ils installent un certificat racine délivré par le gouvernement appelé « national security certificate ». Ce certificat permet aux autorités d'intercepter et de censurer toute connexion HTTPS et TLS chiffrée. [t36]

Un ransomware cause une panne de courant à Johannesburg

La plus grande ville sud-africaine, comptant plus de 5 millions d'habitants, a subi des pannes d'électricité durant plusieurs jours. Son principal fournisseur, City Power, avait été frappé par une attaque par ransomware. [t37]

AOÛT

La Banque Centrale Européenne ferme le portail « BIRD » après un piratage

Des tiers non autorisés sont parvenus à s'introduire sur leur site Bank'Integrated Reporting Dictionary (BIRD). Ce site était hébergé par un prestataire externe. Cet incident a poussé la BCE à fermer ce site. [t39]

POC : des ransomware se propagent aux appareils photo reflex numériques

Les chercheurs de Check Point ont découvert des vulnérabilités critiques dans le logiciel des appareils photo Canon. La preuve en a été faite quand ils ont démontré qu'elles pouvaient facilement être exploitées infecter l'appareil avec un ransomware, au moyen d'une clé USB ou via le Wi-Fi. [t38]

La gendarmerie française a neutralisé à distance un réseau de 850 000 PC infectés par le malware RETADUP

La Gendarmerie nationale française a mis un terme au botnet RETADUP en utilisant une faille dans les serveurs de commande et de contrôle du malware. Le Centre de lutte contre la criminalité numérique (C3N) a mis fin au contrôle du serveur et forcé le malware à s'autodétruire. [t40]

Un service de protection contre les ransomware frappé par un ransomware

DDS Safe, solution Cloud de sauvegarde de données populaire auprès des cabinets dentaires américains (pour protéger les dossiers médicaux d'éventuelles cyberattaques) a été frappé par le ransomware Sodinokibi. [t41]

Michael Haugland
Threat Research Analyst
Orange Cyberdefense

Revue technologique

PKI et confiance numérique

La PKI (ou ICP en français, littéralement Infrastructure à Clés Publiques) à laquelle nous recourrons de nos jours facilite nombre de nos activités quotidiennes sécurisées en ligne : e-commerce, les services bancaires, messagerie instantanée et les emails confidentiels. La PKI peut s'utiliser de différentes manières et procurer les quatre ingrédients requis pour insuffler la confiance : confidentialité, authentification, intégrité et non-répudiation. Nous prenons cela pour acquis et nous le remettons rarement en question.

Dans une ignorance béate, nous acceptons que cela fonctionne, tout simplement. Mais est-ce bien le cas ?

Nous avons analysé les éléments constitutifs de la PKI pour comprendre à qui nous faisons confiance lorsque nous utilisons des services chiffrés de transmission de données comme, par exemple, le protocole HTTPS.

Ce que nous avons découvert est alarmant : la confiance numérique est non seulement distribuée de manière très inégale géographiquement (elle est surtout basée aux États-Unis), mais vous faites aussi confiance à des pays qui devraient plutôt vous préoccuper.

Il semblerait que pour sécuriser nos communications nous plaçons notre confiance dans des organisations privées, non surveillées et non transparentes, mais presque personne n'y pense.

Nous croyons aux certificats

L'usage du chiffrement précède les Romains et a été rendu célèbre par César. Le concept d'origine est simple et n'a pas changé depuis des millénaires : utiliser une clé secrète pour convertir un message en texte chiffré, le rendant inutile à tout individu ne disposant pas de la clé secrète pour le déchiffrer.

Avec la PKI, voici ce que nous pouvons aisément parvenir à faire pour le trafic HTTPS :

- Connexion à un serveur Web qui s'identifie avec un certificat numérique.
- Le navigateur vérifie que le certificat numérique est valide (domaine, date et signature par une autorité de certification (AC))
- Si validé, des clés cryptographiques sont échangées et la communication qui en résulte est chiffrée.

Permettre aux parties de s'identifier au moyen de certificats numériques est la base d'une communication fiable, garantissant la confidentialité par le biais du chiffrement, l'intégrité des données et un socle suffisant pour la non-répudiation.

En faisant confiance aux certificats numériques, nous nous appuyons sur des autorités de certification indépendantes qui les distribuent. Nous prétendons qu'elles suivent et remplissent certains principes et critères pour devenir des AC. Nous (utilisateurs finaux) ne jouons aucun rôle dans la sélection de ces autorités et nous fions au souscripteur du certificat numérique (son propriétaire) pour sélectionner celle qui convient lorsque nous utilisons leurs produits et services pour notre communication. Les appareils et logiciels que nous choisissons embarquent des AC prêts à établir la confiance en notre nom et à afficher le fameux cadenas indiquant que les communications sont fiables et sécurisées.

Alors, implicitement, en qui faisons-nous confiance ? Qu'est-ce que cela sous-entend pour les communications professionnelles chiffrées ?

Appliquer la confiance : les implications

Une PKI se définit comme un ensemble de rôles, politiques et procédures requis pour gérer (créer, distribuer, stocker et révoquer) des certificats numériques. Leur mise en œuvre est généralement régie par un territoire ou une région, ce qui en brise leur principe même.

La confiance demande fiabilité, cohérence et transparence soit l'inverse des évolutions observées en matière d'implémentation de PKI. Ce conflit est un dilemme conceptuel plus qu'une faiblesse technique de la PKI, il est donc d'autant plus difficile à résoudre.

Les AC sont au cœur du problème. Les certificats sont comme des « cartes d'identité » d'Internet. Imaginez ce qu'il se passerait si les cartes d'identité n'étaient pas délivrées exclusivement par des organismes gouvernementaux de confiance, mais par un ensemble d'établissements privés non transparents, appliquant chacun leurs propres règles et agendas ?

Certains d'entre eux pourraient même ne plus exister en tant qu'entités légales, mais leurs « cartes d'identité » circuleraient toujours. Quel serait l'impact sur le niveau de confiance dans ces cartes ? Serait-il avisé de confier des informations critiques pour l'entreprise, à un messager présentant une telle carte ?

Pourtant c'est à peu près comme cela que fonctionne la PKI aujourd'hui.

Savoir à qui se fier

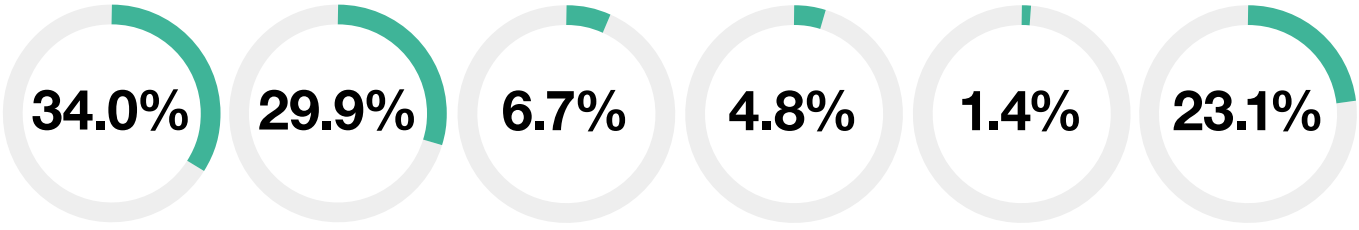
Notre méthodologie

Nous nous sommes servis du classement The Alexa Top Sites Service, un service permettant d'accéder à des listes de sites Web classés par importance de trafic depuis Amazon Alexa. Cette liste fournit une représentation vraisemblable de l'écosystème Web dans son ensemble.

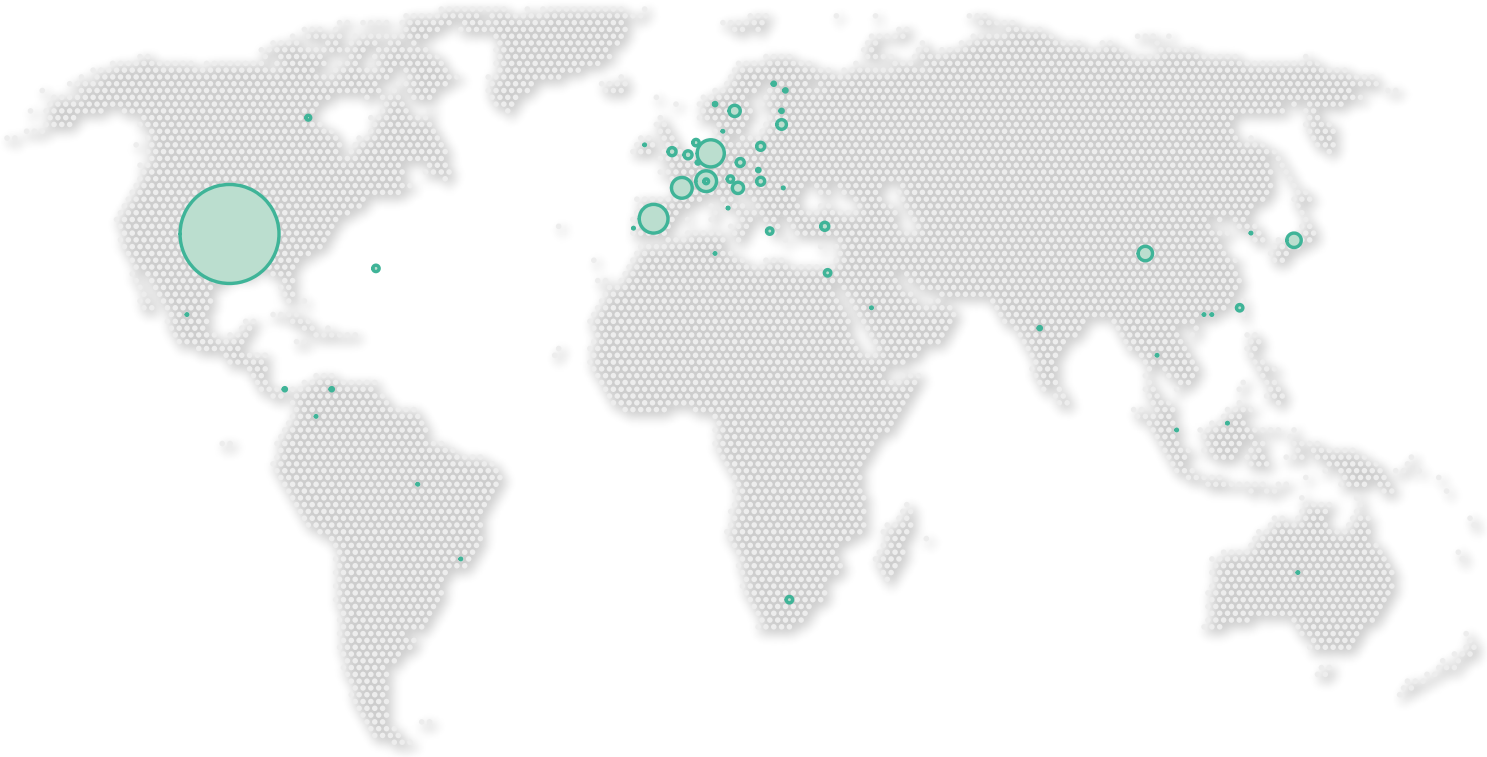
Nous nous sommes connectés au service et avons téléchargé toute la chaîne de certificats pour chaque site de cette liste (environ 1 million) en utilisant un outil propriétaire.

Usage des certificats

Pourcentage des certificats racines utilisés dans la liste



AddTrust External AddTrust AB	**DST Root CA X3** Digital Signature Trust CO	**Go Daddy Secure Certificate Authority - G2** Go Daddy Group Inc.	**DigiCert Global Root CA** Digi Cert Inc.	**Auto-signé**	**Autres (<5%)**



Quelle autorité de certification inspire le plus confiance ?

Définir quelle autorité de certification est la plus fiable dépend de plusieurs facteurs et, principalement, de votre géolocalisation. Toutefois, notre dépendance à deux AC majeures, DST Root CA X3 et AddTrust External, montre qu'il s'agit de celles en qui nous avons le plus confiance. Leurs certificats sont utilisés par 64 % des sites de la liste.

Distribution géographique des Trust Stores (magasins de confiance contenant les certificats)

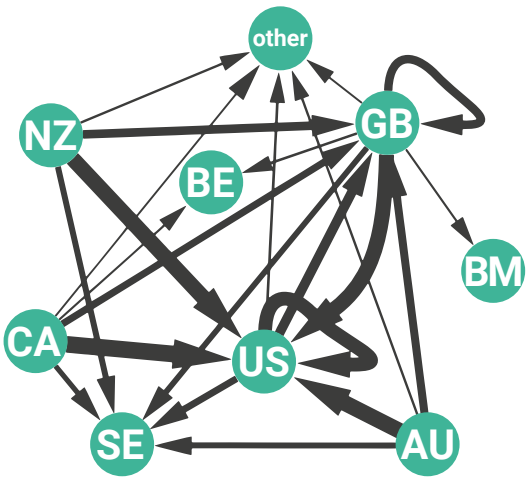
La carte ci-dessus a été établie en examinant le Trust Store pour chaque source et en regroupant les certificats selon le code pays (attribut C) qui le définit. Chaque pays est rattaché à une coordonnée et représenté sur la carte par un cercle de taille proportionnelle au nombre de certificats de chaque groupe.

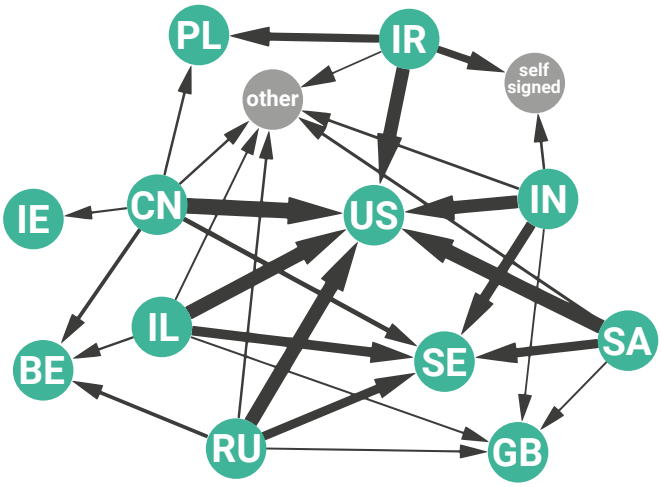
Répartition géographique : En qui se fient les « Five Eyes » ?

Les « Five Eyes » (Les cinq yeux) constituent une alliance anglophone de services de renseignements, comptant l'Australie, le Canada, la Nouvelle-Zélande, le Royaume-Uni et les États-Unis. La confiance au sein des « Five Eyes » est très tournée vers l'intérieur ou, plus précisément, vers une seule entité. Les États-Unis sont de loin l'entité considérée comme la plus digne de confiance. Sans surprise, les autres lieux qui pèsent dans la balance incluent la Grande-Bretagne et la Suède. Aussi étrange que cela puisse paraitre, les certificats racines à l'origine de ce groupement étaient initialement détenus par AddTrust, le mérite devrait donc revenir aux États-Unis.

En qui se fient les suspects ?

Cette répartition géographique nous donne une idée de la façon dont se « distribue la confiance » et présente une organisation similaire à celle des Five Eyes, plaçant les États-Unis au centre. Pourtant, certaines divergences sont notables. Les certificats auto-signés prévalent largement en Inde et en Iran. Par ailleurs, ces pays semblent plus enclins à placer leur confiance dans la Grande-Bretagne, la Pologne et la Belgique que les Five Eyes.





L'usage des Trust Stores

Quelles sont les autorités de certification utilisées par défaut ? nous avons analysé le pourcentage de chaque Trust Store de la liste. Dans le graphique suivant, en vert : les Trust Stores observés. Pour définir leur utilisation, nous comparons deux valeurs :

- Une liste d d'AC « approuvées » et d'AC racines disponibles dans le Trust Store de l'éditeur
- Les AC et AC racines identifiées comme « utilisées » après analyse de la liste.

Des AC « orphelines » persistant dans le système

Nous constatons qu'un grand nombre d'autorités de certification dites de confiance sont inutilisées. Chaque AC additionnelle est une source possible de risques, cette situation est donc quelque peu perturbante. Par exemple, 72% du Trust Store de Microsoft n'est pas utilisé.

Par opposition, Android est l'éditeur dont le Trust Store montre le plus haut pourcentage d'utilisation au regard de la liste : seuls 37 % sont inutilisés. Ce pourcentage est malgré tout élevé.

Qui est derrière les AC ?

Comme indiqué précédemment, les certificats racines qui identifient les autorités de certification sont détenus par des organisations privées. Il ne semble pas exister d'instance de régulation dictant quelles CA peuvent être considérées comme fiables.

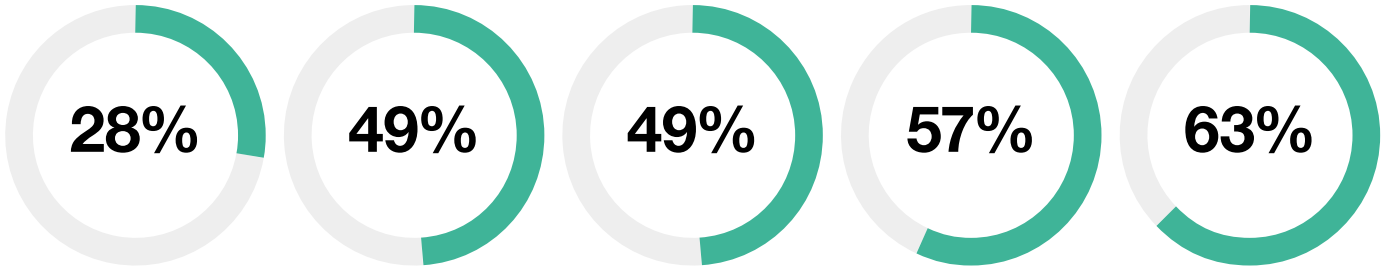
Alors que les certificats sont sujets à des normes (X.509 [6.1]), les moyens par lesquels une autorité de certification publique authentifie ses utilisateurs ne le sont pas. Ces moyens peuvent varier considérablement [6.2]. Les deux types de vérification les plus courants impliquent de simples validations de domaine, ne vérifiant que la propriété du domaine. Une validation étendue contribuerait à renforcer la confiance et enquêterait davantage sur la société proposant un site ou service en HTTPS, mais cela est rarement fait. Les seules instances proposant une certaine forme de contrôle sur ces pratiques et sur la fiabilité des AC sont les quatre grands navigateurs : Google/Chrome, Mozilla/Firefox, Apple/Safari et Microsoft/Edge.

Le manque de transparence est encore aggravé par le fait que, les AC peuvent déléguer (et le font) leur autorité d'émission de certificats à des AC subordonnées (qui à leur tour la délèguent à des filiales). Cette situation génère une chaîne de certification, qui peut être remontée jusqu'à sa racine. Néanmoins, cela ne nous dit pas si les certificats émis ont été suffisamment vérifiés et ne justifie pas la confiance que nous plaçons en eux. Comme il s'agit d'organisations privées, il serait intéressant de savoir qui en est propriétaire.

À ce titre, pour illustrer l'obscurité dans laquelle nous naviguons nous avons enquêté pour savoir à qui appartient AddTrust, l'autorité de certification racine derrière un tiers des certificats rencontrés dans la liste (voir l'appendice plus loin).

Utilisation des Trust Stores

Pourcentage de CA utilisées dans la liste et considérées comme fiables par défaut



Google, Mozilla et Apple bloquent un certificat racine du Kazakhstan

Les principaux navigateurs alertent désormais leurs utilisateurs quand un site tente de s'authentifier avec des certificats suspects émis par le gouvernement kazakh. [t42]

Conclusion

Il est clair que quelque chose pêche dans l'infrastructure à laquelle nous confions nos connexions.

D'abord, il est difficile de dire à qui, ou quoi, nous accordons notre confiance même en y regardant de plus près.

Vous vous fiez implicitement à des autorités de certification basées dans des pays desquels vous pourriez douter.

Les AC sont elles-mêmes des organisations qui peuvent, ou non, vérifier correctement à qui elles délivrent des certificats, mais il n'existe pas d'autorité de contrôle outre les principaux navigateurs. Et seule la position dominante de ces navigateurs sur le marché leur permet de cesser leur soutien à des autorités de certification douteuses. Est-ce suffisant, compte tenu du rôle central que jouent les certificats dans la sécurisation des communications ?

Le cœur du problème c'est que tout cela est très opaque pour les utilisateurs finaux et qu'ils ne peuvent savoir à qui ils font véritablement confiance.

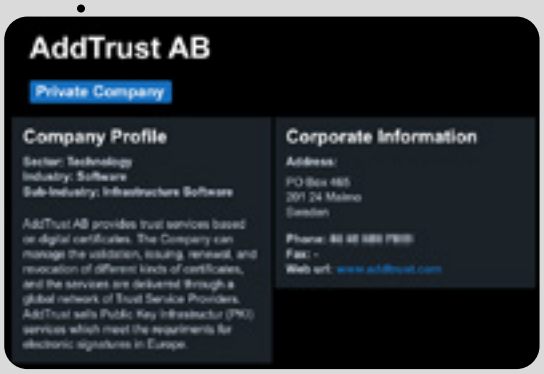
Par exemple, quand nous nous fions à AddTrust, l'une des autorités de certification les plus connues, nous faisons confiance à une autorité qui n'existe même plus en tant que société. Ses certificats racines ont été rachetés par Comodo, maintenant appelée Sectigo. Cet exemple illustre bien le manque de transparence de la PKI.

Il ne s'agit d'ailleurs sans doute que du sommet de l'iceberg.

Appendice : Qui est AddTrust ?

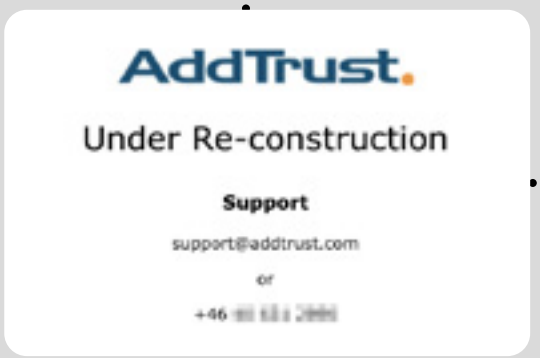
La société « AddTrust » représente plus de 30 % des certificats signés par une autorité de certification dans la liste décrite plus haut. Mais, peu d'informations sont directement disponibles pour garantir la crédibilité de cette entreprise numérique suédoise. Ce constat n'aide pas à améliorer la réputation déjà instable des AC. Nous tentons ici de décrire qui est exactement AddTrust.

Nous avons commencé par essayer d'évaluer la fiabilité de cette société, supposément basée à Malmö, en consultant Bloomberg [6.2]:

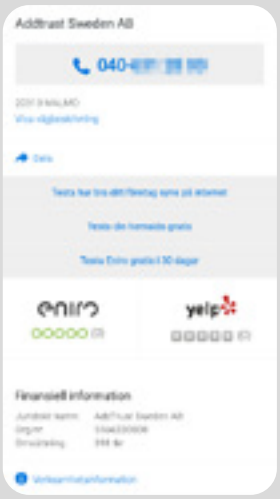


Nous trouvons un lien vers le site de la société, **www.addtrust.com**, mais il est impossible d'y accéder.

Nous accédons finalement au site via des archives Internet datant du 28 janvier 2011[6.3].
Nous y voyons un numéro de téléphone et une adresse mail support@addtrust.com



En entrant ce numéro dans www.allabolag.se (qui liste les informations publiques de toutes les sociétés en Suède), nous constatons qu'AddTrust est enregistréeau nom d'**Anders O.** Le numéro de téléphone est le même que celui trouvé sur et nous obtenons une nouvelle adresse.



En cherchant ensuite la société sur le site suédois **Eniro** nous trouvons d'autres informations. En plus d'un numéro de téléphone, nous obtenons un numéro d'immatriculation d'entreprise suédoise.

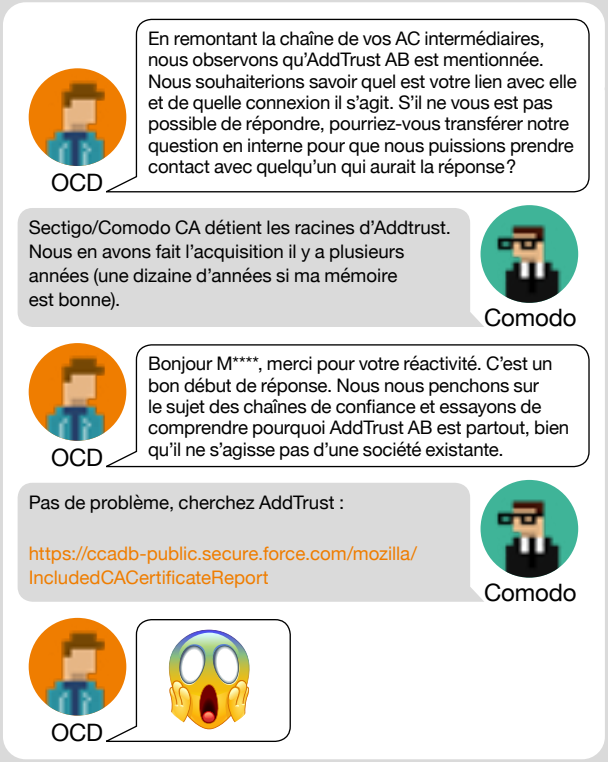
En vérifiant cette adresse sur Google Maps, nous tombons sur une société appelée **Lequa AB.**

Nous trouvons aussi **« Anders O. »** sur LinkedIn, où il déclare être le propriétaire **d'Internet Express Scandinavia (IES).**

Dans la section « Qui sommes-nous » du site **d'IES**, il est dit que l'entreprise travaille à 45 % pour la société **Lequa AB**. Le domaine pour Lequa est **lequa.com.**

Le produit qu'ils mettent en avant pointe vers cette URL : **http://www.lequinox.com/**, mais ce domaine n'était plus disponible à l'époque

IES nous renvoie vers **Lequa**, qui à son tour nous renvoie vers une organisation appelée **Comodo**, dont nos savons qu'elle est un acteur majeur dans le milieu des autorités de certification [6.4].

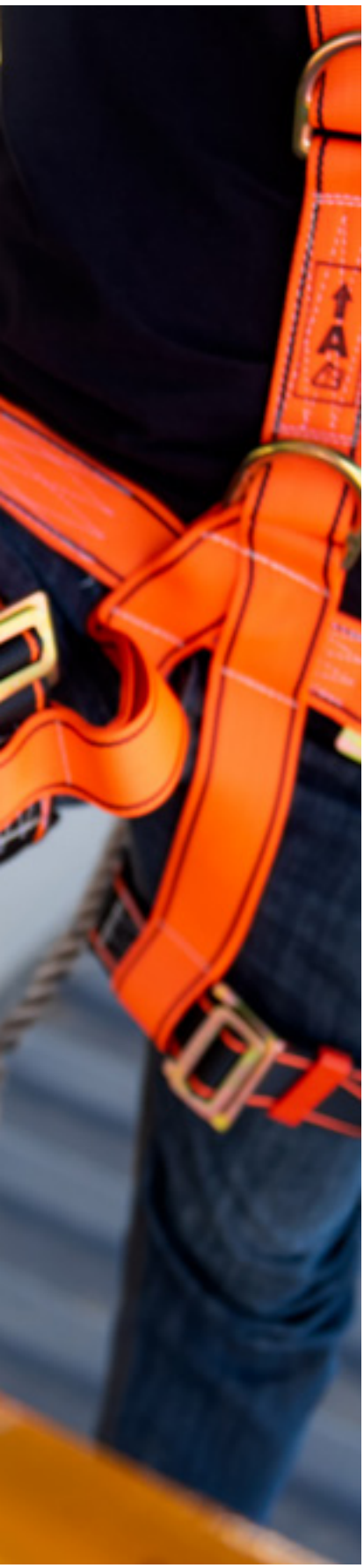


En résumé :

Après une longue enquête avec des indices obscurs disséminés sur le Web, nous avons découvert qu'il y a environ dix ans, AddTrust a été rachetée par Comodo CA, désormais connue sous le nom de Sectigo.

Elle a émis son dernier certificat en 2013[6.4]. Du fait de la longévité des chaînes de confiance, nous pouvons voir qu'AddTrust est toujours la racine de nombreux certificats sur Internet.

À noter qu'AddTrust External CA Root a expiré le 30 mai 2020[6.5].



Stefan Lager
Senior VP Global Service Lines
Orange Cyberdefense

Prédictions cyber

Resserrez les lignes de votre cyberdéfense

En septembre 2019, la NASA a divulgué une étude Google sur la suprématie quantique. Les spéculations quant au comment (et au pourquoi) vont bon train [7.1] mais une chose est sûre : l'informatique quantique gagne du terrain et pourrait faire plus qu'impacter des concepts tels que la cryptographie. Elle pourrait en effet changer la façon dont les ordinateurs fonctionnent et sont utilisés à une échelle telle que même la révolution de l'Intelligence Artificielle passerait pour une mise à jour mineure de système d'exploitation. Toutefois, comme avec tout ce qui a trait à l'informatique quantique, de multiples incertitudes persistent.

Concentrons-nous alors sur des prédictions plus fiables. Que nous apprennent nos données sur ce que 2020 nous réserve encore ?

Un nouveau modèle d'évaluation des menaces

Pendant longtemps, la cybersécurité était dictée par une approche réactive qui consistait à investir dans la technologique pour prévenir les incidents.

Malheureusement, cette approche s'est avérée infructueuse puisque le nombre de violations a progressé malgré des dépenses plus conséquentes. Nous pensons qu'il est important d'équilibrer les investissements entre anticipation des menaces, détection des intrusions, protection des actifs, réponse à incident et remédiation.

A propos des incidents, nous estimons que les entreprises devront les envisager sous deux aspects :

1. L'incident au niveau de l'infrastructure : quand des équipements ou workloads sont affectés
2. La violation de données : quand des données critiques sont détruites, prises en otage à des fins d'extorsion ou divulguées.

Les organisations doivent accepter que leurs infrastructures soient attaquées, quel que soit le montant de leur investissement dans des technologies préventives.
Une fois cette notion admise, il leur faut un plan pour détecter les intrusions, limiter l'impact d'éventuelles atteintes à l'infrastructure et une réponse aussi rapide que possible.
Nous pensons qu'en 2020 les investissements seront déplacés vers ces besoins.

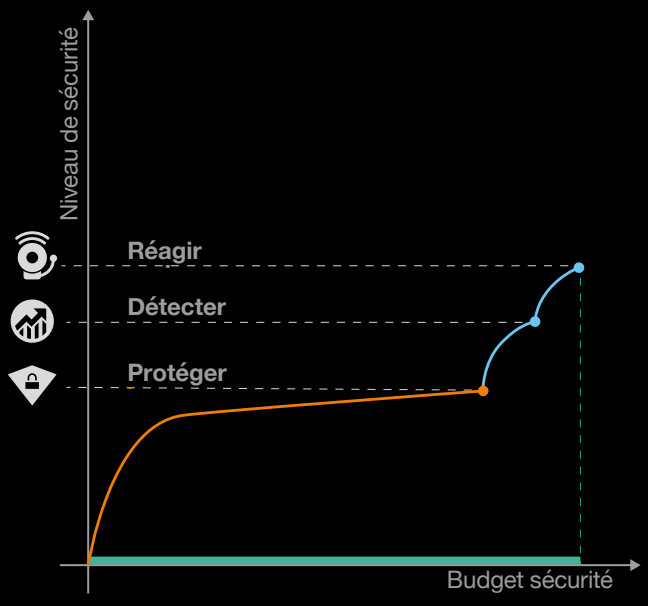
Penser la détection

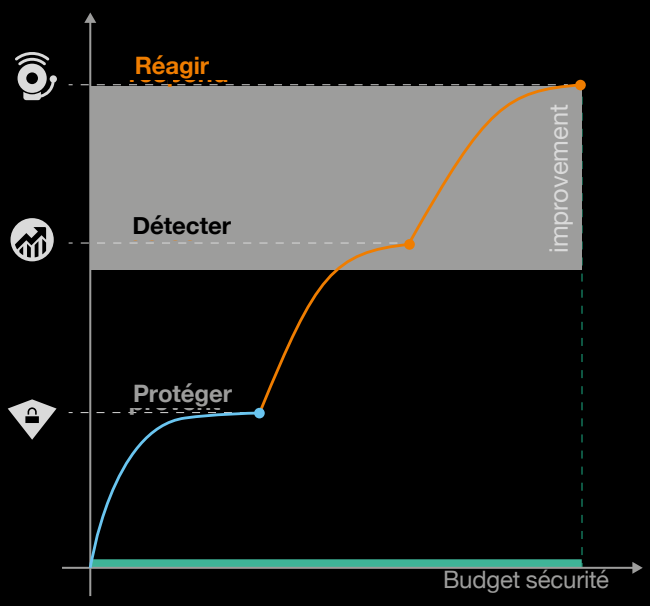
Admettons que nous devons améliorer notre capacité à détecter les menaces : comment y parvenir ? Nous estimons que la simple détection par revue des logs évoluera pour inclure aussi la détection réseau et la détection sur les postes de travail.
Vous devez choisir votre stratégie de détection en fonction de votre environnement et de vos besoins.

Si une détection par souci de conformité prévaut, fiez-vous aux logs. Si vous visez la rentabilité, des capacités de détection et de réponse avancées, alors la détection sur les postes de travail est primordiale. S'il vous est impossible d'installer des systèmes de prévention d'intrusions sur vos postes (HIPS), orientez-vous vers la détection réseau. Si vos exigences de détection sont élevées, il vous faut combiner ces approches.

Il est désormais de notoriété publique que la cybersécurité est une question de « Big Data ». Et ce, que vous analysiez les données des postes, du réseau ou des logs. Pour résoudre ce problème, les organisations devront augmenter leurs investissements dans des technologies solides d'intelligence artificielle et de Machine Learning pour les aider à analyser cette quantité massive de données. La clé pour faire usage de ces technologies d'IA et de Machine Learning est d'être conscient que les technologies ne sont pas une panacée. Par souci d'efficacité, il faut définir un problème auquel la technologie sera appliquée en tant qu'outil et non en tant que solution.
Une bonne mise en œuvre des technologies d'IA et de Machine Learning peut considérablement délester la charge des analystes. Au même titre que l'orchestration et l'automatisation, les composantes clé pour construire le SOC du futur.

Allouer une partie de votre budget sécurité à la détection et à la réponse vous mènera plus loin que de trop dépenser en prévention





La réponse à incidents : un atout supplémentaire

La réponse à incidents : un atout supplémentaire

Une fois l'approche technologique mise au point, quelle est la prochaine étape ? il vous faut des équipes et procédures pour assurer l'analyse et la classification des détections, 7 jours sur 7 et 24 heures sur 24. Beaucoup d'entreprises ont du mal à trouver le budget et le temps pour mettre ces services en œuvre. Elles souscrivent alors à des services managés de détection et de réponse à incidents (MDR) pour disposer d'un support permanent en 24/7

Quel que soit l'incident de sécurité, plus il est détecté tôt, moins les dommages sont conséquents. En somme : plus vite vous identifiez un incident potentiel, moins les dommages seront étendus.

Les risques induits par un incident dépendent de la rapidité de détection et de réponse à la menace. Mais détecter l'attaque n'est qu'une partie du problème, la réponse et la remédiation sont tout aussi importantes.

En 2019, plusieurs clients ont contacté notre support pour les aider à régler d'urgence des incidents. Nous pensons qu'en 2020, les clients seront plus proactifs, s'appuieront sur leurs capacités internes pour répondre plus rapidement aux menaces et compléteront ces efforts en souscrivant des contrats auprès de fournisseurs de services de cybersécurité.

À l'origine : la visibilité

Les budgets dédiés à la cybersécurité étant limités, ces investissements doivent ainsi être dépensés de façon avisée. Afin de prendre les bonnes décisions, il vous faut des données et de la visibilité pour comprendre quelles dépenses seraient les plus judicieuses. C'est pourquoi nous pensons que les investissements augmenteront à l'avenir dans le domaine de la détection et de la réaction.

Voici des exemples et domaines pour lesquels nous avons vu la demande augmenter.

Visibilité sur les endpoints et les réseaux

Des décennies durant, des SIEM ont été déployés comme premier moyen de détecter et répondre aux menaces. Leur implémentation demande souvent du temps, des ressources, des réglages et de la maintenance. En fin de compte, leur performance ne va pas au-delà du type de données qu'ils fournissent (données souvent limitées par ailleurs pour des raisons budgétaires. Nous continuons de penser que les SIEM sont des composantes centrales de vos SOC, mais vous pouvez maximiser votre rentabilité et améliorer vos capacités de détection des menaces en déployant des systèmes de détection sur les endpoints et les réseaux. Nous observons une tendance qui consiste à investir dans ces deux technologies. Là aussi, sous forme de service managé pour les clients ne disposant pas de leur propre équipe CSIRT, 7 jours sur 7 et 24 heures sur 24.

Un SIEM pour visualiser les données machine

Les données sont le nouvel « or noir » alors pourquoi ne pas essayer d'utiliser celles que vous créez chaque jour pour vous aider à prendre des décisions et gérer votre entreprise plus efficacement ? Nous estimons que la seule collecte et analyse des logs pourrait servir d'autres besoins en informatique voire même des besoins commerciaux

Visibilité du Cloud

Tous passent au Cloud et les équipes DevOps font tourner de nouveaux environnements chaque minute. Pour autant, nous savons que les principaux incidents dans les infrastructures Cloud sont liés à des défauts de configuration ou à une exploitation inadéquate. Nous pensons que la technologie, qui se connecte aux API Cloud pour extraire des données d'inventaires et de sécurité, sera d'une grande aide pour vos équipes sécurité, leur permettant de contrôler leur infrastructure Cloud tout en simplifiant le travail de mise en conformité.

Visibilité sur les OT (technologies d'exploitation) et ICS (Systèmes de contrôle industriel)

L'Internet des objets industriel (IIOT) et l'industrie 4.0 relèvent de la connexion de machines à d'autres machines, ainsi que de l'optimisation et de la productivité requises pour créer des usines intelligentes.

Les bénéfices sont immenses, les défis également. L'un des plus grands défis : combler le fossé entre experts en OT et experts en sécurité. Aussi, ils comprendraient chacun mieux les difficultés propres à ces deux domaines pour construire ensemble des environnements opérationnels sécurisés. Un bon début serait de gagner en visibilité sur ce qui se connecte aux réseaux et comment ils communiquent. Cette compréhension permettrait de mettre en place des solutions de protection et de détection des menaces pour sécuriser ces environnements.

Visibilité sur les comptes à privilèges

La majorité des violations de données repose sur l'usage de comptes à privilèges pour se déplacer latéralement et exfiltrer des données. Pourquoi ? Et bien… parce que c'est facile. Beaucoup d'organisations n'ont pas de visibilité ou de contrôle sur tous les comptes hautement sensibles. Selon une estimation récurrente : le nombre de comptes à privilèges est environ trois fois supérieur au nombre de comptes utilisateurs normaux. Contrôlez-vous qui accède à ces comptes, comment les mots de passe sont partagés ou changés, et ce que les gens en font lorsqu'ils sont connectés en tant qu'administrateurs ? Gagner en visibilité sur vos comptes à privilèges est une première étape dans votre stratégie de sécurisation de ces derniers.

120 cliniques privées du groupe Ramsay visées pas une cyberattaque

Une attaque a causé une panne informatique à Marseille, mais a été contenue par les équipes de réponse à incident avant qu'elle ne puisse se propager. [t43]

SEP

Firefox 69 bloque par défaut les cookies des tierces parties et le cryptojacking

En activant par défaut une protection avancée contre le traçage pour tous ses utilisateurs, Mozilla désactive automatiquement des cookies populaires, tels que Google Analytics, et empêche le cryptojacking JavaScript de fonctionner. [t44]

Conclusion : Et après ?

Une fois que vous avez gagné en visibilité sur vos actifs et vos données, les investissements doivent inclure la prévention, la détection et la réponse. Nous prévoyons que :

La prévention passera de « tout ou rien » à une approche gérée par risque. Les données critiques ou les collaborateurs autorisés à accéder à des données critiques, devraient bénéficier de protections appropriées.

La détection passera de « standard » à une détection centrée sur le client. Les règles génériques au sein du SIEM ne sont pas suffisantes pour détecter des opposants avertis.

La réponse passera du « Oups ! À l'aide ! » à une approche proactive et planifiée.

Cartographier vos propres capacités et souscrire à des ressources externes sera une priorité.

De nombreuses organisations ne disposent pas des capacités requises en matière de détection et de réponse.
Nous pensons donc que le marché des services managés de détection et de réponse connaîtra une croissance significative.

Le profil du PDG de Twitter, Jack Dorsey, piraté

Twitter désactive le Tweeting via SMS après que des pirates ont profité d'une attaque par SIM swapping pour s'emparer du numéro de mobile de Jack Dorsey. Ils l'avaient obtenu au moyen de techniques d'ingénierie sociale visant un employé d'AT&T. [t45]

Les informations personnelles de la quasi-totalité des citoyens équatoriens dans la nature

Le directeur général de la société de conseil en informatique Novaestrat a été arrêté après que les données personnelles de la quasi-totalité de la population ont été exposées sur un serveur Elasticsearch non protégé. [t46]

Le botnet de cryptojacking Smominru poursuit sa propagation

Selon les recherches de Guardicore, le malware infecte près de 90 000 clients chaque mois et utilise la vulnérabilité EternalBlue, connue depuis la tristement célèbre attaque WannaCry. [t47]

Plus de 16 millions de données de patients de 50 pays laissées sans protections

Les données comptent des images et scanners médicaux (radios, TDM, IRM) ainsi que des informations personnelles (noms, adresses et numéro de sécurité sociale). Dans ce cas, pas de piratage, mais un problème avec la manière dont les clichés sont stockés depuis des années. [t48]

OCT

Un mot de passe cassé après 39 ans

Ce mot de passe appartient à Ken Thompson, l'un des pères d'UNIX. Même en 2019, le mot de passe à 8 caractères s'est avéré étonnamment difficile à casser. Il s'est avéré être le raccourci d'un coup d'échecs (l'ouverture du Gambit Dame) : « p/q2q4!a ». [t49]

Go Sport et Courir frappés par un ransomware

Le groupe de distribution et détaillant de vêtements Go Sport et Courir a subi une attaque par ransomware fin octobre 2019. Les points de vente ont dû être fermés et leur système de paiement a dû être mis hors ligne. [t50]

L'agglomération du Grand Cognac refuse de payer une rançon

400 ordinateurs, ainsi que les serveurs principaux et de sauvegarde ont été infectés par e-mail, causant le chiffrement de 10 ans de documents de travail interne. La rançon s'élève à 180 000 €. [t51]

Le groupe M6 impacté par un ransomware

Le plus grand groupe multimédia privé en France a été frappé par un ransomware. Les mises à jour cybersécurité ont permis d'éviter toute interruption radio et télé. [t52]

InfoTrax détecte une fuite après que ses serveurs ont manqué d'espace de stockage

L'infraction semblait courir depuis 2014, mais n'a été découverte qu'après qu'une archive de données volées créée par les pirates a menacé les capacités de stockage du serveur de la société. InfoTrax fournit des solutions d'PGI (progiciel de gestion intégrée). [t55]

Le géant Edenred admet avoir subi une cyberattaque

Edenred est le spécialiste des avantages aux salariés, diversifié dans les solutions de mobilité et de paiements pour 50 millions de clients dans le monde entier. Grâce à une réponse rapide, l'impact de cette attaque a été relativement limité. [t54]

T-Mobile US touché par une fuite de données

Des malfaiteurs ont pu mettre la main sur les données personnelles de plus d'un million de clients. Les informations financières et mots de passe n'auraient pas été pillés. [t56]

DEC

Un bug récemment découvert permet aux attaquants de contourner les connexions VPN chiffrées

CVE-2019-14899 affecte la plupart des systèmes d'exploitation Linux et Unix, dont FreeBSD, OpenBSD, macOS, iOS et Android. Elle permet à des attaquants d'espionner (et de manipuler) les connexions VPN chiffrées, à distance depuis un réseau adjacent. [t57]

Le CHU de Rouen repasse au « papier-stylo » après une cyberattaque

Une réponse rapide de l'ANSSI en France a aidé à limiter l'ampleur de la propagation du ransomware et à restaurer les systèmes dans un bref délai. [t53]

Le ransomware Snatch redémarre Windows en mode sans échec pour contourner l'antivirus

Ce ransomware modifie une clé de registre Windows pour programmer un service qui démarre en mode sans échec et qui procède au chiffrement. Snatch cible principalement les entreprises et institutions gouvernementales. [t58]

NOV

Synthèse

Qu'avons-nous appris ?

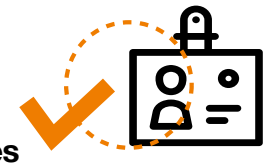
Etienne Greeff
CTO
Orange Cyberdefense

Après tant de faits et d'avis captivants, rédiger une conclusion est un défi. J'essaierai donc de mettre en lumière les points qui, j'estime, sont à retenir de notre Security Navigator. Pour commencer, je tiens à revenir sur le principe de base de la confiance numérique. Il est évident que nous vivons dans un monde hautement connecté. Nos interactions avec des systèmes numériques et connectés sont multiples dans chacun des pendants de nos vies. Ces systèmes simplifient notre quotidien et améliorent substantiellement notre qualité de vie. Mais rien de tout ceci n'est gratuit. En tant que clients, nos données, nos choix, nos comportements et nos interactions avec les autres sont devenus un produit utilisé pour le meilleur, mais aussi pour le pire. Je doute que nous ayons tous fait le choix conscient de donner libre accès à nos données personnelles et, dans les faits, à nos vies, lorsque nous avons commencé à interagir avec et à utiliser ces systèmes en ligne et ces systèmes électroniques. En d'autres termes, quand nous avons commencé à profiter des avantages de la technologie, nous n'avons pas pleinement pris en compte les inconvénients potentiels. Comme parfaitement illustré dans ce rapport, nos données sont souvent compromises, vendues et utilisées sans que nous ne l'ayons jamais anticipé.

Je ne dis pas qu'il faut se passer des technologies, mais je pense que les entreprises se doivent d'apporter leur contribution et prendre l'entière responsabilité des données que nous leur confions. Je pense que, de nos jours, l'industrie de la cybersécurité dans son ensemble ne répond pas à la promesse faite de garantir la confiance de ses clients. Bien que les dépenses augmentent, nous devons faire face à des incidents de sécurité dont l'ampleur et la fréquence progressent. Certaines personnes, lassées d'en entendre parler, haussent simplement les épaules quand elles apprennent que de nouvelles infractions ont été identifiées.

Les actualités sont constellées d'informations sur ces grands piratages, mais les enseignements n'en sont pas tirés. Notre industrie est dominée par la technologie et les éditeurs de services qui proposent de plus en plus de solutions pour résoudre un problème qui est presque invariablement le même. Selon moi, plus d'attention devrait être portée à la compréhension des risques, la recherche d'éventuelles failles et la construction d'une capacité de réponse et de remédiation fortes.

Pour améliorer l'aspect préventif de la menace, je tiens à insister sur quatre axes génériques, des axes qui ont été décrits au fil de ce rapport.



1 Modifier les comportements humains

Il s'agit souvent de l'axe qui est le moins investi. La cyberdéfense commence avec et se termine par nos utilisateurs. Souvent considérés comme le maillon faible, ils peuvent aussi devenir nos principaux alliés, agissant comme des capteurs humains intelligents. S'il ne me fallait donner qu'un conseil aux RSSI, il concernerait le besoin d'éduquer et de responsabiliser les utilisateurs, de cesser de les considérer comme des victimes.

2 Se concentrer sur l'authentification et les autorisations

Au vu du grand nombre de mots de passe utilisateur compromis – près de la moitié de la population mondiale–, il est clair que la seule utilisation des mots de passe est insuffisante. L' authentification forte devrait être une obligation, tout en étant transparente et encore plus simple d'utilisation qu'un mot de passe. Il est sans doute temps de leur donner congé. Au-delà des seuls mots de passe, il convient de porter attention aux autorisations et de mettre en pratique le principe du moindre privilège. Nos hackers éthiques sont ravis de tomber sur des comptes utilisateurs disposant de droits d'administration ou sur des comptes admin présentant les mêmes mots de passe qu'un utilisateur.

Google lance un nouveau « Patch Rewards Program » encourageant le renforcement de la sécurité des open source

Une fois achevé, le programme récompensera et apportera un soutien financier aux développeurs de solutions open source donnant priorité à la sécurité des projets. [t59]

3 Compartimenter les réseaux

L'un des principes fondamentaux de la sécurité des réseaux consiste en l'instauration de zones de confiance. Une zone de confiance rassemble des équipements ou des données dont le niveau de confiance est similaire. Beaucoup d'entreprises présentent une seule zone de confiance et peu de barrières dans leur réseau. Ce qui est surprenant de la part d'un grand nombre d'organisations n'est pas tant le fait qu'elles endurent des compromissions, mais qu'une fois compromises, les pirates peuvent se déplacer librement dans le réseau cible.

4 Comprendre votre surface d'attaque et vos vulnérabilités

Les cas de piratage sont rarement aussi avancés que la presse le laisse entendre. Dans la plupart des cas, les vulnérabilités exploitées sont anciennes et bien comprises. Plusieurs preuves démontrent que l'ancienneté moyenne des vulnérabilités exploitées lors de grandes attaques est de 90 jours. Pour bon nombre de compromissions récentes, les pirates n'ont même pas eu besoin d'exploiter une vulnérabilité. Ils n'ont eu qu'à télécharger une base de données depuis un serveur public sans mot de passe requis. Si les entreprises passaient autant de temps à comprendre l'ampleur de leur surface d'attaque et leurs vulnérabilités qu'à tenter de mettre en œuvre des technologies de cybersécurité à la mode, notre rapport serait bien moins long.
Un programme bien structuré de gestion des vulnérabilités et une compréhension détaillée de votre environnement et de la localisation de vos données, améliorera le niveau de votre sécurité de manière exponentielle.

Je conclurai en disant que, pour l'instant, la cybercriminalité paie, et paie bien. Comme présenté dans ce rapport, les pirates se font souvent payer les rançons, en particulier quand des assurances contre les cyber risques sont souscrites. Ces hackers percevant des « récompenses » à six chiffres pour leurs crimes contribuent à alimenter l'écosystème criminel, ce qui mènera probablement à une augmentation substantielle des activités de piratage. Selon moi, il s'agit du changement le plus marquant dans le monde de la cybersécurité en 2019. Les criminels peuvent monétiser leur savoir-faire au moyen d'outils de plus en plus sophistiqués, souvent développés par les gouvernements. Cette situation est préoccupante et montre que chaque entreprise doit se dire qu'elle sera un jour ciblée. Comme le dit Stefan Lager, il nous faut porter autant d'attention à l'identification de nos risques, la détection des problèmes, la réaction et la remédiation, qu'à la protection de nos actifs.

Évidemment, la pandémie de COVID-19 a donné lieu à de nouveaux défis en matière de cybersécurité. Mais ils pourraient ne pas être si « nouveaux » après tout. Le travail à distance est une réalité depuis de nombreuses années. La migration massive vers le télétravail et les infrastructures Cloud a simplement augmenté le besoin de visibilité. Les périmètres traditionnels ayant presque disparus, les solutions intelligentes doivent être mises en œuvre pour prévenir, détecter et répondre aux menaces.

Chronologie 2020 ▸

Contributeurs, sources et liens

Sources

Ce rapport n'aurait pu voir le jour sans l'investissement de la part de plusieurs chercheurs, journalistes et organisations dans le monde entier. Nous leur sommes reconnaissants de nous avoir permis de nous appuyer sur leurs publications en ligne pour référence ou pour une meilleure contextualisation.

Statistiques

All statistics originate from Orange Cyberdefense's CyberSOCs

La Fondation de Patrimoine et l'incendie de Notre-Dame de Paris

[1.1] https://www.zdnet.fr/actualites/notre-dame-de-paris-elan-de-solidarite-et-arnaques-en-tout-genre-39892077.htm

[1.2] Letter dated July 12, 2019 from Mr. Guillaume Poitrinal, President of the Fondation du Patrimoine to Orange Cyberdefense

Les statistiques de nos CyberSOC

[2.3] https://coinmarketcap.com/currencies/monero/

[2.4] https://coinmarketcap.com/currencies/ethereum/

[2.5] https://coinmarketcap.com/currencies/litecoin/

[2.6] https://coinmarketcap.com/currencies/bitcoin/

[2.7] https://www.biznesstransform.com/transforming-the-food-and-beverage-industry-with-digital-technologies/

L'essor des fuites de données

[4.1] https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/

[4.2] https://www.lowyat.net/2019/177033/over-1-million-uitm-students-and-alumni-personal-details-leaked-online

[4.3] https://www.cnn.com/2019/01/28/health/hiv-status-data-leak-singapore-intl/index.html

[4.4] https://www.theregister.co.uk/2019/02/11/620_million_hacked_accounts_dark_web/

[4.5] https://thehackernews.com/2019/02/data-breach-website.html

[4.6] https://thehackernews.com/2019/02/data-breach-sale-darkweb.html

[4.7] https://www.todayonline.com/singapore/personal-data-808000-blood-donors-compromised-nine-weeks-hsa-lodges-police-report

[4.8] https://thehackernews.com/2019/03/data-breach-security.html

[4.9] https://www.upguard.com/breaches/facebook-user-data-leak

[4.10] https://www.businessinsider.com/facebook-uploaded-1-5-million-users-email-contacts-without-permission-2019-4

[4.11] https://economictimes.indiatimes.com/tech/internet/data-breach-at-justdial-leaks-100-million-user-details/articleshow/68930607.cms

[4.12] https://www.vpnmentor.com/blog/report-millions-homes-exposed/

[4.13] https://www.analyticsindiamag.com/data-breach-truecaller-exposes-indian-users-data-shows-cracks-in-cyber-security-infrastructure/

[4.14] https://gizmodo.com/885-million-sensitive-records-leaked-online-bank-trans-1835016235

[4.15] https://www.cisomag.com/nearly-140-million-user-data-leaked-in-canva-hack/

[4.16] https://finance.nine.com.au/business-news/westpac-data-breach-100000-australian-customers-at-risk/84c91581-90b6-464e-9137-a2d973492614

[4.17] https://www.theguardian.com/australia-news/2019/jun/04/australian-national-university-hit-by-huge-data-breach

[4.18] https://www.publishedreporter.com/2019/06/05/nearly-12-million-quest-diagnostics-patients-medical-info-exposed-in-new-data-breach/

[4.19] https://www.cbc.ca/news/canada/montreal/desjardins-data-breach-1.5183297

[4.20] https://www.reuters.com/article/us-bulgaria-cybersecurity/hackers-steal-millions-of-bulgarians-financial-records-tax-agency-idUSKCN1UB0MA

[4.21] https://edition.cnn.com/2019/07/29/business/capital-one-data-breach/index.html

[4.22] https://techcrunch.com/2019/08/03/stockx-hacked-millions-records/

[4.23] https://www.propublica.org/article/millions-of-americans-medical-images-and-data-are-available-on-the-internet

[4.24] https://www.vpnmentor.com/blog/report-ecuador-leak/

[4.25] https://www.upguard.com/breaches/mts-nokia-telecom-inventory-data-exposure

[4.26] https://japan.cnet.com/article/35143123/

[4.27] https://techcrunch.com/2019/09/26/doordash-data-breach/

[4.28] https://venturebeat.com/2019/09/30/words-with-friends-player-data-allegedly-stolen-for-218-million-users/

[4.29] https://www.worldometers.info/world-population/

[4.30] https://pages.riskbasedsecurity.com/2019-midyear-data-breach-quickview-report

[4.31] https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf

PKI et confiance numérique

[6.1] https://docs.microsoft.com/en-us/windows/win32/seccertenroll/about-certification-authorities

[6.2] https://www.bloomberg.com/profiles/companies/108453Z:SS-addtrust-ab

[6.3] http://web.archive.org/web/20110128085641/http://www.addtrust.com/

[6.4] https://en.wikipedia.org/wiki/Certificate_authority

[6.5] https://www.xolphin.com/support/Rootcertificates/Phasing_out_Addtrust_External_CA_Root_certificate

Prédictions cyber

[7.1] https://towardsdatascience.com/google-has-cracked-quantum-supremacy-cd70c79a774b

Chronologie

[t1] https://www.avanan.com/resources/zwasp-microsoft-office-365-phishing-vulnerability

[t2] https://www.justice.gov/usao-ma/pr/jury-convicts-man-who-hacked-boston-childrens-hospital-and-wayside-youth-family-support

[t3] https://www.safetydetectives.com/blog/major-security-breach-discovered-affecting-nearly-half-of-all-airline-travelers-worldwide/

[t4] https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/

[t5] https://www.reuters.com/article/us-altran-tech-cyber/frances-altran-tech-says-it-was-hit-by-cyber-attack-idUSKCN1PM0IJ

[t6] https://www.carbonblack.com/2019/01/24/carbon-black-tau-threatsight-analysis-gandcrab-and-ursnif-campaign/

[t7] https://www.reuters.com/article/us-airbus-cyberattack-report/hackers-tried-to-steal-airbus-secrets-via-contractors-afp-idUSKBN1WB0U9

[t8] https://thehackernews.com/2019/02/cryptocurrency-exchange-exit-scam.html

[t9] https://blog.zimperium.com/dont-give-me-a-brake-xiaomi-scooter-hack-enables-dangerous-accelerations-and-stops-for-unsuspecting-riders/

[t10] https://thehackernews.com/2019/02/vfemail-cyber-attack.html

[t11] https://www.theregister.co.uk/2019/02/11/620_million_hacked_accounts_dark_web/ , https://thehackernews.com/2019/02/data-breach-sale-darkweb.html

[t12] https://www.mcafee.com/enterprise/en-us/about/newsroom/press-releases/press-release.html?news_id=20190303005031

[t13] https://blog.mozilla.org/blog/2019/03/12/introducing-firefox-send-providing-free-file-transfers-while-keeping-your-personal-information-private/

[t14] https://thehackernews.com/2019/03/data-breach-security.html

[t15] https://unit42.paloaltonetworks.com/new-mirai-variant-targets-enterprise-wireless-presentation-display-systems/

[t16] https://www.reuters.com/article/us-norsk-hydro-cyber/aluminum-producer-hydro-hit-by-cyber-attack-shuts-some-plants-idUSKCN1R00NJ

[t17] https://www.us-cert.gov/ics/advisories/ICSMA-19-080-01

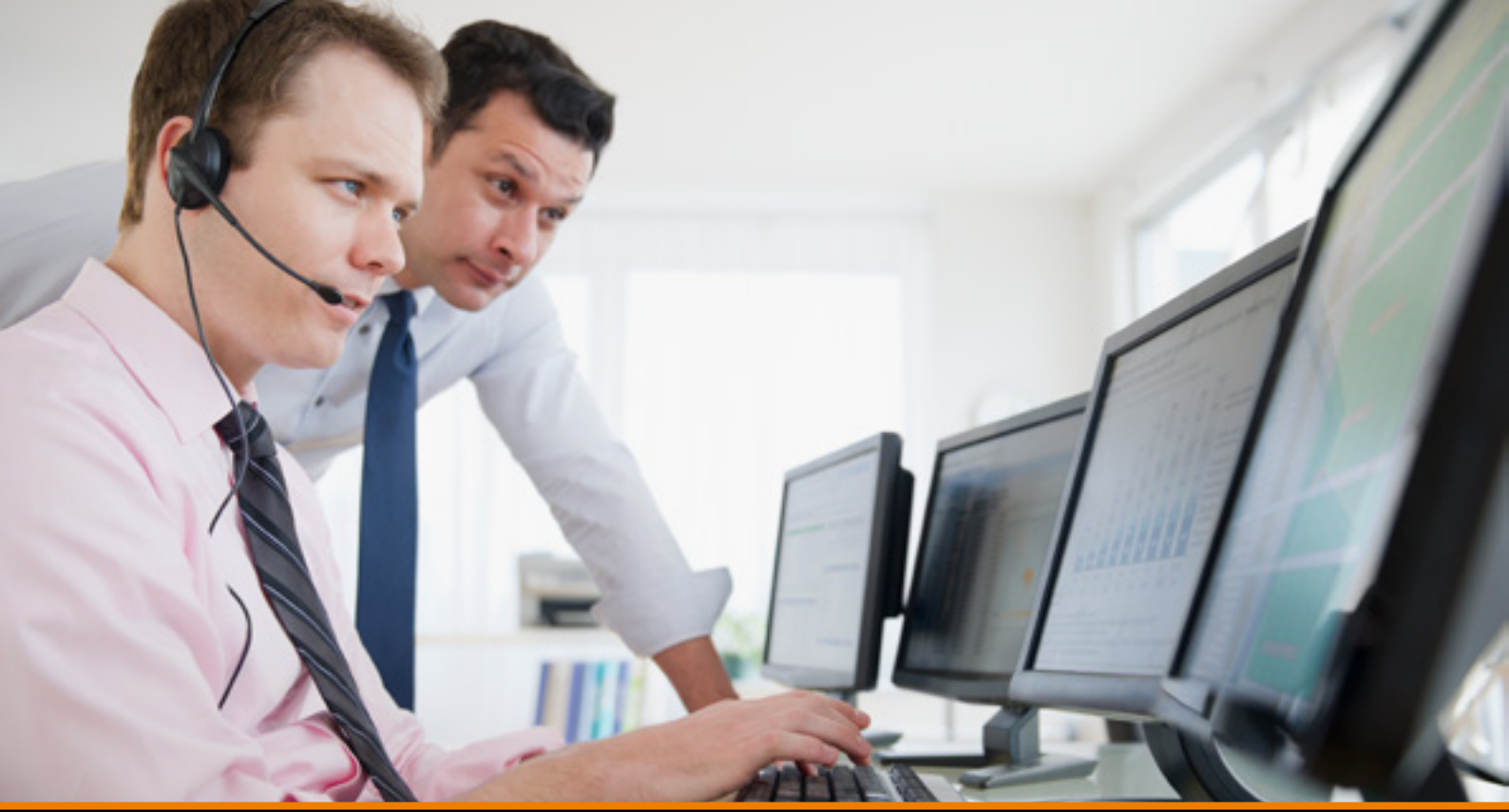
[t18] https://cafe.bithumb.com/view/board-contents/1640037
[t19] https://www.upguard.com/breaches/facebook-user-data-leak
[t20] https://www.reuters.com/article/us-bayer-cyber/bayer-contains-cyber-attack-it-says-bore-chinese-hallmarks-idUSKCN-1RG0NN
[t21] https://securelist.com/project-tajmahal/90240/
[t22] https://medium.com/@fs0c131y/tchap-the-super-not-secure-app-of-the-french-government-84b31517d144
[t23] https://blog.malwarebytes.com/cybercrime/2019/04/electrum-ddos-botnet-reaches-152000-infected-hosts/
[t24] https://vaaju.com/franceeng/fleury-michon-stopped-production-for-five-days-due-to-a-computer-virus/
[t25] https://www.vpnmentor.com/blog/report-millions-homes-exposed/
[t26] https://www.europol.europa.eu/newsroom/news/double-blow-to-dark-web-marketplaces
[t27] https://thehackernews.com/2019/05/baltimore-ransomware-cyberattack.html
[t28] https://www.lemondeinformatique.fr/actualites/lire-le-site-des-aeroports-de-lyon-cible-par-une-cyberattaque-75489.html
[t29] https://morphuslabs.com/goldbrute-botnet-brute-forcing-1-5-million-rdp-servers-371f219ec37d
[t30] https://labs.bitdefender.com/2019/06/good-riddance-gandcrab-were-still-fixing-the-mess-you-left-behind/
[t31] https://moneyandpayments.simonl.org/2019/06/perspectives-on-ca-libra-1-first-we-get.html
[t32] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/
[t33] https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related
[t34] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-internation-al-inc-more-than-99-million-under-gdpr-for-data-breach/
[t35] https://thehackernews.com/2019/07/ransomware-nas-devices.html
[t36] https://www.zdnet.com/article/kazakhstan-government-is-now-intercepting-all-https-traffic/
[t37] https://twitter.com/CityPowerJhb/status/1154277777950093313
[t38] https://research.checkpoint.com/say-cheese-ransomware-ing-a-dslr-camera/
[t39] https://www.ecb.europa.eu/press/pr/date/2019/html/ecb.pr190815~b1662300c5.en.html
[t40] https://decoded.avast.io/janvojtesek/putting-an-end-to-retadup-a-malicious-worm-that-infected-hundreds-of-thousands/
[t41] https://thehackernews.com/2019/08/dds-safe-dental-ransomware-attack.html
[t42] https://www.theregister.co.uk/2019/08/21/kazakstan_snooping_blockade/
[t43] https://www.tellerreport.com/life/2019-08-13---the-120-hospitals-of-the-ramsay-health-group-in-france-victims-of-a-cyber-attack-.rJQ3yHqg4r.html
[t44] https://blog.mozilla.org/blog/2019/09/03/todays-firefox-blocks-third-party-tracking-cookies-and-cryptomining-by-default/
[t45] https://thehackernews.com/2019/09/tweet-via-sms-text-message-hacking.html
[t46] https://www.vpnmentor.com/blog/report-ecuador-leak/
[t47] https://www.guardicore.com/2019/09/smominru-botnet-attack-breaches-windows-machines-using-eternalblue-exploit
[t48] https://www.propublica.org/article/millions-of-americans-medical-images-and-data-are-available-on-the-internet
[t49] https://thehackernews.com/2019/10/unix-bsd-password-cracked.html
[t50] https://www.lemondeinformatique.fr/actualites/lire-go-sport-et-courir-victimes-d-un-ransomware-77403.html
[t51] http://www.leparisien.fr/societe/cyberattaque-l-agglomeration-grand-cognac-refuse-de-payer-la-ran-con-31-10-2019-8183676.php
[t52] https://www.zdnet.com/article/m6-one-of-frances-biggest-tv-channels-hit-by-ransomware/
[t53] https://www.bbc.com/news/technology-50503841
[t54] https://www.bleepingcomputer.com/news/security/edenred-payment-solutions-giant-announces-malware-incident/
[t55] https://thehackernews.com/2019/11/hacking-file-storage.html
[t56] https://www.techradar.com/news/over-a-million-t-mobile-customers-hit-in-data-breach
[t57] https://thehackernews.com/2019/12/linux-vpn-hacking.html
[t58] https://www.zdnet.com/article/snatch-ransomware-reboots-pcs-in-windows-safe-mode-to-bypass-antivirus-apps/
[t59] https://security.googleblog.com/2019/12/announcing-updates-to-our-patch-rewards.html

Avertissement

Orange Cyberdefense publie ce rapport « tel quel » en s'efforçant d'offrir à ses lecteurs l'information la plus fiable et la plus qualitative possible mais sans prétendre à l'exactitude ou à l'exhaustivité. Les informations présentées dans ce rapport sont de nature générique et ne sauraient être utilisées pour répondre à des problèmes de sécurité spécifiques. Les opinions et conclusions rendues ici reflètent un jugement à l'heure de la publication et sont susceptibles de changer sans préavis. Tout usage des informations contenues dans ce rapport se ferait aux risques de l'utilisateur. Orange Cyberdefense n'est en aucun cas responsable des éventuelles erreurs, omissions ou dommages pouvant résulter de l'usage ou du recours aux présentes informations. En cas de problématiques spécifiques liées à la cybersécurité de votre entreprise, veuillez contacter Orange Cyberdefense pour des analyses détaillées et pour tout service de conseil.

En cas d'urgence, vous pouvez joindre nos équipes du CSIRT depuis des lignes dédiées 7 jours sur 7 et 24 heures sur 24 ! Retrouvez la liste des numéros d'assistance par pays sur orangecyberdefense.com !

Un remerciement particulier à l'ensemble des « chasseurs cyber », analystes et ingénieurs de nos CyberSOC.



Pourquoi Orange Cyberdefense ?

Des spécialistes en cybersécurité
Orange Cyberdefense est le spécialiste des services et solutions de cybersécurité, et s'appuie sur 25 ans d'expertise en services managés pour les plus grands groupes mondiaux.

Une expertise de pointe
Nos services sont délivrés par nos 10 CyberSOC et 16 SOC dans le monde entier, fournissant un accès immédiat et permanent (7 jours sur 7 et 24 heures sur 24) à des spécialistes chargés de gérer les incidents et de vous garantir une disponibilité continue.

L'éclairage des éditeurs
Nos partenariats avec un grand nombre d'éditeurs nous procurent un accès privilégié à leurs experts techniques et à leurs stratégies produits, donnant ainsi une longueur d'avance à nos CyberSOC.

Une connaissance poussée de la sécurité
La plateforme Orange Cyberdefense « Greater Intelligence » traite plus de 50 milliards d'évènements chaque mois, nous et vous offrant un accès inégalé aux menaces actuelles et émergentes. Notre équipe de consultants d'élite à l'avant-garde de la cybersécurité est en première ligne et nous éclaire sur l'état d'esprit des criminels. Nous utilisons ces informations pour garantir à nos clients la meilleure sécurité possible.

www.orangecyberdefense.com