Orange
Cyberdefense

Security Navigator 2021

Notre contribution pour construire une société numérique plus sûre

Hugues Foulon
Directeur exécutif de la stratégie et des activités de cybersécurité
Orange

Michel Van Den Berghe
Président
Orange Cyberdefense

© Orange Cyberdefense

Grâce à nos 17 SOC et 11 CyberSOC, nous avons analysé plus de 50 milliards d'alertes de sécurité chaque jour en 2020, résolu plus de 45 000 incidents et mené plus de 195 missions de réponse à incident. Nos experts internationaux ont assimilé ces informations et synthétisé leurs principales découvertes dans ce rapport à l'intention de nos clients et de la communauté cybersécurité dans son ensemble.

Nous sommes heureux de la publication de cette nouvelle édition du Security Navigator d'Orange Cyberdefense. En tant que leader européen de la cybersécurité et entité du groupe Orange, notre vision de la cybersécurité est unique.

La pandémie de COVID-19 a généré des bouleversements sans précédent sur la société et l'économie. Elle a fondamentalement transformé la façon dont nous travaillons et exerçons nos activités. Nous le voyons déjà, nombre de ces changements se transforment en améliorations durables et les états d'esprit évoluent. Une forte progression des demandes en matière de sécurité du cloud, des réseaux (via SSL) et de visioconférence a été constatée — le télétravail est là pour durer.

Cette crise prouve aussi que la liberté numérique n'est pas acquise. Elle est remise en question par des acteurs malveillants qui font de nos anciens et nouveaux espaces de connexion et de progrès des fenêtres d'attaques pour nous nuire. Chacun peut en être victime, individuellement comme collectivement : un état de fait susceptible d'affecter la confiance numérique. 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.

Jamais il n'aura été plus important de sortir de l'état de crise et de la réaction permanente pour reprendre les commandes. Il nous faut protéger la liberté et la sécurité du monde numérique, non seulement en temps de crise, mais durablement. Notre but : construire une société numérique plus sûre.

Cette année, grâce à nos 17 SOC et 11 CyberSOC, nous avons déjà analysé plus de 50 milliards d'évènements de sécurité chaque jour, résolu plus de 45 000 incidents et mené plus de 195 missions de réponse à incident.

Nos experts internationaux ont assimilé ces informations et synthétisé leurs découvertes clés dans ce rapport à l'intention de nos clients et de la communauté cybersécurité dans son ensemble.

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

Merci pour votre confiance !

Hugues Foulon
Michel Van Den Berghe

Table des matières

Introduction : Ce que vous devez savoir 6

Les statistiques du CyberSOC : Ce qu'il s'est passé 9

Des alertes aux incidents 10
Typologies d'incidents 11
L'année du COVID-19 13
Les effets du confinement 14
Une journée au bureau : les menaces le jour 16
Les menaces la nuit 17
Malwares : les tendances 18
Ransomwares 19
Types d'incidents selon la taille de l'organisation 20
Types d'incidents selon les secteurs 22
Conclusion 26

Test d'intrusion de l'IoT– Cadenas connecté au Bluetooth-LE 28

World Watch : 2020, faits marquants 31

Signalements 32
Vulnérabilités 33
Recherche des CVE : l'effet domino Vulnérabilités découvertes dans les produits de sécurité 34
L'heure des correctifs 36
Les acteurs de la menace 37
Conseils du CIS par rapport aux violations de données effectives 38
Contrôles de sécurité et défaillances 39
Conclusion 40

Ce qui a bouleversé 2020 : L'impact caché du COVID-19 43

Le comportement des attaquants 44
Les acteurs étatiques 45
Les ransomwares 46
Le comportement des utilisateurs 47
Couverture de presse et intérêt 48
Technologies de sécurité 49
Gérer la crise 50
Les priorités que nous proposons 53
Conclusion 54

© Orange Cyberdefense

Tech insight : au cœur de la cybercriminalité 57

De nouvelles réalités 58

Les places de marché 58

Malvertising, malwares, exploits, infrastructures 60

Spam et hameçonnage, informations volées, pirates 61

Botnets, blanchiment d'argent 62

Réseaux criminels : une histoire de ransomware 63

Conclusion 64

Les récits du CSIRT et du pentest 67

Un doux parfum de ransomware 68

Bonjour, je suis AD\steve-admin 70

Alerte rouge 72

Quel service de visioconférence choisir ? 75

La vidéoconférence : entre sécurité et fonctionnalités 76

Zoom 77

Tixeo, Google Meet 78

Teams, Skype for Business 79

Cisco Webex 80

BigBlueButton, Jitsi Meet 81

BlueJeans 82

Tableau récapitulatif 83

Conclusion 84

Prédictions de sécurité 87

Cybersécurité vs. menace 88

Cybersécurité vs. sécurité des données 89

Cybersécurité vs. post-COVID 90

La cybersécurité vs. sécurité physique 91

Conclusion : Qu'avons-nous appris ? 94

Sources 96

Introduction :

Ce que vous devez savoir

Laurent Célérier
EVP Marketing & Technology
Orange Cyberdefense

Security « Navigator » : pourquoi ce titre ? Ce choix renvoie, bien sûr, aux navigateurs Web, mais s'inspire aussi du monde maritime. Avant de prendre la mer, tout navigateur doit disposer de données statistiques, de conseils pratiques et de prévisions météo pour peaufiner sa trajectoire.

Avec ce document — dédié aux équipes sécurité et IT, ainsi qu'aux managers et décideurs — nous souhaitons partager notre analyse des données recueillies cette année, fournir des conseils pratiques et donner certaines prédictions cyber.

Nous espérons ainsi sincèrement vous aider à définir et établir votre stratégie de sécurité.

Notre analyse globale des écosystèmes cyber, renforcée par des données provenant de nos SOC, montre une diminution des menaces et des vulnérabilités en avril dernier, quand le confinement était généralisé. Depuis, les attaques ont repris et, dans certains cas, nous avons eu à subir une aggravation des activités de piratage. Les ransomwares comptent indubitablement parmi les vecteurs d'attaque les plus fréquents et dangereux du fait de leur haut niveau de sophistication et de leur disponibilité grandissante sur le Dark Web. Dans ce rapport, vous trouverez une analyse de l'écosystème criminel actuel.

L'année 2020 aura démontré le caractère opportuniste des attaquants. Certains équipements qui pouvaient être considérés comme accessoires — la vidéoconférence et les accès à distance, par exemple — sont devenus hautement stratégiques pour l'économie globale. Chercheurs et attaquants ont donc été poussés à s'intéresser à ces nouveaux aspects clés en informatique. Nous nous sommes penchés sur la sécurité des accès à distance dans notre premier Security Navigator. Cette année, nous partageons notre analyse sécurité des solutions de vidéoconférence.

Autre changement majeur ces derniers mois : la transition vers le cloud s'est accélérée. Flexibilité, investissement faible de départ, et adaptabilité aux contextes de télétravail ont boosté son adoption. D'ici 2023, plus de la moitié des activités informatiques seront déplacées vers le cloud alors que 75 % des sociétés sont déjà « cloud first ». Cette transformation, comme toute transformation, présente des bénéfices et des risques, en particulier lorsqu'il s'agit de sécurité.

Enfin, autre enseignement de la crise COVID : la valeur de la proximité. Bien que technologique, la cybersécurité reste, avant tout, imprégnée de la notion de confiance. Le fait d'être proche de nos clients réside au cœur de cette notion. La distribution globale de nos centres opérationnels nous aide à être là où vous avez besoin de nous. Ce besoin est d'autant plus important par temps de crise. Dans ce Navigator, nous partageons certaines expériences, des cas où nous avons eu à porter assistance à des clients affrontant des crises partout dans le monde.

Assurément, les cybermenaces persisteront. Et, de ce que nous observons, les eaux risquent de se troubler encore davantage. La crise économique et les tensions géopolitiques emboîtent le pas de la crise sanitaire. Ces déstabilisations ne peuvent que renforcer cybercriminalité et attaques étatiques.

Dans cet environnement, la place de la cybersécurité augmentera sûrement. Nous estimons que notre rôle est d'aider ceux qui cherchent à améliorer leur résilience et limiter leurs vulnérabilités. Afin qu'ils soient en mesure d'orienter leurs investissements vers les problématiques qui engendreraient le plus d'impact.

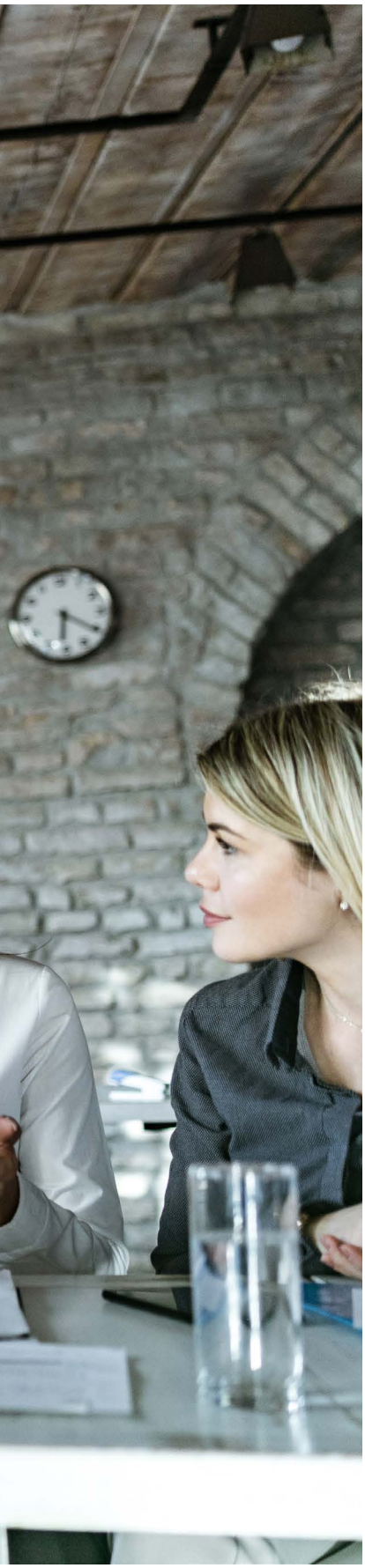
Profitons de cette période d'exception pour considérer une stratégie de sécurité différente, plus équilibrée. L'approche qui consiste à empiler les strates de protection sans les optimiser ou les gérer correctement induit un faux sentiment de sécurité… et un coût bien réel. Une sécurité forte et optimisée s'appuie sur un juste équilibre entre connaissance des menaces et vulnérabilités ; des mesures de protection adaptées et, surtout, exploitées à leur maximum ; des capacités de détection couvrant l'ensemble des outils digitaux afin d'ajuster leur configuration en permanence ; une réponse rapide et efficace pour empêcher les fuites de données et les récupérer le plus vite possible.

Cette approche équilibrée permettra de concentrer nos efforts sur les risques et menaces critiques, tout en économisant des ressources financières comme humaines.

Chez Orange Cyberdefense, nous sommes convaincus que la sécurité numérique ne saurait être atteinte sans l'engagement et les compétences des femmes et des hommes qui, chaque jour, imaginent, déploient et font fonctionner la cybersécurité. Leur rôle est essentiel dans notre société. Notre Security Navigator 2021 leur est donc dédié.

© Orange Cyberdefense

© Orange Cyberdefense



Diana Selck-Paulsson
Threat Research Analyst
Orange Cyberdefense

Charl van der Walt
Head of Security Research
Orange Cyberdefense

Les statistiques du CyberSOC

Ce qu'il s'est passé

Pour se faire une idée claire de ce qu'il se passe, il nous faut parfois prendre du recul, examiner les choses dans leur ensemble.

Et, dans le cas présent, l'ensemble est vaste : un flot continu de données transite par nos 11 CyberSOC et 17 SOC. Nous traitons des reports d'incidents en provenance de quatre continents et collectons des renseignements de la dorsale Internet d'un groupe télécom majeur, de 500 sources publiques et privées et d'une vingtaine d'agences nationales de par le monde.

Aussi, l'édition 2021 de notre Security Navigator partage (à nouveau) avec vous un panorama bien réel et de première main des évènements et tendances observés l'an passé.

Cette année aura été pour le moins particulière, la pandémie de COVID-19 ayant eu un impact sans précédent sur le monde entier. Comment cet état de fait se reflète-t-il dans les chiffres recueillis par nos SOC ? Quelles autres tendances avons-nous pu observer ?

Données clés

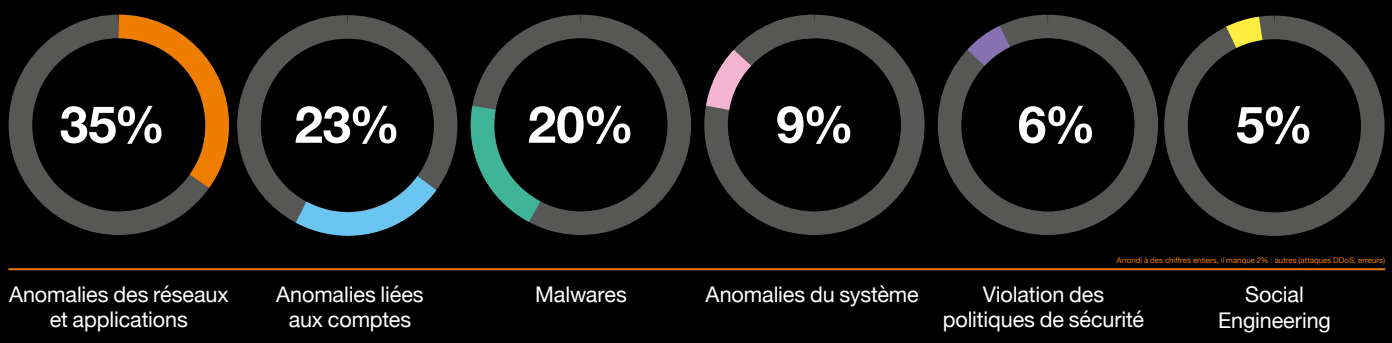
- Évènements analysés : 1 775 505
- Incidents : 45 398
- 41,65 % de ces incidents (18 910) sont confirmés comme incidents de sécurité
- Période analysée : janvier à octobre 2020.
- Sources des données : pare-feu, répertoires, proxys, terminaux, EDR, IPS, DNS, DHCP, SIEM et notre plateforme de détection des menaces.

Tunnel :
Des alertes aux incidents

1 775 505
Évènements

45 398
Incidents potentiels

18 910
Incidents confirmés (41.65%)



Les typologies d'incidents

En 2020, 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 interruption de services).

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

Ingénierie sociale : pièges affectant les utilisateurs, notamment par recours au phishing et à l'usurpation d'identité.

Une vue d'ensemble

Cette année, nous considérons un ensemble plus vaste. Le nombre de clients ayant doublé dans nos bases, nous examinons un volume d'incidents supérieur de 55 %. Les données de l'an dernier englobaient 29391 incidents confirmés issus de 263901 évènements. Cette année, nous avons traité 1775505 évènements qui ont occasionné 45398 incidents. Après les avoir analysés et avoir communiqué avec nos clients, 18910 ont été catégorisés comme de vrais incidents.

Évènements, incidents, incidents confirmés

Un point sur la terminologie : afin de classer un évènement, il lui faut remplir certaines conditions pour être considéré comme un indicateur de compromission (IoC), une attaque ou une vulnérabilité. Le label « incident » est assigné lorsqu'un évènement enregistré (ou plusieurs) est corrélé à, ou signalé par une investigation/analyse humaine (par nos analystes sécurité). Un incident est «confirmé» quand, avec l'aide du client ou à la discrétion de l'analyste, nous pouvons déterminer que la sécurité a effectivement été compromise.

Totaux

2020 est une année particulière pour notre Security Navigator. Non seulement nous avons acquis davantage de clients grâce auxquels nous disposons de plus de données pour travailler, mais nous pouvons aussi nous appuyer sur un ensemble plus vaste d'opérations menées par Orange Cyberdefense pour nos clients à l'échelle mondiale.

Notre ensemble de données a augmenté organiquement de 14,11 % depuis l'an dernier, pour englober 33540 incidents. Notre nouvel ensemble compte 45398 incidents issus de 9 CyberSOC.

Cet ensemble unique de données nous permet d'explorer diverses questions :

- Quels ont été les changements majeurs depuis l'an dernier ?
- Quel a été l'impact du COVID-19 et des confinements sur les incidents de sécurité ?
- Que nous apprennent ces informations sur le comportement des attaquants ?
- Que se passe-t-il sur vos systèmes quand votre équipe sécurité n'est pas à l'œuvre ?
- Pourquoi moins de ransomwares, et pas plus ?
- Pourquoi tant d'adwares en mars 2020 ?

Comment les modèles variant-ils entre petites et grandes organisations, et selon les secteurs d'activité ?

Sur les 45398 incidents dans nos données de janvier à octobre 2020, nos analystes ont confirmé 18910 incidents comme « vrais-positifs ». Ce qui ne veut pas dire que les autres étaient tous des faux-positifs. Certains des incidents que nous traitons sont définis comme avérés, mais bénins et notés comme « vrais légitimes » (« true legitimate »). Certains, aussi, ne peuvent être correctement catégorisés.

Cette année, 41,65 % des incidents étaient confirmés comme « vrais-positifs », 35 % étaient des faux-positifs, 20 % étaient légitimes et les 4 % restants n'ont pu être catégorisés.

© Orange Cyberdefense

Les tendances en matière de détection

Les anomalies réseau et application (35 %) ont été les incidents les plus détectés en 2020, suivies des anomalies sur les comptes utilisateurs (23 %) et des malwares (20 %).

Alors que les anomalies sur les comptes utilisateurs (22 % en 2019) et malwares (20 % en 2019) suivent une tendance similaire à celle observée dans le précédent ensemble de données, les anomalies réseau et application (35 % en 2020) semblent avoir régressé assez significativement par rapport à l'an dernier (46 %). Nous avons détecté davantage d'incidents classés sous ingénierie sociale (5 % en 2020 contre 1 % en 2019) et transgression des politiques de sécurité (6 % en 2020 contre 3 % en 2019). Ceci s'explique en partie par le volume supérieur de données à notre disposition cette année, mais il existe aussi des changements perceptibles dans cet ensemble.

Dans toutes les régions, nous avons remarqué un volume supérieur d'incidents liés à l'ingénierie sociale sur les deux dernières années (2 % en 2018, 1 % en 2019 et 5 % en 2020). Ceci inclut les campagnes de phishing, soit par envoi massif d'e-mails, soit par le biais d'attaques plus ciblées de spear phishing, ainsi que les courriers indésirables (spams) et autres cas d'extorsion.

Les transgressions de politiques de sécurité sont plus souvent détectées dans les grandes organisations pour la simple raison qu'elles ont tendance à mettre en place davantage de politiques. Cette année, nous avons constaté que 2 % des incidents étaient confirmés comme des transgressions des politiques de sécurité dans les petites entreprises, contre 3 % dans les groupes de taille moyenne et 13 % dans les grands comptes.

Cette répartition diffère quelque peu si l'on se concentre uniquement sur les incidents confirmés. Les anomalies réseau et application restent en tête (34 %), suivies des malwares (23 %), puis des anomalies sur les comptes utilisateurs. En d'autres mots, nous voyons plus d'incidents malware confirmés que d'anomalies sur les comptes utilisateurs (18 %), bien que ces anomalies soient remontées plus souvent pour être triées.

Dans l'ensemble, le nombre d'incidents traités par nos CyberSOC au niveau mondial a sensiblement progressé cette année.

L'année du COVID-19

Les données disponibles suggèrent qu'au sommet de la crise en mars, 17 pays dans notre champ opérationnel avaient appliqué des mesures de confinement. Nous remarquons que le volume total des incidents traités a chuté de 12 % quand les confinements ont été mis en place, avant de remonter significativement en mai. Alors que les entreprises européennes reprenaient leurs activités «normales» en juin, le nombre d'incidents a augmenté de 15 %, pour régresser à nouveau du fait de la période des vacances estivales en Europe, en juillet-août.

L'impact de la pandémie sur les activités métier est notable. Selon les données de l'Office for National Statistics britannique, seuls 66 % des entreprises britanniques étaient opérationnelles et 30 % des forces de travail étaient en congé durant la première moitié de juin. En septembre, ces deux chiffres ont régressé à 47 % et 9 %, respectivement.

En France, où le confinement était en place de mi-mars à mi-avril, les volumes d'incidents ont chuté de 30 % entre mars et mai. En Suède, où il a été choisi de ne pas appliquer de confinement général, les volumes n'ont baissé que de 3 %, puis 8 % en avril.

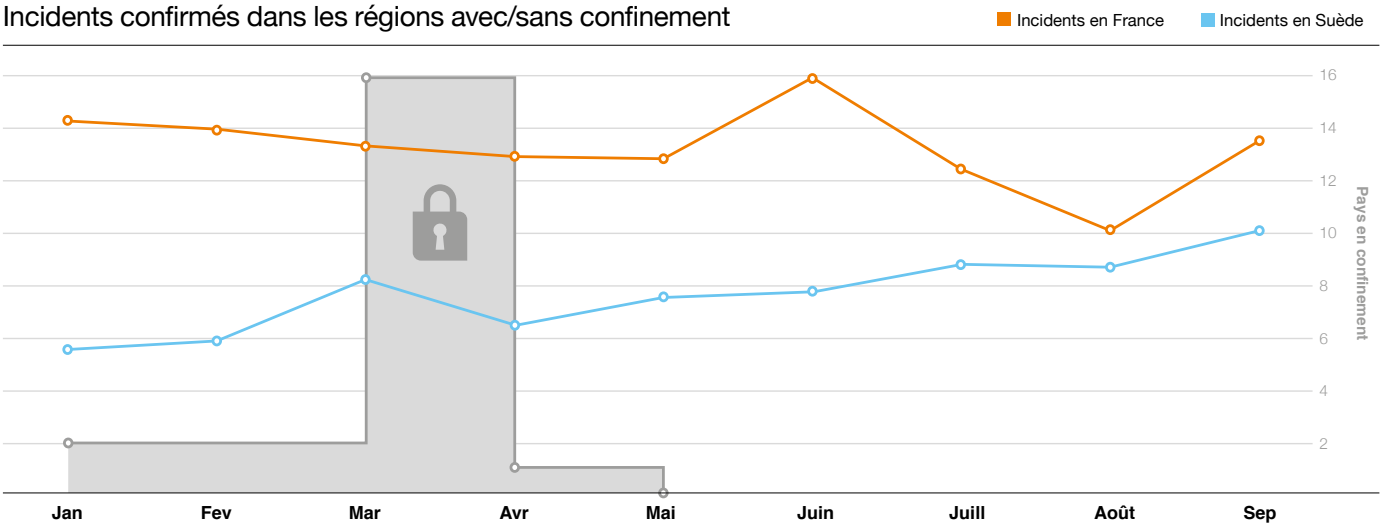
L'impact de ces facteurs sur les volumes d'incidents n'est, toutefois, pas toujours immédiatement évident. Après une période de congés, il n'est pas rare de constater une augmentation des échecs de connexion — qui peut sembler malveillante, sans l'être réellement. Durant les confinements, nous avons aussi vu diminuer l'appétence au changement, d'où moins de changements au niveau des AD et moins d'incidents par élévation de privilèges.

Quand les entreprises ont renoué avec une activité normale en septembre, nos centres ont observé une augmentation de 18 % du nombre d'incidents par rapport au niveau le plus bas de mai.

L'autre question soulevée par cette évolution : le comportement des attaquants a-t-il aussi été impacté par les confinements et le ralentissement général liés à la pandémie ? À nouveau, pour y répondre, nous pouvons nous pencher sur les différences de volumes observées chez nos clients basés en France et en Suède, mais, cette fois, en ne considérant que les évènements confirmés comme malveillants.

Effets du confinement sur le nombre d'incidents

Incidents confirmés dans les régions avec/sans confinement



Pour les incidents confirmés en France, nous voyons que l'impact initial du confinement était toujours sévère — avec une diminution de 27 % de mars à avril — mais que la différence nette entre mars et mai n'était que de 9 %, plus proche des 4 % de diminution en Suède.

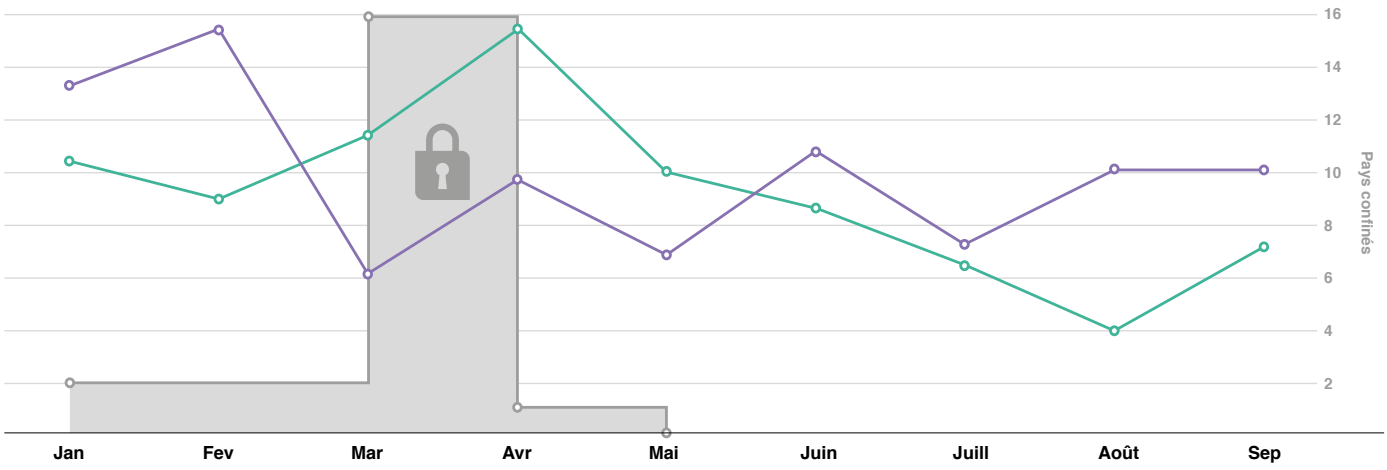
Alors, quel a été l'impact de la COVID-19 sur le comportement des attaquants ?

La question de l'impact global de la pandémie sur la sécurité est traitée dans un chapitre dédié — COVID-19 : L'impact caché. Pour l'heure, il est possible d'en avoir un aperçu en comparant les incidents pour lesquels l'attaque nécessite une interaction avec un utilisateur et ceux pour lesquels l'attaquant peut agir seul.

Nous pouvons déjà conclure que le ralentissement général lié à la COVID-19 a eu un impact marqué sur les volumes d'incidents traités par nos CyberSOC avant, pendant et après les périodes de confinement, mais un impact moindre sur le comportement des attaquants.

Nombre d'incidents liés à une interaction avec l'utilisateur

Comparaison des incidents qui nécessitent ou non une interaction avec l'utilisateur



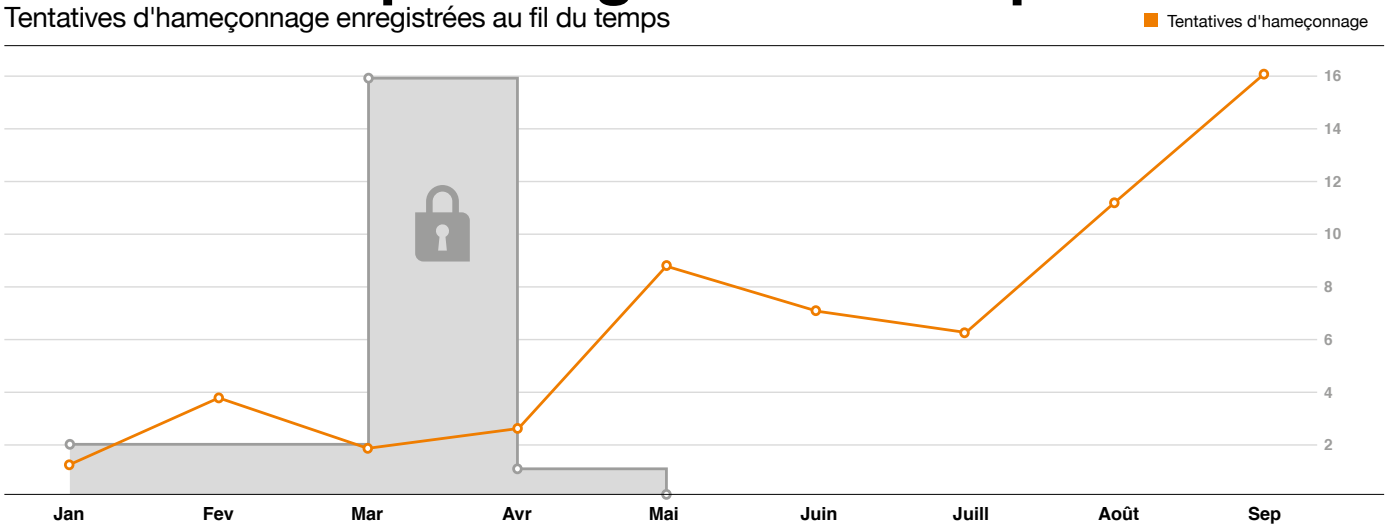
En comparant les incidents confirmés comme malveillants qui impliquent un utilisateur (téléchargements de fichiers) et ceux durant lesquels l'attaquant agit indépendamment (tentatives d'accès à un serveur externe), nous constatons que le volume d'incidents détectés sous la catégorie ingénierie sociale suit, sans surprise, les niveaux d'activité métier. Les attaques indépendantes au cours de la période de confinement ont suivi un tracé bien différent, augmentant considérablement pendant les confinements, avant de retrouver des niveaux plus «normaux» à partir de juin.

La même courbe se dessine pour les incidents liés au phishing dans le graphique suivant.

Outre une progression marquée des attaques par phishing détectées pendant l'année, un motif récurrent dans notre examen des périodes de confinement s'impose encore une fois. Un pic, bref certes, mais important, est perceptible dans l'activité des attaquants au sommet de la pandémie, bien que cette activité soit rapidement «revenue à la normale». Il est intéressant de voir que l'activité de phishing a légèrement ralenti pendant l'été en Europe, suggérant que les attaquants — conscients qu'il s'agit d'une période de vacances — réduisent leurs propres niveaux d'activité en conséquence.

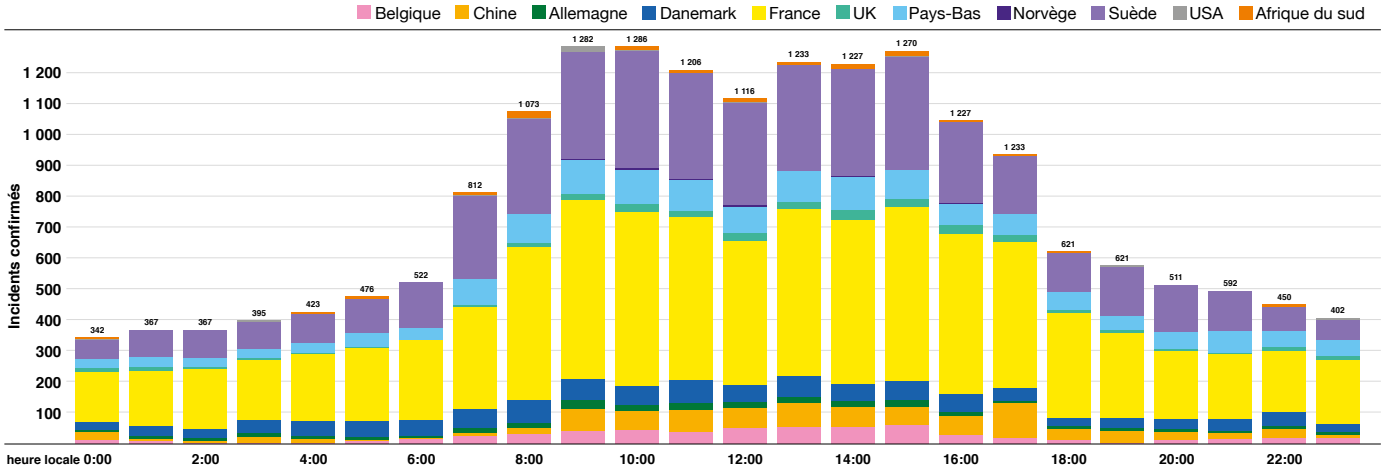
Incidents de phishing au fil du temps

Tentatives d'hameçonnage enregistrées au fil du temps



© Orange Cyberdefense

Nombre d'incidents en fonction de l'heure de la journée



Un jour au bureau

Sachant que les volumes d'incidents ont été influencés par des évènements qui affectent le comportement des utilisateurs, nous examinons les modifications dans les incidents au cours d'une journée. Pour cela, nous ajustons l'horodatage de tous les tickets d'incidents afin de refléter l'heure dans leur fuseau horaire.

En dépit de variations minimes et prévisibles liées aux modes de travail locaux, le volume d'incidents suit parfaitement les horaires habituels de travail des cibles. Ceci ne tient pas seulement au «bruit» généré par les systèmes de détection, puisque les données reflétées plus haut décrivent uniquement des incidents vérifiés. Nous confirmons cette hypothèse en examinant le partage des codes de fermeture d'incidents au fil de la journée : pas de baisse visible des volumes de faux-positifs après les heures de bureau.

En examinant les étapes clés dans une journée — avant le travail, pendant la matinée, au déjeuner, dans l'après-midi et après le travail — il est clair que les volumes de faux-positifs liés au phishing sont purement fonction de l'activité des utilisateurs. Plus il y a d'utilisateurs actifs, plus nous en constatons. Les vrais-positifs suivent un schéma un peu différent. Une observation, somme toute logique : ils arrivent plus fréquemment au début et à la fin de la journée (plutôt que pendant la pause déjeuner).

Une observation moins prévisible, toutefois : proportionnellement, plus de vrais-positifs de phishing sont constatés entre minuit et 3 heures du matin, et après 18 heures (bien qu'un peu moins).

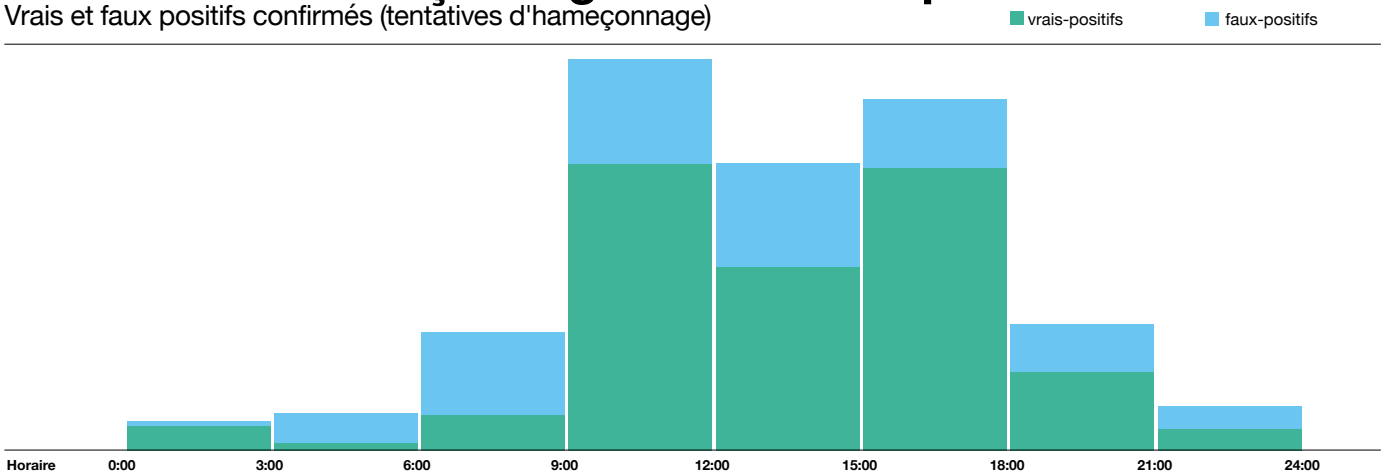
Il est évident que le nombre total d'incidents est moindre dans ces créneaux (d'où, moins de faux-positifs), mais cela peut aussi vouloir dire que les utilisateurs, réveillés et en ligne à ces heures tardives, sont peut-être fatigués et plus susceptibles de succomber à des arnaques.

Les données suggèrent que le volume d'incidents dépend du comportement des utilisateurs. En d'autres mots, plus d'attaques sont menées lorsque l'activité est intense. Certaines catégories d'attaques peuvent, néanmoins, être exécutées indépendamment de cette activité. Cette corrélation est peut-être moins surprenante, mais nous jugeons intéressant de noter à quel point c'est le cas.

Si le volume d'incidents est d'abord corrélé au niveau d'activité des utilisateurs, qu'est-ce qui définit alors la «forme» de ces incidents, à savoir, la combinaison de plusieurs catégories d'incidents ? Cette combinaison est-elle uniforme, quelle que soit l'heure de la journée ? Est-ce qu'elle varie quand les utilisateurs se déconnectent ?

Tentatives d'hameçonnage au fil du temps

Vrais et faux positifs confirmés (tentatives d'hameçonnage)



© Orange Cyberdefense

Au cœur de la nuit

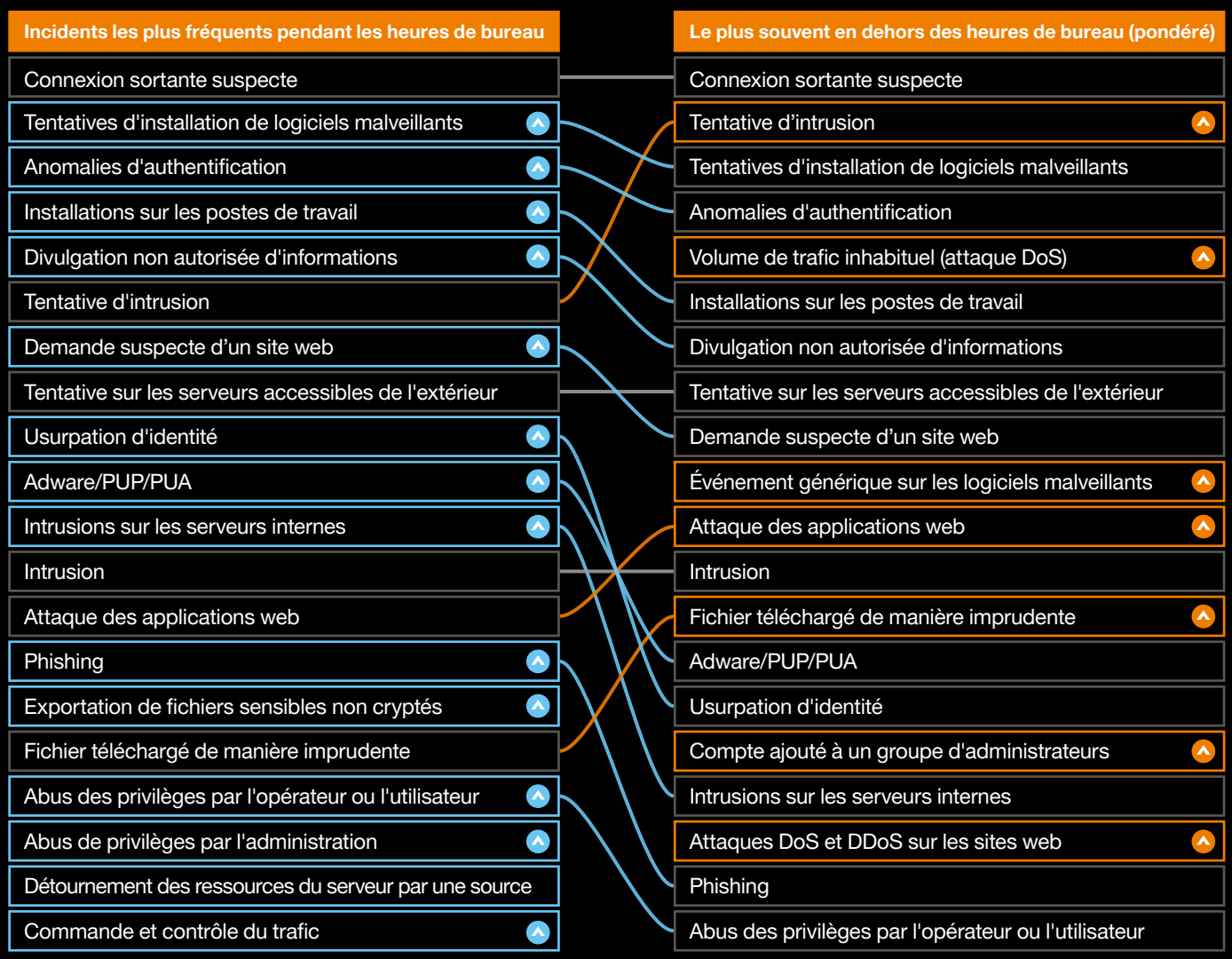
Du fait du «bruit» additionnel induit par des niveaux supérieurs d'activité utilisateurs, nous nous attendrions à voir de plus forts taux de faux-positifs pendant les heures ouvrées. Mais, apparemment, ce n'est pas le cas. La proportion de faux-positifs est marginalement plus haute en dehors de ces horaires. Cependant, les incidents notés comme « vrais légitimes », soit des évènements vérifiés, mais bénins, sont plus fréquents pendant les heures de travail. Les taux d'activité utilisateurs sont donc supérieurs pendant les heures de bureau, il en va de même pour leurs taux d'erreurs. En dehors de cela, la répartition des statuts d'incidents reste pour l'essentiel la même au cours de la journée.

Nos données illustrent la même observation pour la répartition des catégories d'incidents. Si l'on compare la répartition pendant les heures de bureau et les heures non ouvrées, les motifs sont très semblables, outre quelques infimes variations çà et là. Par exemple, les incidents liés aux malwares sont plus représentés après les heures de bureau (22 %) que pendant (19 %).

Du point de vue de l'impact pondéré (Impact Weighted) — qui donne une idée plus claire de ce qu'un incident représente pour une organisation donnée — quelques caractéristiques se démarquent :

1. Les incidents liés aux malwares sont plus représentés hors heures ouvrées (22 %) que pendant (19 %).
2. Les 5 types d'incidents les plus courants pendant les heures de bureau sont aussi les plus fréquents (dans le top 5 ou 6 des problèmes les plus communs).
3. La catégorie "tentative d'intrusion" est la seconde plus importante du point de vue de l'impact pondéré, mais n'apparaît pas dans le top 20 des deux autres listes.
4. Les incidents liés à des dénis de service ne figurent au top 20 que si l'on considère l'impact pondéré des incidents hors des heures de bureau.

Le graphique ci-dessous montre que le top 5 des catégories d'incidents confirmés pendant les heures ouvrées s'illustre aussi au top 6 des catégories confirmées hors heures ouvrées, mais elles surviennent en moyenne 45 % moins souvent.



Nous en concluons que le volume d'incidents que nous traitons est d'abord lié aux utilisateurs, alors que leur type reflète le comportement des attaquants. Les attaquants peuvent aussi avoir à se tenir à des horaires de travail, des routines et des schémas. Cependant, pour l'essentiel, le comportement des attaquants ne devient manifeste que lorsqu'il coïncide avec la connexion et l'activité des victimes. Et, certaines attaques se déroulent hors des heures ouvrées, voire même principalement après les heures de bureau.

Il est donc clair qu'aucune entreprise ne peut se permettre de baisser sa garde quand ses salariés sont inactifs.

Malware : les tendances

Nous avons repéré une légère augmentation du nombre d'incidents liés à des malwares entre janvier et octobre 2020.

Cette année, les ransomwares s'imposent comme une tendance forte, qui aura perturbé les organisations toutes industries confondues. Des acteurs qui se spécialisaient dans d'autres formes de cybercriminalité ont vu qu'il était possible de dégager un bénéfice des ransomwares et se sont adaptés. Emotet en est un exemple : il avait débuté comme cheval de Troie bancaire, mais a récemment fait évoluer son modèle économique pour se consacrer presque exclusivement à la distribution et aux infections par malwares, via des campagnes de spams. Emotet est généralement considéré comme un cheval de Troie, un Downloader ou un Dropper, mais l'accès illégal fourni par les infections est ensuite vendu à des tiers, dont des opérateurs de ransomwares qui le monétisent. Ce modèle est connu sous le nom de Malware-as-a-Service (MaaS). Les acteurs tels qu'Emotet constituent un important maillon de la chaîne d'approvisionnement qui a réussi aux opérateurs de ransomwares. (Pour plus de détails sur l'agilité des modèles économiques retenus par les opérateurs de malwares, voir le chapitre sur la cybercriminalité.)

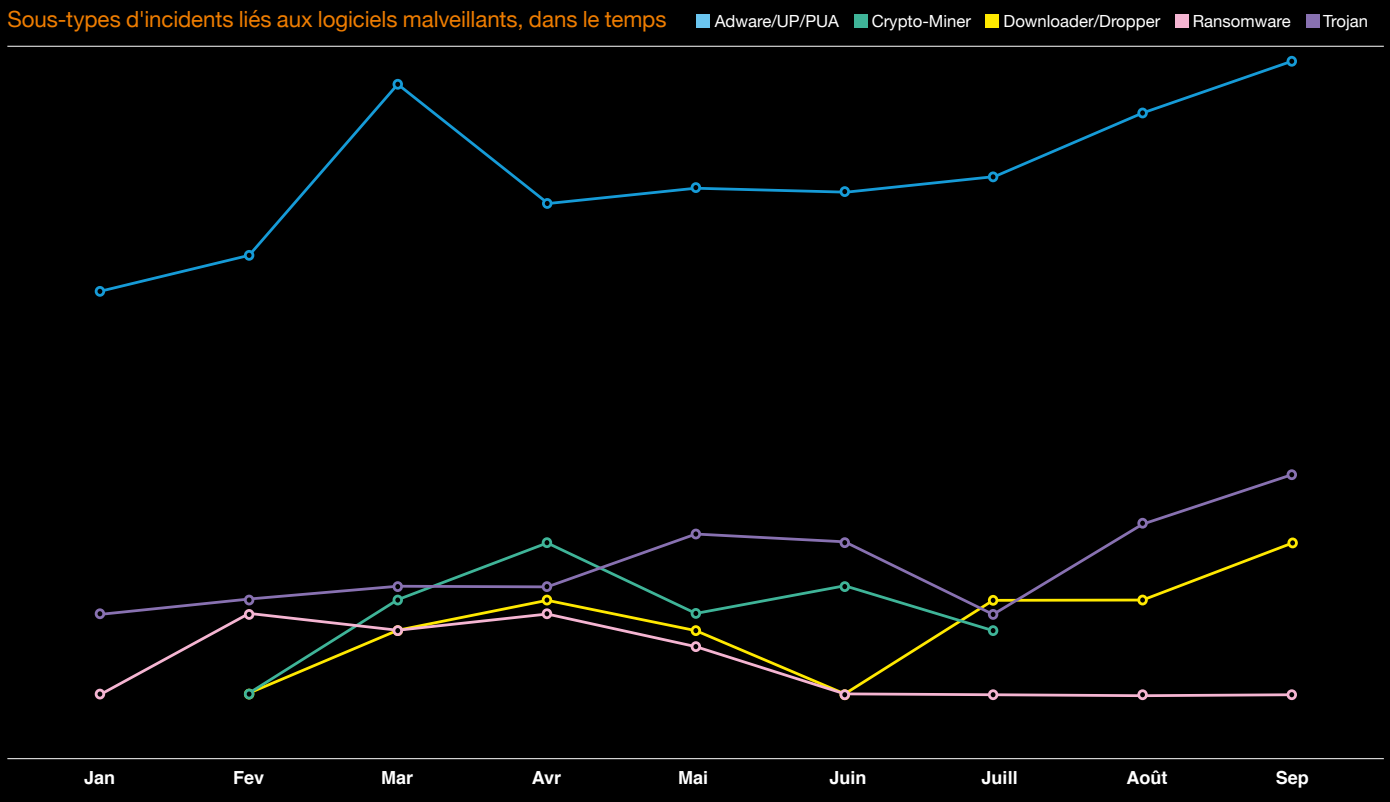
Détection de ransomwares : des particularités

L'an passé, nous avons enregistré très peu d'incidents liés à des ransomwares confirmés chez nos clients. Pourquoi ? Le chiffrement des données par ransomware est généralement la dernière étape d'une stratégie d'infection par malware — l'ultime phase d'une compromission qui est déjà passée par plusieurs étapes d'exploitation. Les opérateurs de malwares extraient toute valeur du terminal infecté avant de lancer le chiffrement et de révéler leur présence.

En juillet, les chercheurs et la presse technologique ont signalé qu'Emotet — peut-être le botnet le plus coûteux et le plus destructeur au monde — avait refait surface après, semble-t-il, une pause, et reprenait ses marques dans le paysage cybercriminel. Nos données montrent que nous avons détecté des incidents liés à Emotet chez des clients de nos CyberSOC. Bien que le nombre d'incidents soit faible, il donne une idée de la tendance. Le nombre d'incidents en lien avec Emotet a continué d'augmenter depuis le début d'année. L'augmentation est surtout plus marquée depuis la fin de l'été (européen), en phase avec les tendances constatées pour le paysage dans son ensemble.

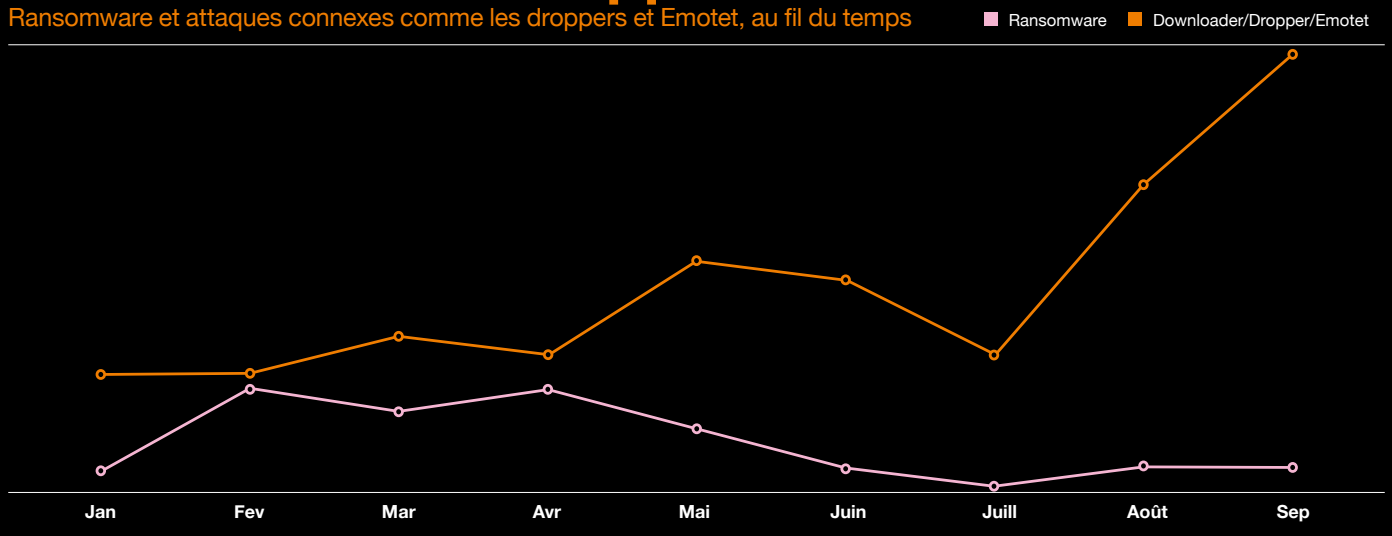
Tendances en matière de malwares

Sous-types d'incidents liés aux logiciels malveillants, dans le temps



Ransomware vs. droppers

Ransomware et attaques connexes comme les droppers et Emotet, au fil du temps



La taille des organisations

Les incidents constatés chez nos clients sont catégorisés selon leur échelle organisationnelle :

1. Petite (101 à 1 000 employés),
2. Moyenne (1 001 à 10 000 employés),
3. Grande (10 000 à plus de 200 000 employés).

La proportion d'incidents détectés dans de petites entreprises passe à 14 % (vs 10 % en 2019). Les organisations de taille moyenne représentent le même pourcentage qu'antérieurement (31 % en 2019). La proportion d'incidents détectés pour les grandes organisations a, quant à elle, continué de baisser pour atteindre 55 % (contre 58 % en 2019, et 73 % en 2018).

Il n'est pas surprenant de voir les grandes organisations afficher les volumes d'incidents les plus élevés, suivies des organisations de taille moyenne puis des petits groupes. Si l'on normalise notre perspective en donnant à chaque incident un poids reflétant sa proportion dans l'ensemble des incidents pour un client, nous constatons que les entreprises de taille moyenne pèsent le plus dans ces statistiques, suivies des petites organisations, puis des grands groupes. Ceci s'explique par le fait que nous comptons plus d'entreprises de taille moyenne parmi nos clients que de groupes d'autres tailles.

Cette tendance est aussi notable au fil du temps : les organisations de taille moyenne et les grands groupes ont constaté une baisse assez importante de leurs volumes d'incidents en juin, tandis que les petites entreprises ont vu augmenter leur nombre d'incidents confirmés.

Malware : petits et grands

Les tendances relatives aux malwares diffèrent en fonction de la taille des organisations. Notamment, les incidents liés aux malwares au sein des petites et moyennes entreprises ont progressé au fil du temps, tandis que les organisations de plus grande taille ont vu le nombre de cas régresser après un pic en mars et en avril cette année.

En y regardant de plus près, nous voyons se dessiner une tendance particulièrement intéressante, les petites organisations subissent plus d'incidents liés à des malwares, confirmés, catégorisés comme chevaux de Troie, ver, backdoor/RAT (porte dérobée/outil d'accès distant) ou ransomwares. Suivent les entreprises de taille moyenne et les grands groupes. Les entreprises de taille moyenne, quant à elles, présentent un taux supérieur d'incidents confirmés catégorisés sous piratage de cryptomonnaies et kits d'exploitation. Et les grands groupes constatent davantage d'incidents catégorisés comme « virus », et le second taux le plus haut d'adwares et de programmes et applications indésirables (Potentially Unwanted Programs or Applications PUP/PUA).

Les individus sous pression

Cette année, nous avons constaté un fort taux d'incidents confirmés impliquant l'installation d'adwares et de PUP/PUA. Ces incidents représentent 60 % de l'ensemble des détections malware confirmées. La plupart des incidents impliquent l'installation par des utilisateurs de programmes ou d'extensions indésirables (outils de décompression de fichiers .zip, extensions pour navigateurs qui envoient les données utilisateurs à des entités externes, torrents, etc.).

Une augmentation particulière a été observée pour les incidents liés aux adwares et PUP/PUA en mars dernier. Elle est cohérente avec la tendance constatée en matière d'activité malware : un pic en mars, puis à la fin de l'été, moment où nous avons aussi vu progresser le nombre d'incidents confirmés en général. Le pic de mars pourrait s'expliquer par le fait qu'un grand nombre d'employés avaient commencé à travailler de chez eux. Ils auraient alors pensé qu'il leur fallait installer des applications gratuites, bien que non-approuvées, pour s'adapter à leur nouvelle réalité et maintenir leur charge habituelle. Cette tendance a été plus notable chez les entreprises de petite et moyenne taille.

Types d'incidents selon la taille de l'organisations

Comme l'an passé, nous avons constaté que les organisations de taille moyenne montrent un plus grand nombre d'anomalies réseau et application que les petits et grands groupes. Près de la moitié (49 %) de l'ensemble des incidents détectés était catégorisée sous anomalie réseau et application chez les moyennes entreprises. Dans les petites et grandes organisations, la répartition a changé, mais les anomalies réseau et applications restent les incidents les plus détectés.

Nous avons détecté une augmentation de 13 % des confirmations d'incidents malware chez les petites organisations (24 % en 2020 contre 10 % en 2019), et de + 9 % chez les organisations de taille moyenne (22 % en 2020 contre 13 % en 2019). Il semble que les organisations de petite et moyenne taille ont «rattrapé leur retard» sur les grands groupes et subissent aussi la tendance malware.

Si l'on considère les incidents confirmés en 2020, les malwares s'imposent ainsi comme le second type d'incident le plus répandu, touchant les organisations de toutes tailles. En 2019, la catégorie anomalie au niveau des comptes se classait deuxième pour les petites et moyennes organisations.

Il est également intéressant de noter que plus l'organisation est petite, moins, proportionnellement, elle présente de faux-positifs sur les incidents liés à des malwares. Les petites organisations montrent un volume de détection des malwares sensiblement plus bas que les moyennes et grandes organisations, mais, proportionnellement, bien moins de faux-positifs. Une théorie explique ce constat : les grandes organisations mettent en œuvre des capacités de détection pour diverses que les petites afin de remédier aux lacunes qu'elles peuvent discerner dans leur détection des malwares. Ces capacités supplémentaires améliorent l'efficacité de leurs programmes de détection. Aussi, nous détectons davantage de problèmes, mais certaines des fonctionnalités sont moins efficaces : produisent plus de faux-positifs par rapport à ce qu'elles trouvent. Comme les organisations de plus grande taille ajoutent des fonctionnalités plus diverses à leurs programmes de détection de malwares, leur «efficacité» décroit : leur bénéfice est donc moindre.

Une autre théorie consiste à dire que les organisations de plus grande taille ont une surface d'attaque plus importante, qui les expose à davantage de campagnes d'e-mails de phishing ou de spams. La probabilité que quelqu'un clique sur un lien malveillant est donc plus élevée du simple fait d'un plus grand nombre d'employés. La raison pour laquelle les grandes organisations subissent plus de faux-positifs peut ainsi s'expliquer par la plus grande probabilité qu'un utilisateur clique sur un lien suspect. Plus d'utilisateurs veut dire plus de risques qu'ils interagissent avec des liens malveillants ou suspects. D'où, un nombre plus important de sites potentiellement malveillants, qui une fois étudiés ne s'avèrent pas malveillants, simplement des faux-positifs.

Avec les malwares, cependant, le coût d'une infection dépasse de loin le coût de l'analyse d'un faux-positif. Et c'est encore plus vrai dans le nouveau monde des «extortionware». En somme, le coût d'un faux-négatif est infiniment plus grand que celui d'un faux-positif.

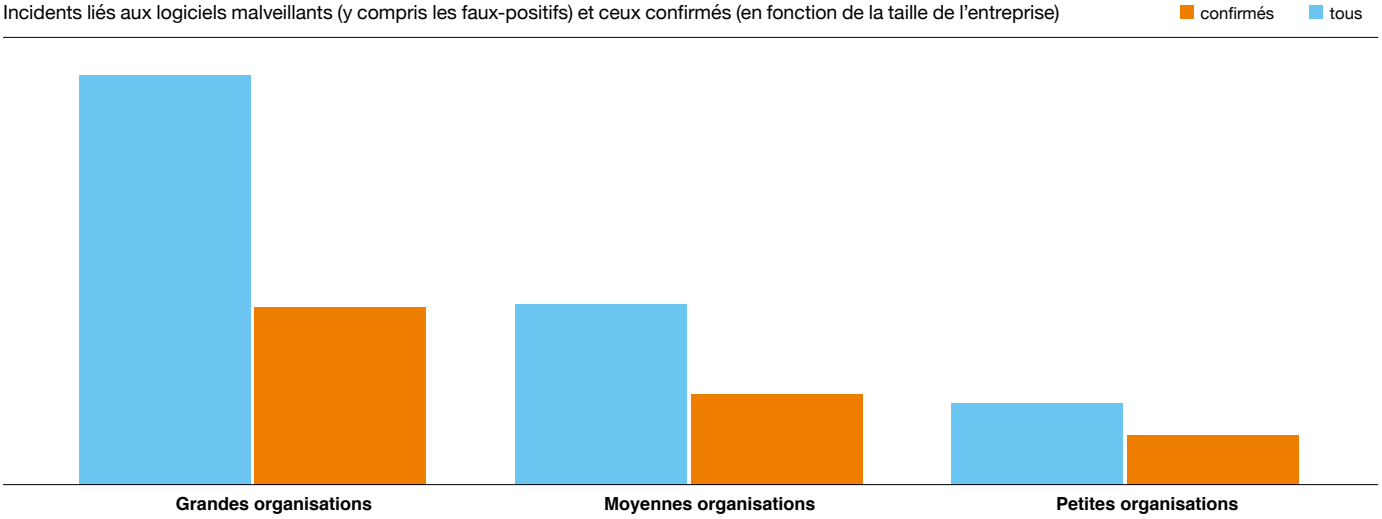
Volume par organisation en fonction de leur taille

Nous avons enregistré, en moyenne, environ 101 (contre 63 en 2019) incidents confirmés par entreprise pour les petits groupes durant les 9 mois couverts par ce rapport. Cette moyenne pour les organisations de taille moyenne est de 77 (266 en 2019) et de 278 pour les grandes organisations (463 en 2019). Il n'est pas surprenant que les grands groupes présentent le plus d'incidents, mais il est un peu inattendu d'en voir autant chez les petites organisations que chez les organisations de taille moyenne.

Cette année, certains de nos clients dont les entreprises sont de taille moyenne ont eu à subir un nombre très faible d'incidents confirmés. Un bon signe, somme toute, qui a conduit à une baisse globale des taux d'incidents confirmés par organisation d'une année sur l'autre.

Les vrais positifs par rapport à l'ensemble des incidents liés aux malwares

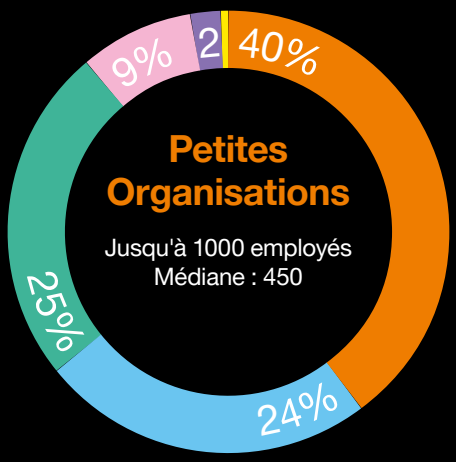
Incidents liés aux logiciels malveillants (y compris les faux-positifs) et ceux confirmés (en fonction de la taille de l'entreprise)

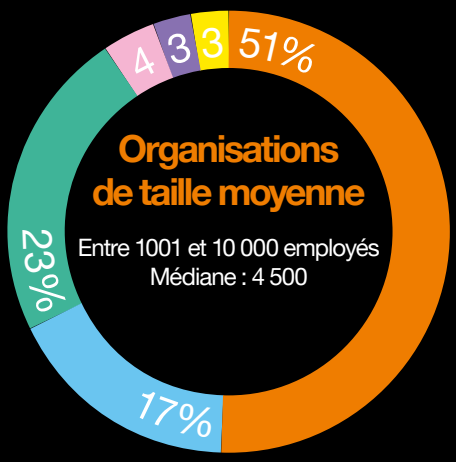


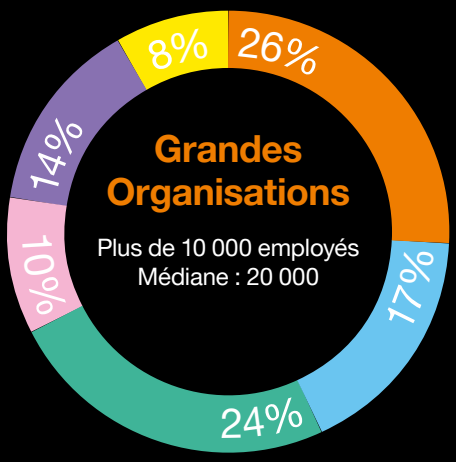
© Orange Cyberdefense

Incidents selon la taille de l'entreprise

Réseau | Anomalies des comptes | Malware | Anomalies système | Violation des politiques | ingénierie sociale





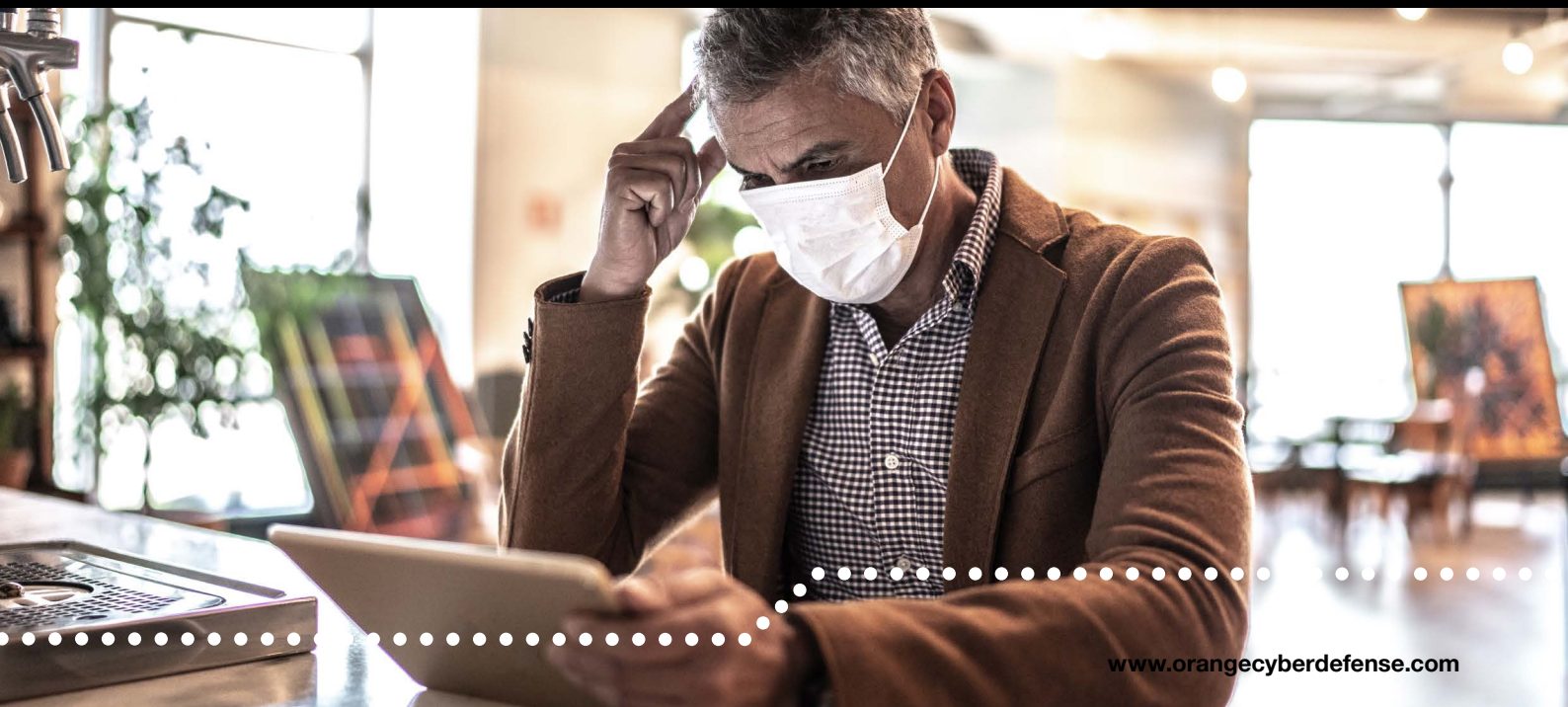


Incidents

par organisation dans chaque catégorie

Cette année, certains de nos clients dont l'entreprise est de taille moyenne ont eu à subir un nombre très faible d'incidents confirmés. Un bon signe, somme toute, qui a conduit à une baisse globale des taux d'incidents, confirmés par entreprise d'une année sur l'autre.

Petites Organisations	Moyennes Organisations	Grandes Organisations
101	77	278



Les incidents selon les secteurs d'activité

Comment sont répartis les incidents selon des secteurs d'activité ?
Nous avons analysé sept industries et avons été surpris des différences observées.

Les pourcentages les plus hauts de ces graphiques ne veulent pas simplement dire que des incidents arrivent plus fréquemment et que le secteur est plus «vulnérable». Ils peuvent en effet indiquer l'inverse. La capacité d'identifier un incident peut signifier une grande maturité en matière de sécurité. Par exemple, dans la finance les «volumes» d'ingénierie sociale à des fins de fraude sont élevés, puisque les institutions financières montrent une plus grande maturité dans la gestion de ces incidents et sont capables d'en détecter et d'en remonter davantage.

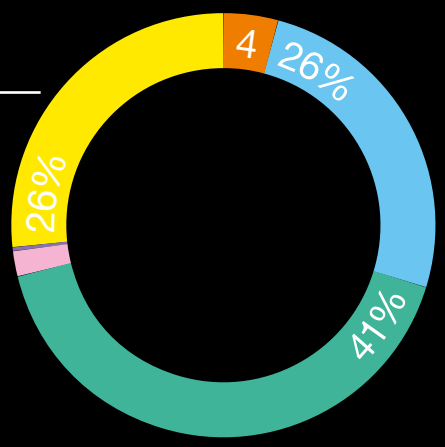
Répartition des incidents par secteurs

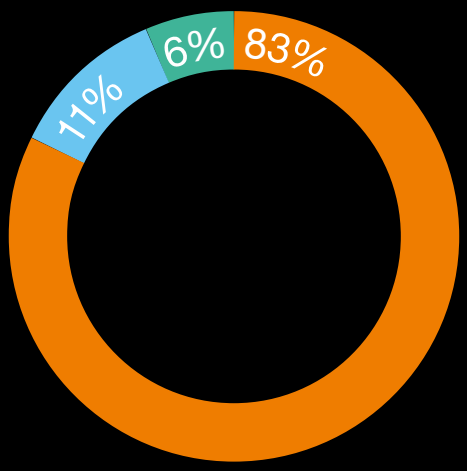
Confirmés, vrais-positifs uniquement

	Réseau	Comptes	Malware	Système	Politique	Ingénierie	DoS
Herbergement et restauration	4,20%	25,61%	41,19%	1,76%	0,27%	26,42%	0,00%
Education	82,50%	11,25%	6,25%	0,00%	0,00%	0,00%	0,00%
Finance et assurance	37,15%	19,30%	19,57%	5,07%	4,03%	10,92%	2,27%
Soins de santé	81,01%	12,37%	5,52%	0,24%	0,08%	0,08%	0,00%
Industrie manufacturière	29,10%	21,26%	26,54%	10,98%	9,50%	1,73%	0,00%
Services scientifiques et techniques	45,91%	23,06%	15,72%	3,46%	1,99%	7,23%	0,42%
Administration publique	38,27%	3,40%	25,31%	6,79%	24,69%	0,00%	0,00%
Immobilier, location et leasing	11,24%	23,34%	27,95%	30,84%	6,05%	0,00%	0,58%
Commerce	29,97%	12,86%	23,33%	6,20%	13,20%	6,89%	0,35%
Transport et entrepôts	40,28%	20,83%	19,64%	15,67%	3,17%	0,00%	0,00%

Hôtellerie et restauration

Ce secteur se démarque avec 41 % d'incidents confirmés comme des malwares, suivis du plus haut taux d'ingénierie sociale (26 %). Une raison possible à cela : ces deux types d'incidents vont souvent de pair. L'ingénierie sociale est utilisée comme vecteur d'attaque (via phishing, vhishing etc.) et, après plusieurs étapes, mène à des infections par malwares.



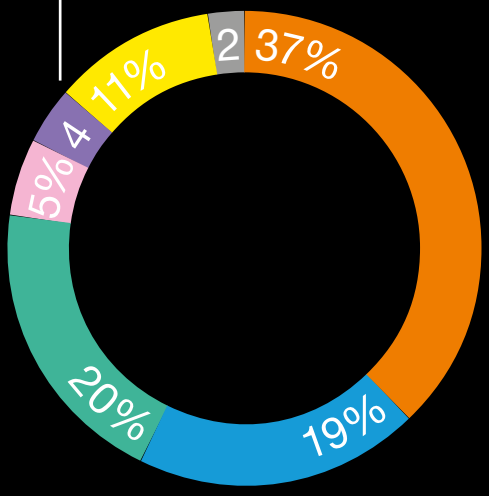


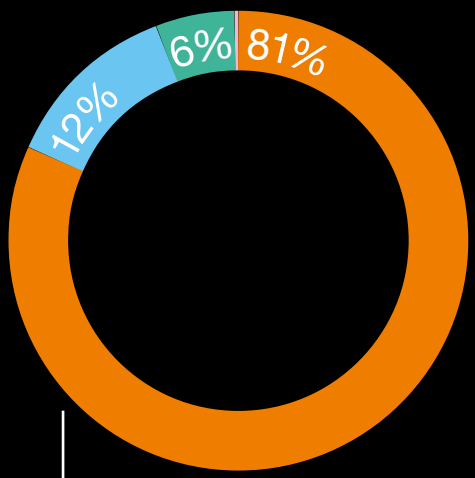
Education

Le secteur de l'éducation montre un fort taux d'anomalies du réseau et des applications confirmées. Cette industrie présente surtout des connexions sortantes suspectes. Nous avons enregistré plus d'incidents confirmés en mars et en juin. Autrement, les volumes d'incidents étaient assez bas, peut-être du fait des confinements et de leur impact sur l'activité numérique.

Finance et assurance

Le secteur de la finance continue de présenter de plus forts taux d'incidents confirmés liés à l'ingénierie sociale que la majorité des autres secteurs, en particulier les incidents confirmés de phishing. Cette année, nous avons aussi détecté des attaques par déni de service ciblant cette industrie : aucun autre secteur n'a présenté autant d'attaques DDoS. Pour mettre cela en perspective, le nombre absolu est encore assez bas. Les incidents dans cette industrie suivent la tendance générale. Plus d'incidents sont survenus au cours du premier trimestre, période suivie d'une baisse en avril et, particulièrement, en mai, avant que les volumes ne remontent en juin et en juillet.



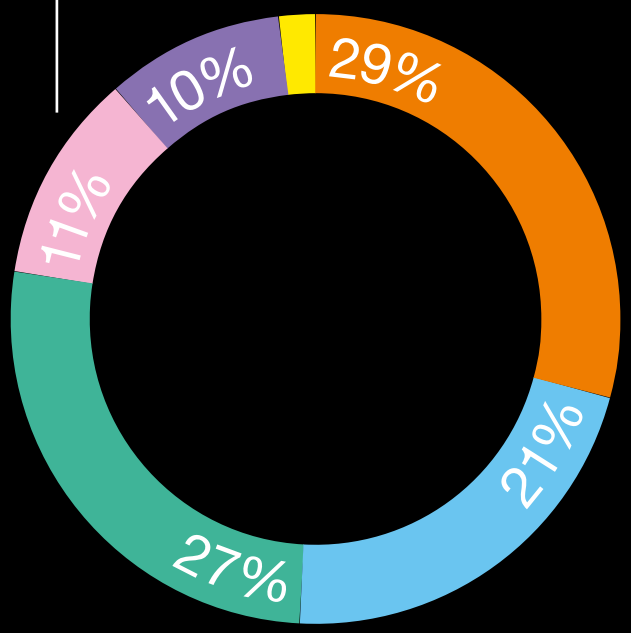


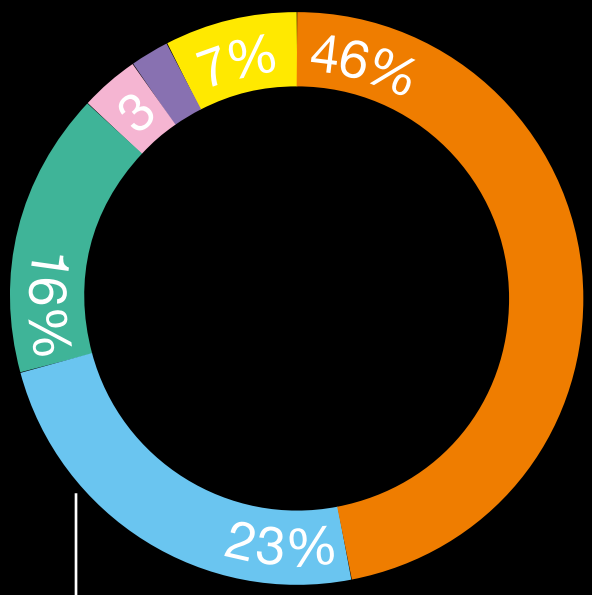
Santé et aide sociale

Dans le secteur de la santé et de l'aide sociale, le nombre d'incidents liés à des anomalies réseau et application se démarque. L'industrie de la santé, en particulier, montre des taux élevés d'incidents confirmés de divulgation non autorisée d'informations (activités de scan, tentatives infructueuses d'injections SQL, etc.), de connexions sortantes suspectes et de tentatives d'intrusion. La santé et l'aide sociale ont présenté plus d'incidents en janvier cette année, puis les taux ont baissé. Outre une exception en avril, cette tendance baissière s'est poursuivie jusqu'au troisième trimestre.

Industrie manufacturière

Dans l'industrie manufacturière de forts volumes d'incidents causés par des malwares ont été constatés (27 %), la plaçant au top 3 si l'on considère l'ensemble des secteurs. Cette industrie a aussi subi un nombre d'anomalies système supérieur à la moyenne et, donc, d'incidents en lien avec ses systèmes d'exploitation et leurs composants. L'industrie manufacturière se détache aussi avec un taux de 10 % de transgressions des politiques de sécurité, en troisième position sur l'ensemble des industries.



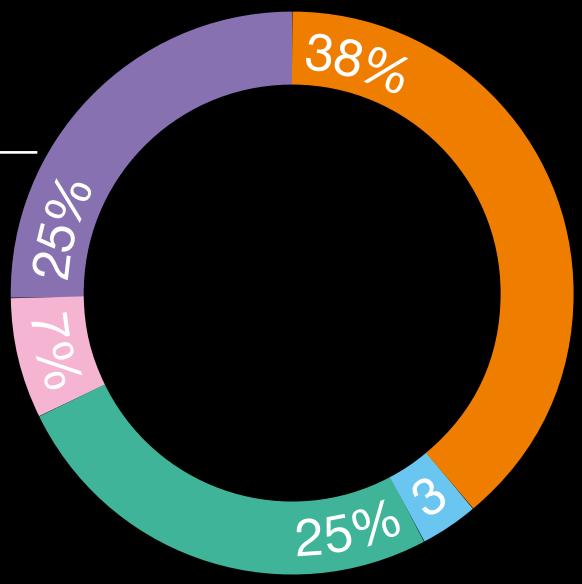


Services scientifiques et techniques

Dans cette industrie, on constate le plus fort taux d'anomalies sur les comptes utilisateurs. Par ailleurs, elle figure au top 3 des secteurs ayant connu le plus d'incidents confirmés liés à l'ingénierie sociale (surtout des cas de phishing et des spams). À la différence des autres secteurs, les services professionnels, scientifiques et techniques présentent un plus fort volume d'incidents en août.

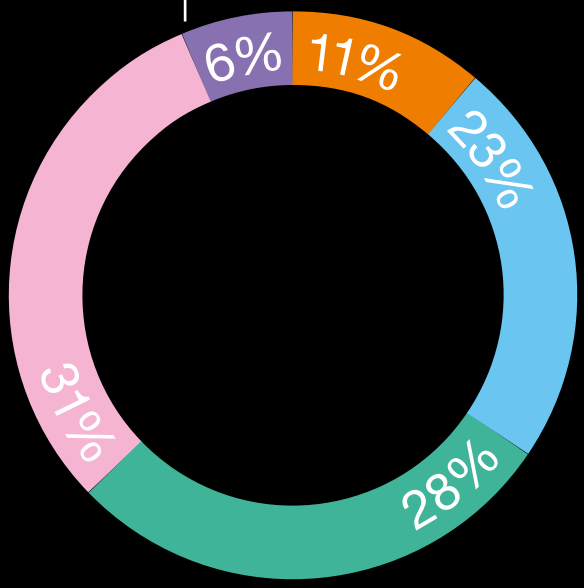
Administration publique

Ce secteur montre le plus fort taux de transgressions des politiques de sécurité. Rien d'étonnant, puisque cette industrie peut être soumise à plus de régulation que les autres. Elle représente ¼ de l'ensemble des incidents confirmés catégorisés comme malwares. L'administration publique se place donc dans le top 4 pour ce type d'incidents.



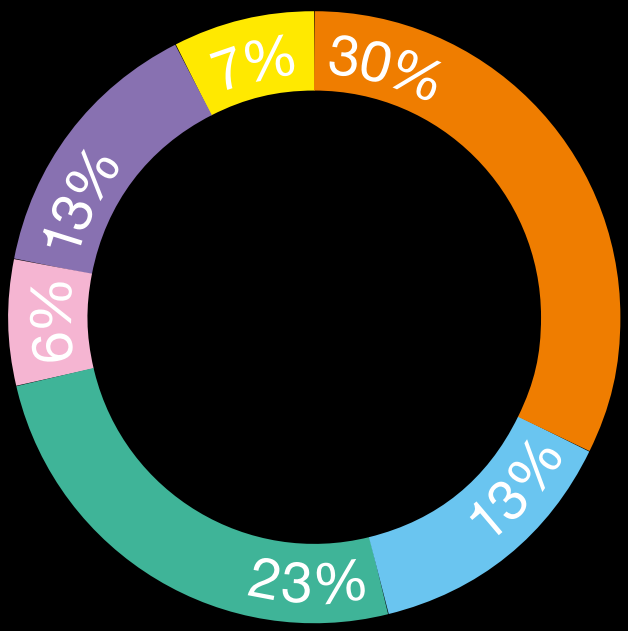
Immobilier, location et leasing

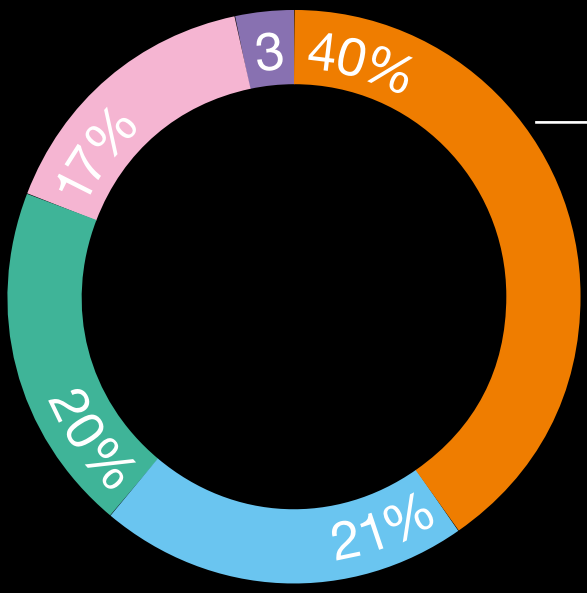
Dans le secteur de l'immobilier, nous constatons le plus fort taux d'incidents système : 31 % de l'ensemble des incidents. Les malwares sont le second type d'incident le plus fréquent pour ce secteur (28 %), suivent les anomalies sur les comptes utilisateurs (23 %). L'industrie de l'immobilier, de la location et du leasing est aussi le secteur qui présente le moins d'anomalies réseau et application, bien qu'il s'agisse des incidents les plus observés tous secteurs confondus.



Commerce et vente de détail

Le secteur du commerce et de la vente de détail suit la tendance générale en ce qui concerne les deux types incidents les plus fréquents, à savoir, les anomalies réseau et application (30 %) et les malwares (23 %). Outre un fort taux d'incidents catégorisés comme «erreurs», le secteur de la vente de détail connaît beaucoup d'incidents liés à des transgressions de politiques de sécurité et à l'ingénierie sociale. Dans cette industrie, une augmentation constante des volumes d'incidents a été observée cette année, en dépit d'un léger creux en août. C'est en septembre qu'elle a connu le plus d'incidents.





Transport et stockage

Dans le secteur des transports et du stockage, nous enregistrons plus d'anomalies système que dans les autres industries. 16% de l'ensemble des incidents sont confirmés comme en lien avec des anomalies dans les systèmes d'exploitation ou leurs composants. Outre les anomalies système, ce secteur subit les trois principaux types d'incidents : anomalies réseau et application, anomalies sur les comptes utilisateurs et malwares. Pour ce qui est de la tendance globale, elle a enregistré plus d'incidents en avril et en mai.

Conclusion

Les données de nos détections nous procurent plusieurs perspectives uniques, améliorant notre compréhension du paysage sécuritaire.

Les tendances en matière d'incidents de sécurité cette année ont été fortement impactées par un ralentissement du monde des affaires, conséquence de la pandémie de COVID-19. Ces tendances suivent donc les caractéristiques et comportements des utilisateurs en entreprise, indépendamment des efforts fournis par les attaquants. Plus d'incidents sont donc détectés pendant les heures de bureau, quand les ordinateurs sont connectés. Certains types d'incidents, cependant, se produisent après les heures ouvrées, aussi, il est clair qu'aucune entreprise ne peut se permettre de baisser sa garde quand ses salariés sont inactifs.

En particulier, nous avons constaté une augmentation du nombre d'incidents confirmés liés aux adwares et programmes potentiellement indésirables pendant les confinements. Beaucoup d'employés avaient alors commencé à travailler de chez eux et à installer des applications gratuites, bien que non-approuvées, pour s'adapter à la nouvelle réalité du télétravail.

Les ransomwares ont été un sujet majeur cette année et constituent une part importante de cette étude. Nous avons détecté plus d'incidents en lien avec des ransomwares pendant les confinements qu'ensuite. Nous pensons qu'ils résultent de niveaux de réponse insuffisants de la part des équipes sécurité durant ces périodes. Après avril, nous observons une hausse du nombre de downloaders et droppers (dont Emotet), mais une régression du nombre d'incidents liés à des ransomware confirmés. Cette évolution est peut-être due à une meilleure réponse aux cas de malware, plus tôt dans la chaîne après le «retour à la normale» des entreprises. En y portant plus d'attention, nous pouvons détecter et répondre à des attaques durant leurs premières phases, évitant ainsi qu'elles ne dégénèrent jusqu'à la phase ultime de chiffrement : une bonne nouvelle dans notre combat contre le fléau des ransomwares.

La taille et le secteur d'activité des entreprises clients méritent aussi d'être pris en compte. Les observations les plus marquantes renvoient à l'intensité des incidents qu'ont eu à affronter les plus petites entreprises : ils rejoignent souvent les niveaux rencontrés par les grands groupes. Il semble aussi que les organisations de petite et moyenne taille ont «rattrapé leur retard» sur les grands groupes et subissent aussi la tendance malware.

Nos données nous forcent à considérer l'intérêt d'ajouter davantage des technologies de détection, puisque les taux de détection les plus probants impliquent aussi un volume plus important de «bruit». Plus vous ajoutez d'outils de détection, moins leur bénéfice est incrémental. Néanmoins, en ce qui concerne les malwares, le coût d'une infection dépasse de loin celui d'un investissement dans le tri de faux-positifs : et, c'est encore plus vrai dans le nouveau monde des «extortionware». En somme, le coût d'un faux-négatif est infiniment plus grand que celui d'un faux-positif.

Chaque secteur d'activité dans notre base client présente ses propres combinaisons d'incidents. Toutefois, pour tous, une tendance est claire : les volumes d'attaques et d'incidents croissent sans relâche. Aucune entreprise, quels que soient sa taille et son secteur, ne peut se permettre de baisser sa garde.

© Orange Cyberdefense

TENSION

Test d'intrusion de l'IoT

Cadenas connecté au Bluetooth-LE

L'Internet des Objets (Internet of Things – IoT) est une industrie montante : les outils « intelligents » se généralisent. Cette expansion peut toutefois s'avérer dangereuse quand la sécurité n'est pas une priorité.

De nos jours, il est courant d'opter pour le vélo. C'est pourquoi l'un de nos clients nous a demandé d'auditer un cadenas connecté en Bluetooth à basse consommation (BLE) utilisé pour ses vélos en libre-service.

Thomas Bygodt, Managing Consultant, Orange Cyberdefense

orange™

Étape 1 : L'application Android

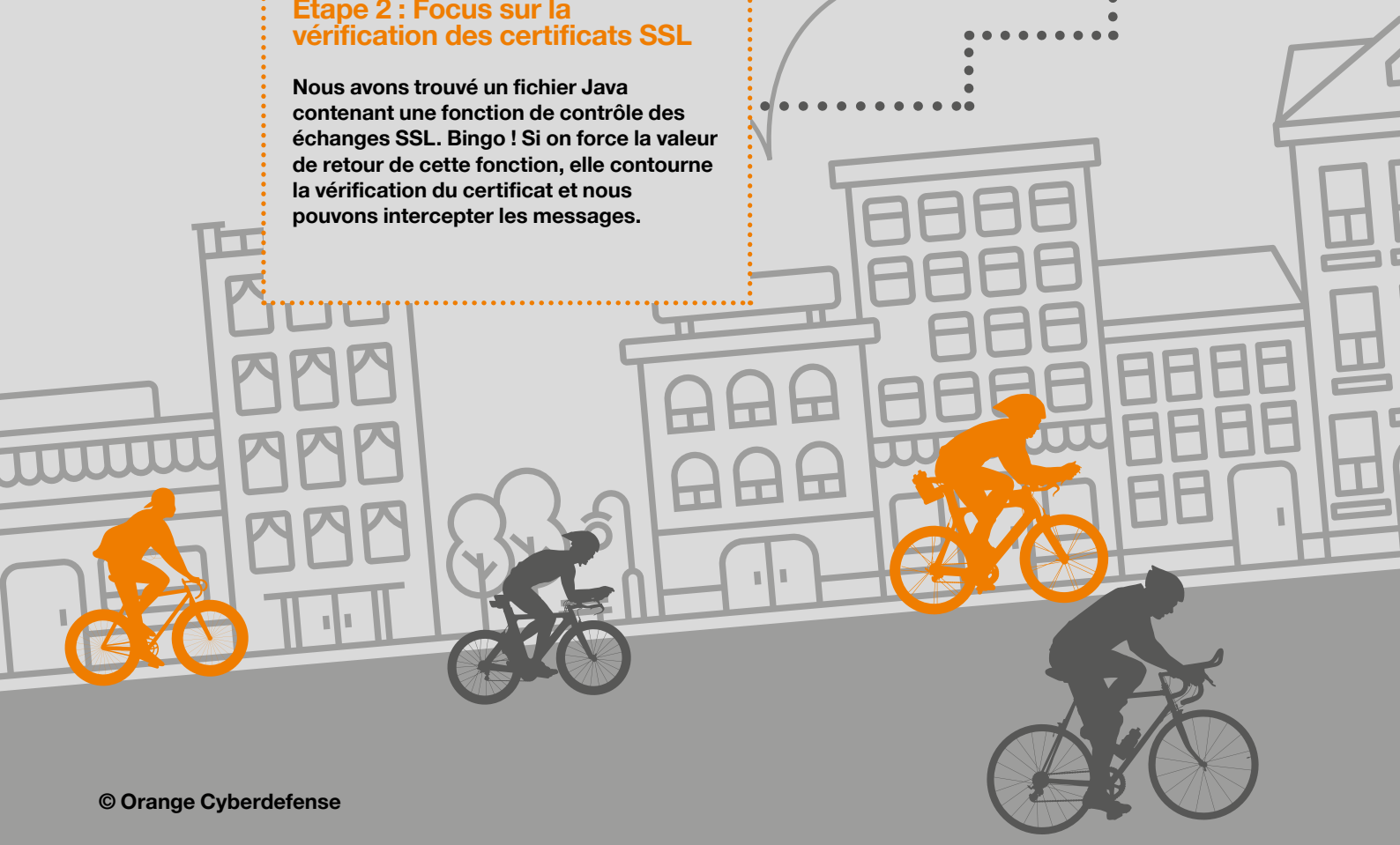
Nous avons décidé de commencer par une analyse statique de l'application mobile utilisée pour verrouiller/déverrouiller le cadenas. Le fichier APK de l'application a donc été téléchargé et décompressé.

Étape 2 : Focus sur la vérification des certificats SSL

Nous avons trouvé un fichier Java contenant une fonction de contrôle des échanges SSL. Bingo ! Si on force la valeur de retour de cette fonction, elle contourne la vérification du certificat et nous pouvons intercepter les messages.

Étape 3 : Au cœur des choses

Après nous être attardés sur le langage assembleur (Smali) de l'application, nous l'avons recompilé. Résultat : davantage de logs et finies les vérifications SSL !



© Orange Cyberdefense

Étape 4 : Bluetooth et Crypto

Les éléments échangés avec le serveur sont la clé BLE, le mot de passe BLE et l'adresse MAC de l'outil connecté. La clé BLE faiblement protégée, déchiffrée dans l'application, est facile à découvrir. Il reste juste à s'occuper des communications chiffrées en AES-CBC.

Étape 5 : Python, mon meilleur ami

Avec un adaptateur Bluetooth et un script Python, nous parvenons à verrouiller et déverrouiller le cadenas… Fin de partie !

Enseignements :

L'évaluation d'un objet connecté permet de rechercher des vulnérabilités sur l'ensemble de son environnement : matériel, logiciel embarqué, protocoles de communication, serveurs, applications mobiles, API, interfaces Web, etc.

- Concevoir et développer en gardant à l'esprit l'aspect sécurité.
- Sécuriser chaque terminal : matériel, composants électroniques, applications mobiles, outils de gestion dans le cloud, etc.
- Sécuriser les communications entre chaque composant.
- Ne jamais faire confiance à un utilisateur.

© Orange Cyberdefense

Charl van der Walt
Head of Security Research
Orange Cyberdefense

World Watch : veille mondiale

2020 : faits marquants

Le service World Watch d'Orange Cyberdefense œuvre pour ses clients à collecter, analyser, prioriser et contextualiser les menaces mondiales, par géographie et par secteur. Il fournit également des informations sur les vulnérabilités ainsi que des données pertinentes pour chaque métier, infrastructure et application.

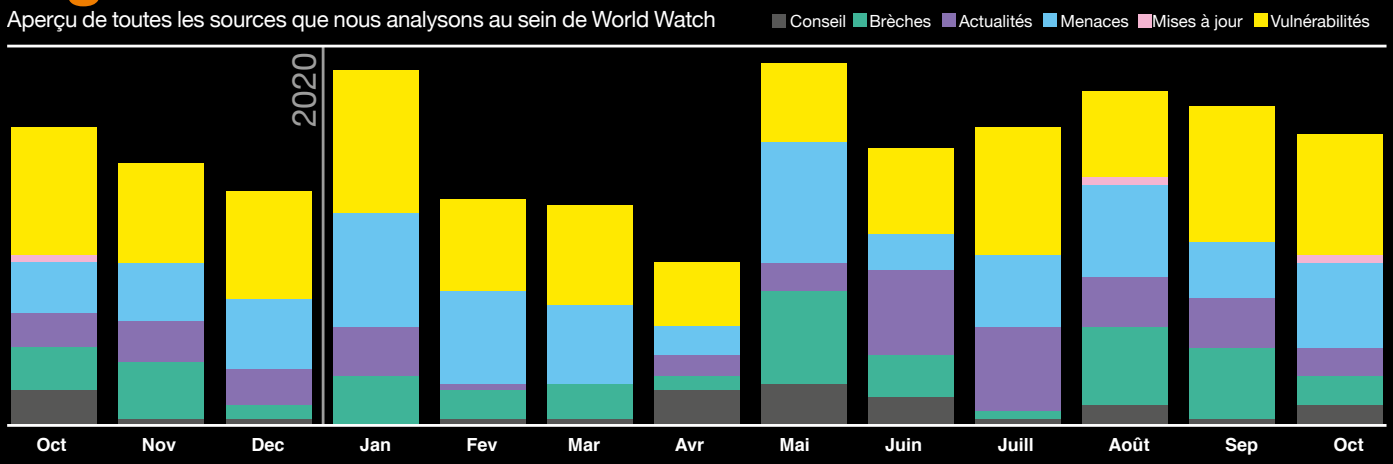
Il émet chaque mois entre 30 et 50 signalements traitant des vulnérabilités, brèches, menaces et actualités jugées importantes pour nos clients au niveau mondial. Au fil des 12 mois qui ont précédé le 30 septembre 2020, il a produit près de 500 signalements.

Les descriptions au sein de ces signalements s'appuient sur un système normalisé de tags nous permettant de suivre les technologies, acteurs et menaces traités. Nous surveillons aussi les tendances émergentes. Nous les utilisons pour construire et maintenir une bonne vision des menaces. Cette année, nous comptons déjà plus de 5000 tags, qui offrent une idée des évènements importants qui façonnent notre industrie.

Si les données collectées ne sont pas volumineuses, elles procurent une perspective nouvelle et éclairante. En combinaison avec d'autres sources (internes et externes), nous l'utilisons pour savoir de ce qu'il se passe vraiment dans le monde de la sécurité.

Signalements

Aperçu de toutes les sources que nous analysons au sein de World Watch



COVID : quand la « fatigue » gagne du terrain

Dans ces graphiques, nous constatons d'abord un ralentissement des signalements en avril dernier, suivi d'une augmentation considérable de leur volume en mai. Cet important creux reflète à quel point l'industrie dans son intégralité a été déconcentrée par les périodes de confinement généralisé. Cette déconcentration sera examinée en détails plus loin, mais il faut en prendre note pour bien comprendre les autres données que nous partageons dans ce rapport.

Les données ci-dessus suggèrent que le volume de sigalements publiés par notre équipe World Watch a diminué de janvier à avril, puis a connu une hausse spectaculaire en mai, malgré le faible volume de l'actualité générale.

Après un recul de l'activité en avril, une croissance prononcée a été constatée en mai : les entreprises se remettant sur pied au lendemain du choc du confinement. Il ne fait pas de doute que les attaquants ont aussi été impactés, d'une manière ou d'une autre, par ces confinements. Cependant, nous pensons que le marasme d'avril fait écho à l'activité des entreprises, et non à celle des attaquants. Comme le soulignent d'autres sections de ce Security Navigator, nous avons remarqué une « fatigue » similaire dans les volumes d'incidents de sécurité gérés par nos CyberSOC à la même période.

Du point de vue des signalements liés aux incidents de sécurité que nous évoquions plus tôt : avril, mai et juin ont très clairement été des mois anormaux.

Signalements critiques

Signalements publiés au cours de la période couverte par notre rapport, classés comme "critiques" :

Categorie	Date	Summary
Vulnérabilité	15/10/2020	Un bug critique du portail VPN SonicWall permet au DoS et au Worming RCE de se connecter
Vulnérabilité	14/10/2020	Octobre Patch Tuesday : Microsoft corrige un bug RCE critique et vermifuge
Vulnérabilité	15/09/2020	Attaque Zerologon contre Windows
Vulnérabilité	15/07/2020	Microsoft corrige un bug SIGRed vermifuge dans le serveur DNS de Windows
Vulnérabilité	14/07/2020	Le bug RECON permet aux pirates de créer des comptes administrateurs sur les serveurs SAP
Vulnérabilité	02/07/2020	F5 TMUI Remote Code Execution Vulnerability
Vulnérabilité	10/03/2020	Microsoft SMBv3 Vulnerability
Vulnérabilité	14/01/2020	Mise à jour de sécurité de Microsoft de janvier 2020

Les vulnérabilités

Les huit signalements catégorisés comme critiques l'an dernier ont été des vulnérabilités. Cinq de ces vulnérabilités impactent Microsoft Windows, qui continue d'être une source de vulnérabilités sévères et une cible privilégiée. Une vulnérabilité peu usuelle relevée dans les systèmes SAP aurait permis à un attaquant non authentifié d'accéder pleinement au système SAP affecté.

Les deux derniers problèmes listés impliquaient des technologies de sécurité périmétriques — un bug critique dans un portail VPN SonicWall et une exécution de code à distance (Remote Code Execution) dans le TMUI de F5.

Ces deux vulnérabilités critiques au sein de technologies de sécurité sont de sérieux exemples de ce que nous considérons comme l'un des sujets de sécurité dominants cette année, à savoir, les vulnérabilités et attaques impliquant des technologies que nous déployons pour protéger les périmètres de nos réseaux, en particulier pour permettre des accès distants sécurisés à nos systèmes internes.

Les éditeurs sous les projecteurs en 2020

Jetons un œil aux éditeurs de solutions technologiques qui se démarquent cette année dans nos signalements au travers des différentes catégories.

Microsoft (Windows)

De nombreuses vulnérabilités résidaient dans les produits Microsoft. Microsoft a occupé une place prépondérante dans nos catégories Menaces et Actualités, indiquant la fréquence à laquelle les produits Microsoft contribuent à des menaces significatives.

Les vulnérabilités Microsoft (et Windows) sont toujours des défis en matière de correctifs. Le volume de vulnérabilités graves au sein des produits Windows varie en fonction du volume de problèmes signalés pour l'ensemble des technologies. Comme l'indique le graphique ci-dessous, ce volume a beaucoup augmenté au cours des 18 derniers mois.

Le nombre de vulnérabilités Windows a connu une progression importante les trois premiers trimestres de 2020. Les vulnérabilités communes (CVE) jugées élevées ou critiques ont en effet doublé entre le quatrième trimestre 2019 et le premier trimestre 2020.

En septembre dernier, nous avons publié un signalement critique qui impliquait une vulnérabilité Windows appelée « ZeroLogon » — CVE-2020-1472. Cette CVE décrit un bug dans l'Active Directory de Windows Server, patchée en août par le Microsoft August 2020 Patch Tuesday. Elle est présentée comme une élévation de privilèges dans Netlogon, protocole authentifiant les utilisateurs aux contrôleurs de domaine. Elle est ensuite devenue une arme, activement utilisée par les attaquants, notamment les cybercriminels usant de ransomwares.

Produits de sécurité

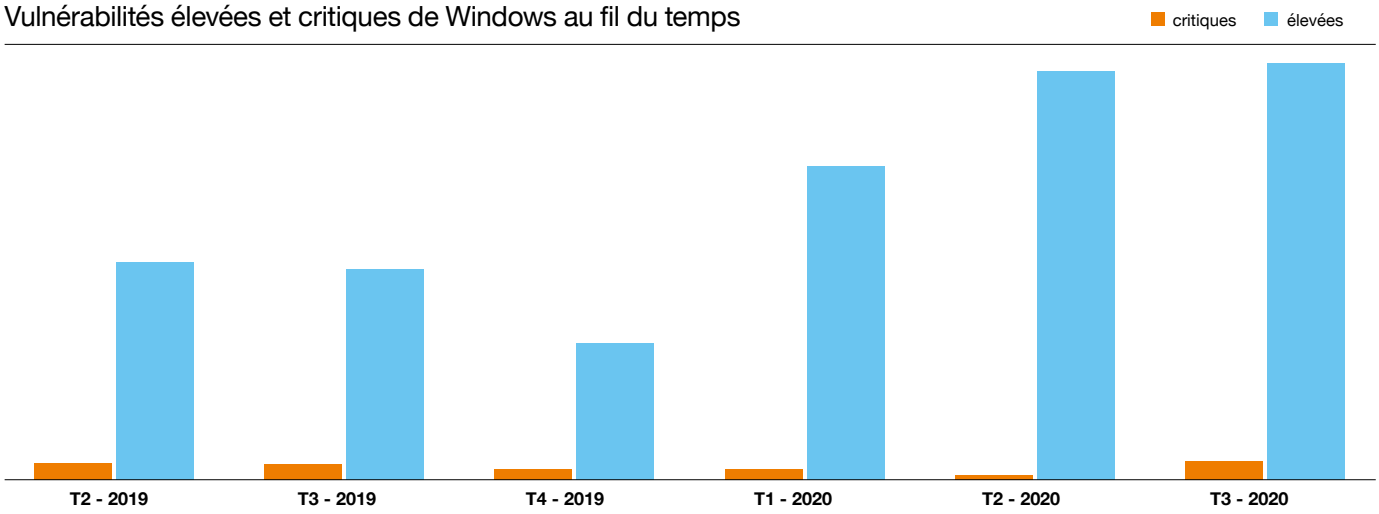
Si les grandes marques comme Microsoft seront toujours surreprésentées, la visibilité de plusieurs éditeurs de produits de sécurité interpelle aussi au cours des 12 derniers mois. Ils figurent dans la courte liste d'éditeurs mis en exergue à plusieurs reprises par nos signalements cette année.

Nous avons remarqué une augmentation caractéristique en mai : une proportion inhabituelle de vulnérabilités a été remontée pour ces technologies de sécurité. En effet, le nombre de vulnérabilités signalées a quadruplé pour certaines technologies de sécurité entre mars et mai 2020.

En page suivante, nous proposons ce qui peut être décrit comme une « cascade » de recherche. Nous montrons comment des CVE ont été étudiées et ont amené à plus de recherches, ainsi qu'à la découverte d'autres CVE dans des familles de produits similaires.

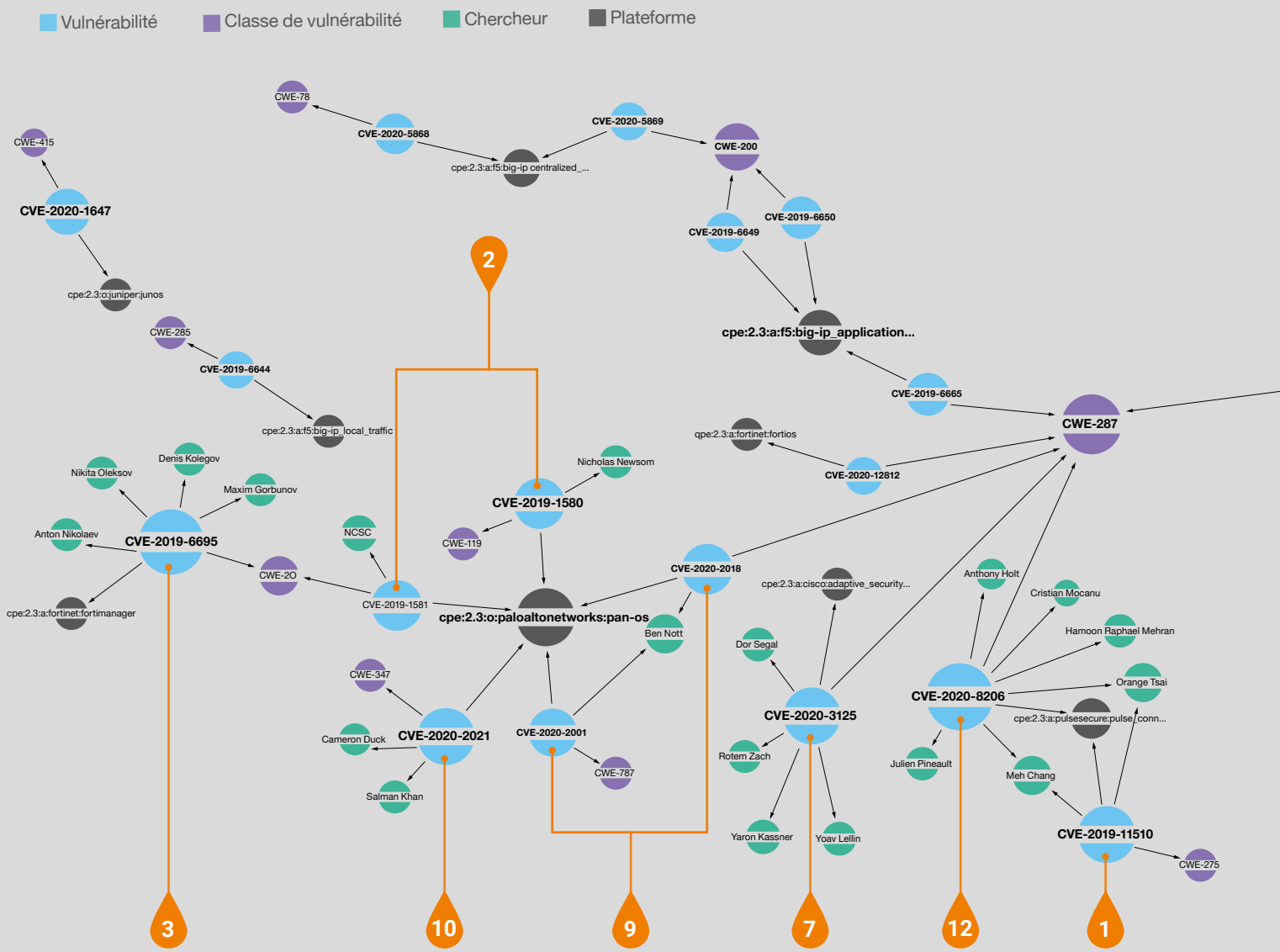
Vulnérabilités Windows

Vulnérabilités élevées et critiques de Windows au fil du temps



Recherche des CVE : l'effet domino

Vulnérabilités découvertes dans les produits de sécurité



1 8 mai 2019 : CVE-2019-11510

Orange Tsai et Meh Chang découvrent une vulnérabilité critique affectant Pulse Connect Secure, qui permet la lecture arbitraire de fichiers du fait de problèmes de droits.

2 23 août 2019 : CVE-2019-1580 / CVE-2019-1581

Nicholas Newsom découvre une vulnérabilité critique de corruption de mémoire affectant le logiciel SSHD du système PAN-OS de Palo Alto Networks. Le National Cyber Security Center britannique a remonté une vulnérabilité RCE dans l'interface de gestion SSH de PAN-OS.

3 23 août 2019 : CVE-2019-6695

Du fait d'une validation inexacte d'entrée, une autre vulnérabilité critique est remontée par une équipe de recherche indépendante concernant FortiManager de Fortinet.

4 27 décembre 2019 : CVE-2019-19781

Une vulnérabilité « directory traversal » dans Citrix Application Delivery Controller et Citrix Gateway pouvant conduire à une exécution de code arbitraire est découverte par Mikhail Klyuchnikov, Gianlorenzo Cipparrone et Miguel Gonzalez.

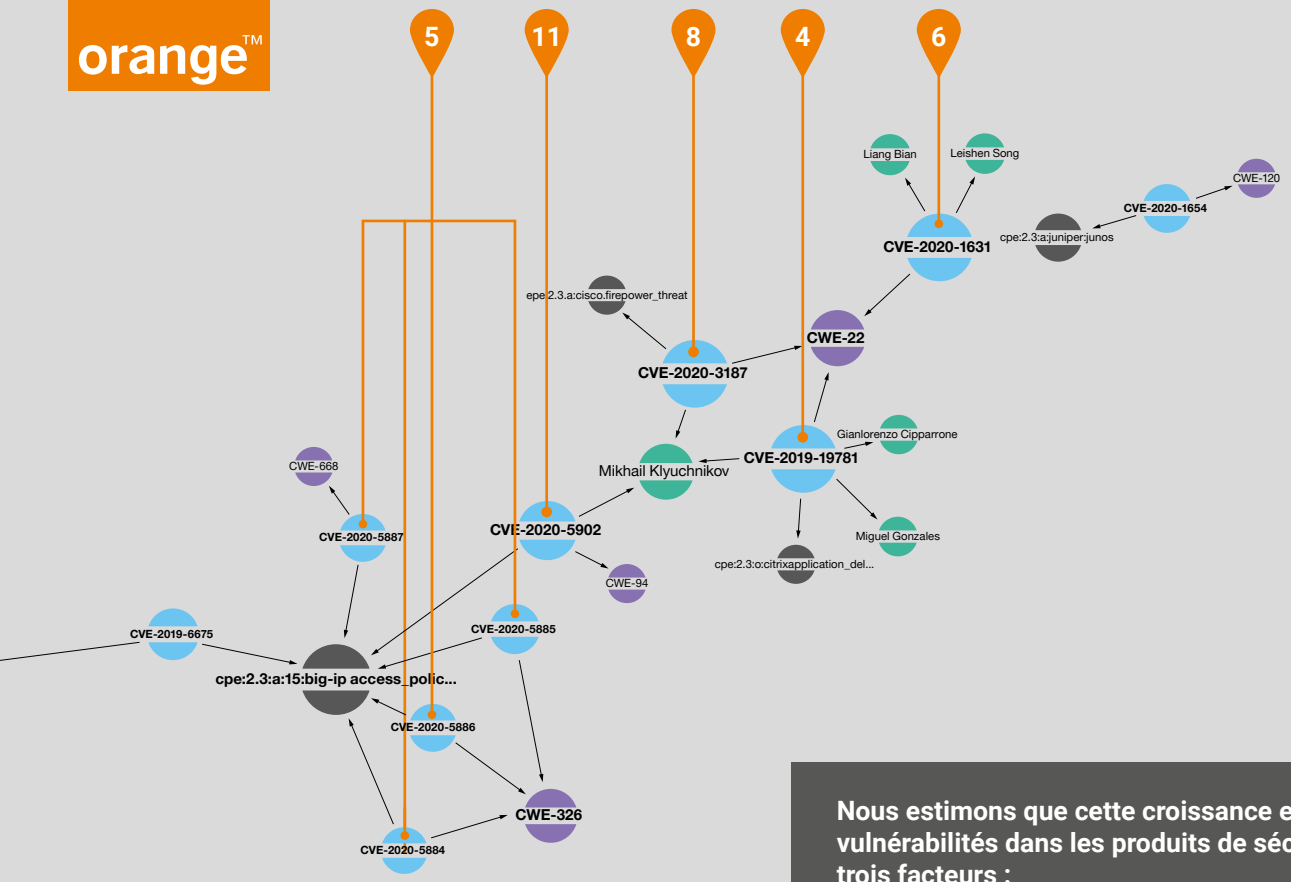
5 30 avril 2020 : CVE-2020-5884 / CVE-2020-5885 / CVE-2020-5886 / CVE-2020-5887

Quatre vulnérabilités sont découvertes et affectent divers produits BIG-IP de F5. Trois d'entre elles sont causées par un problème de chiffrement (Inadequate Encryption Strength). La quatrième est indiquée comme « Exposure of Resource to Wrong Sphere ».

6 4 mai 2020 : CVE-2020-1631

Une vulnérabilité critique dans le service HTTP/HTTPS de Juniper Junos OS est découverte par Liang Bian et Leishen Song. Il s'agit d'un autre exemple de vulnérabilité « directory traversal ».

© Orange Cyberdefense



Nous estimons que cette croissance exceptionnelle des vulnérabilités dans les produits de sécurité résulte de trois facteurs :

- Le « succès » notable de la vulnérabilité Pulse, CVE-2019-11510, de mai 2019, qui a été exploitée par plusieurs attaques majeures.
- L'adoption ou l'expansion rapide de fonctionnalités d'accès distant pour répondre au télétravail massif a fait de ces technologies des cibles de choix.
- Un effet domino : la découverte d'une vulnérabilité crée de nouvelles connaissances qui conduit parfois à la découverte de vulnérabilités similaires (voire même différentes) au sein du produit, ou dans d'autres.

7 6 mai 2020 : CVE-2020-3125

Quatre chercheurs sont crédités de la découverte d'une vulnérabilité dans le protocole d'authentification Kerberos de Cisco Adaptive Security Appliance (ASA) Software. Cette faille est due à un défaut d'authentification permettant à l'attaquant de contourner le protocole d'authentification Kerberos.

8 6 mai 2020 : CVE-2020-3187

Mikhail Klyuchnikov découvre une autre vulnérabilité « directory traversal » affectant Cisco Adaptive Security Appliance Software et Firepower Threat Defense Software.

9 13 mai 2020 : CVE-2020-2001 / CVE-2020-2018

Ben Nott est crédité de la découverte de deux vulnérabilités affectant le système PAN-OS du logiciel Panorama de Palo Alto Networks.
La première est une faille critique permettant à un attaquant non authentifié d'élever ses droits. La seconde permet à l'attaquant d'accéder à l'interface de gestion.

10 29 juin 2020 : CVE-2020-2021

Une autre vulnérabilité affectant Palo Alto Networks PAN-OS est remontée par Cameron Duck et Salman Khan. Cette faille permet à des attaquants non authentifiés d'accéder à des ressources protégées.

11 1er juillet 2020 : CVE-2020-5902

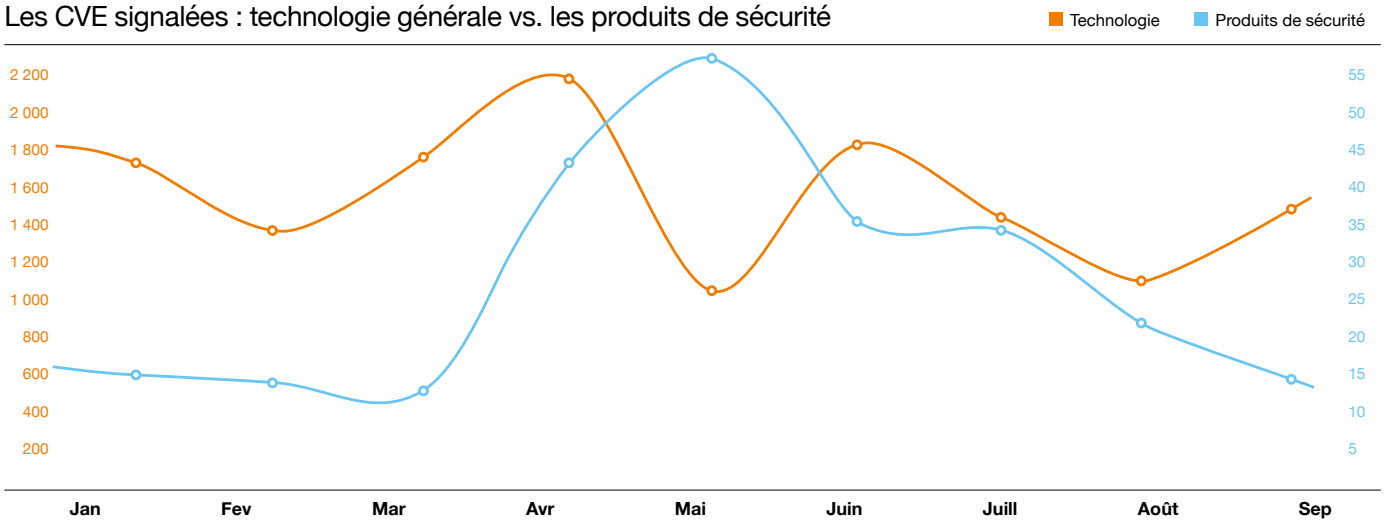
Mikhail Klyuchnikov est à nouveau crédité pour la découverte d'une vulnérabilité impactant plusieurs produits BIG-IP de F5. Cette faille critique permet à un attaquant d'exécuter des commandes arbitraires et d'aboutir à la compromission complète du système.

12 30 juillet 2020 : CVE-2020-8206

Une très grave vulnérabilité affectant Pulse Connect Secure est dévoilée dans une alerte sécurité. Orange Tsai et Meh Chang, qui ont découvert la vulnérabilité CVE-2019-11510 en mai 2019, se distinguent à nouveau. Cette vulnérabilité est liée à un défaut d'authentification permettant à l'attaquant de contourner le TOTP de Google (Time-based One Time Password).

Vulnérabilités au sein des produits de sécurité

Les CVE signalées : technologie générale vs. les produits de sécurité



Les vulnérabilités découvertes dans des produits de sécurité

Ce graphique illustre les vulnérabilités présentes dans des produits de sécurité périmétriques de premier plan, comparativement aux vulnérabilités dans les technologies en général. Une progression exceptionnelle du nombre de vulnérabilités impactant les produits de sécurité est observée en mai 2020 (au cœur de la période de confinement).

Ce graphique montre une anomalie en mai 2020 : environ deux fois moins de vulnérabilités étaient remontées par rapport au mois précédent, alors qu'une proportion inhabituellement élevée de vulnérabilités était constatée dans les produits cités précédemment. De fait, le nombre de vulnérabilités remontées a quadruplé pour certaines technologies de sécurité entre mars et mai 2020.

L'heure des correctifs

Nous avons mené une étude restreinte sur 168 vulnérabilités au sein des produits de sécurité au cours des 12 derniers mois. Cette étude montre non seulement que l'augmentation du volume de vulnérabilités est un problème, mais aussi que bien trop de temps s'écoule avant que les entreprises les corrigent.

Nous avons pu voir que moins de 19 % des vulnérabilités sont patchées sous 7 jours. Par ailleurs, 56,8 % de ces vulnérabilités prennent de 31 à 180 jours à être résolues, et, plus préoccupant encore, 14 % ne sont toujours pas adressées six mois après avoir été notifiées.

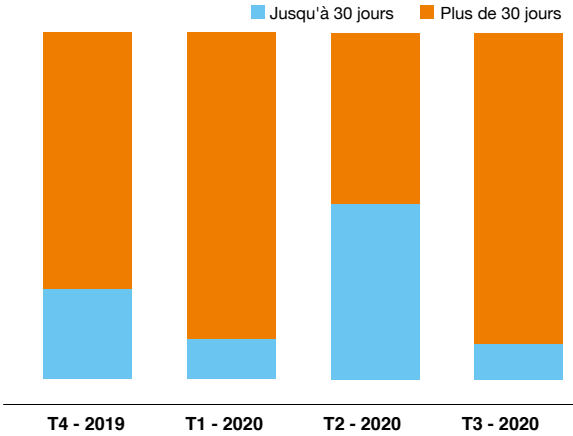
Une récente alerte intitulée State-Sponsored Actors Exploit Publicly Known Vulnerabilities émise par la National Security Agency (NSA) américaine, liste 25 vulnérabilités connues activement utilisées par des hackers étatiques. Six de ces 25 failles impliquent des technologies de sécurité périmétriques.

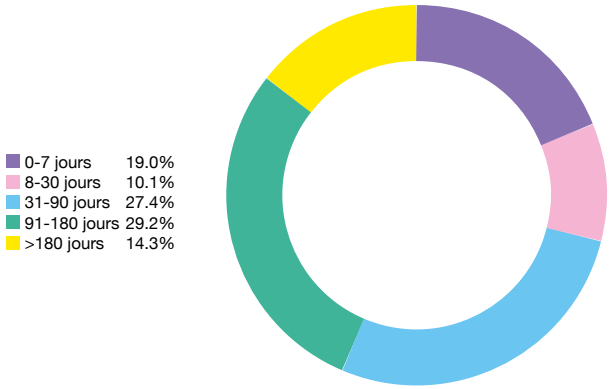
Au vu de l'incroyable vitesse à laquelle les attaquants trouvent et exploitent des vulnérabilités, cette fenêtre d'exposition étendue exacerbe des problèmes liés aux ransomwares, aux attaques de type « big game hunting », aux vols d'IP et aux fuites de données.

Les clients sont encouragés à s'assurer qu'ils disposent des ressources humaines et des procédures pour répondre dans les temps aux vulnérabilités découvertes dans les produits de sécurité une fois les annonces faites. Il est certain que le nombre de ces vulnérabilités augmente en ce moment. Combinées à la précipitation des déploiements et des ajustements de services d'accès distant, elles exposent des périmètres de sécurité critiques, contribuant directement à de possibles compromissions et brèches de sécurité.

Retard dans l'application des patchs

Temps nécessaire à l'application d'un patch pour une CVE connue (part par trimestre, sur l'ensemble du scope)



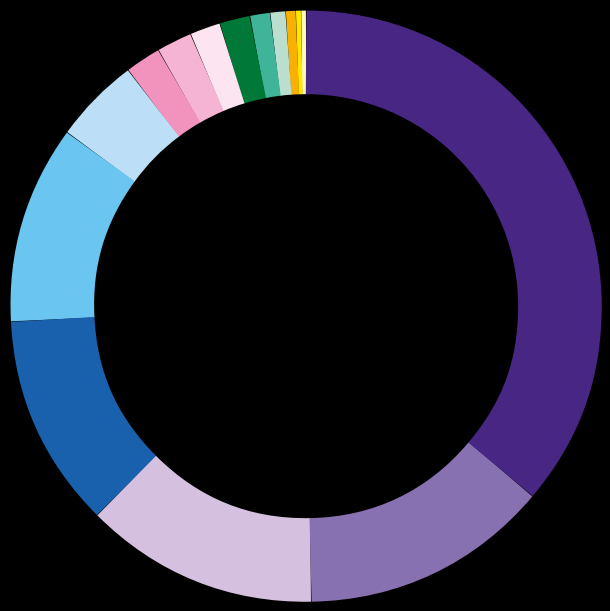


© Orange Cyberdefense

Acteurs de la menace

Activités liées à des ransomwares au cours des 12 derniers mois (surveillance du Dark Web)

Maze	36.31%
REvil	13.48%
Conti	12.77%
NetWalker	11.77%
Doppelpaymer	10.78%
PYSA	4.68%
CLOP	2.13%
Nefilim	1.84%
Suncrypt	1.70%
Ako	1.56%
Ragnar	1.14%
Sekhmet	0.99%
Avaddon	0.43%
Nemty	0.28%
Darkside	0.14%



Scruter le Dark Web

Le Laboratoire d'épidémiologie d'Orange Cyberdefense suit systématiquement des portails et forums de hacking sur le Dark Web afin d'identifier les évolutions métier dans l'écosystème des malwares. Ainsi, nous observons de nouveaux modèles économiques, des changements d'alliances, d'infrastructures techniques et des annonces de compromissions et rançons. Le Dark Web est opaque : il n'est pas indexé par les robots (« crawlers »), moteurs de recherche et autres outils automatisés. Il est donc difficile de le suivre de manière systémique. En répertoriant les annonces observées et les échanges de plusieurs opérateurs de ransomwares, des tendances émergent néanmoins.

Notre équipe suit ces changements en scrutant le trafic sur les forums en ligne. Nous pouvons ainsi comprendre les changements qui s'opèrent en arrière-plan, plutôt que simplement à la surface, là où des variantes de code malveillant finissent par impacter les victimes.

« MAZE » : l'éveil

Selon notre analyse du Dark Web, 36,3 % de fuites publiées étaient attribuées à MAZE. D'après MITRE, le ransomware MAZE, anciennement connu sous le nom de « ChaCha », a été découvert en mai 2019. En plus de chiffrer les données sur les machines infectées et, pour augmenter son impact, les cybercriminels mènent des campagnes de vol d'informations avant le chiffrement. Ils publient les informations pour exhorter les victimes à payer des rançons.

MAZE a explosé sur la scène des menaces depuis son apparition en 2019. En tant qu'acteur phare du moment, il promet d'influer sur la cybercriminalité encore quelque temps. REvil, Conti (Ryuk), DoppelPaymer et NetWalker sont aussi des acteurs majeurs de menaces ; le paysage change à mesure qu'ils ajustent leurs modèles économiques et fondent de nouvelles alliances. L'écosystème criminel qui se manifeste au travers des ransomwares est complexe et dynamique. Il consiste en une myriade d'acteurs très divers qui négocient leurs produits et services. Ces solutions sont vectrices d'attaques par ransomware et induisent donc des paiements.

La dominance persistante de MAZE au fil du temps est claire à en croire ces données. L'émergence de nouveaux entrants dans cet écosystème est tout aussi flagrante, peut-être du fait d'alliances et pratiques métier clandestines nouvelles et différentes.

Tendance : la double extorsion

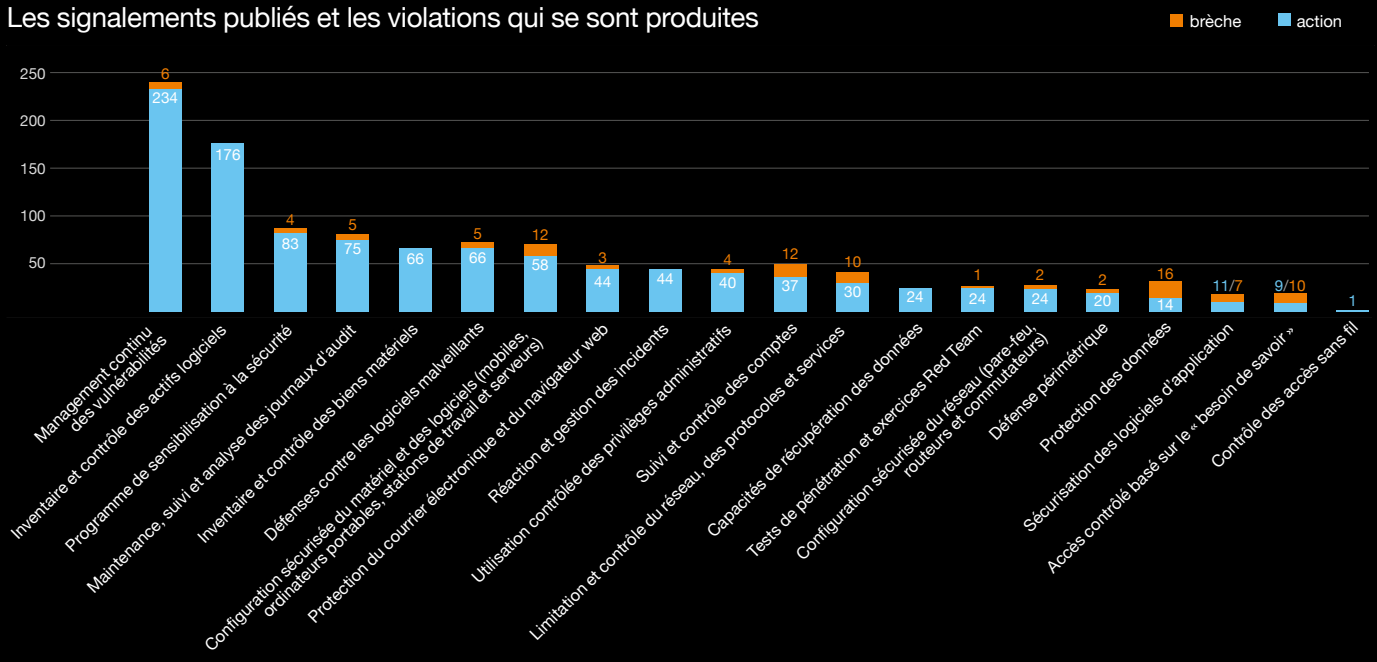
La tendance la plus récente pour les opérateurs de ransomwares consiste dans la maintenance de sites exposant les fuites de données à des fins de « double extorsion ». Les gangs proposent les clés de déchiffrement si les rançons sont réglées, mais menacent de divulguer les informations si elles ne le sont pas.

Durant le trimestre qui a précédé la publication de ce rapport, nous observons une plus grande visibilité du groupe Conti, aussi connu sous le nom de Ryuk. Adepte de cette pratique de double extorsion depuis août 2020, il a lancé son site de divulgation. Conti dépasse MAZE au troisième trimestre et revendique 22 % de l'activité ransomware que nous avons observée. Très récemment, le 20 octobre, le géant français des services informatiques Sopra Steria a subi une cyberattaque qui a, semble-t-il, causé le chiffrement de certaines portions de son réseau par Ryuk. L'attaque contre l'Universal Health Services — qui a impacté des hôpitaux aux États-Unis en septembre — a aussi été attribuée à ce groupe. Nous nous attendons à voir apparaître plus d'acteurs de ce type dans les prochains mois.

Ici, le principal enseignement selon nous est que les ransomwares sont devenus un business et plus seulement une technologie. Ils doivent donc être envisagés d'abord en tant que problématique métier. En complétant la triade optimale — demande insatiable, fourniture limitée et échanges monétaires fluides — les cryptomonnaies ont aidé à ce que les attaques par ransomware deviennent un modèle économique viable. Les polices d'assurance cyber ont d'ailleurs commencé à payer des rançons pour les victimes. Les ransomwares s'imposent comme des produits emblématiques sur le marché cybercriminel, pour autant que nous sachions, ils ne sont pas prêts de disparaître.

Conseils du CIS vs violations de données effectives

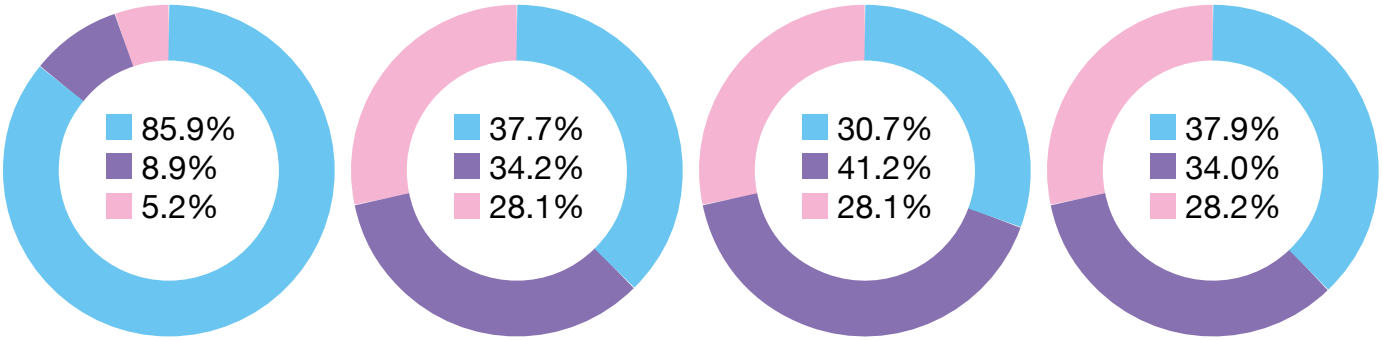
Les signalements publiés et les violations qui se sont produites



Contrôles	Niveau	Contrôle recommandé	Identifié dans les fuites
Gestion continue des vulnérabilités	basique	234	6
Inventaire et contrôle des actifs logiciels	basique	176	
Mise en place d'un programme de sensibilisation à la sécurité	organisationnel	83	4
Maintenance, suivi et analyse des rapports d'audit	basique	75	5
Inventaire et contrôle des actifs matériels	basique	66	
Défense contre les malwares	fondamental	66	5
Configuration sécurisée du matériel et des logiciels sur les mobiles, ordinateurs portables, postes de travail et serveurs	basique	58	12
Protections des e-mails et navigateurs Web	fondamental	44	3
Réponse aux incidents et gestion des incidents	organisationnel	44	
Usage contrôlé des droits d'administration	basique	40	4
Suivi et contrôle des comptes	fondamental	37	12
Limitation et contrôle des ports, protocoles et services réseaux	fondamental	30	10
Capacités de récupération de données	fondamental	24	
Tests d'intrusion et exercices Red Team	organisationnel	24	1
Configuration sécurisée des outils réseaux, dont les pare-feu, routeurs et commutateurs	fondamental	24	2
Défense périmétrique	fondamental	20	2
Protection des données	fondamental	14	16
Sécurité des applications logicielles	organisationnel	11	7
Accès contrôlé selon le "besoin de savoir"	fondamental	9	10
Contrôle des accès sans fil	fondamental	1	

Vulnérabilité, menace, fuite de données

Comment les conseils demandés et donnés correspondent-ils aux besoins réels ?



Recommandations du CIS sur les vulnérabilités

Actions requises selon le CIS pour répondre aux menaces observées

Les actions du CIS qu'il aurait été préférable d'éviter

Les défaillances de contrôle identifiées par notre équipe d'intervention d'urgence (CSIRT)

Contrôles de sécurité et défaillances

Pour s'assurer que des leçons sont tirées des mésaventures des autres, il nous faut examiner leurs erreurs plus en détail et prendre en compte ce qu'elles nous apprennent.

Aussi, quand nous ajoutons une recommandation à un signalement World Watch, cette recommandation est fondée sur la liste de points du contrôle du Center for Internet Security (The 20 CIS Controls & Resources, voir : https://www.cisecurity.org/controls/cis-controls-list/). Nous pouvons ainsi proposer, via nos conseils, la base sur laquelle les contrôles de sécurité standard se basent le plus souvent.

Ce graphique résume les recommandations émises par nos analystes dans les signalements, séparés en fonction des menaces et des vulnérabilités d'une part, et les insuffisances en matière de contrôle identifiées dans des brèches de sécurité, d'autre part.

Comme illustré par la liste plus haut, la gestion continue des vulnérabilités, les inventaires logiciels et matériels, la mise en place de programmes de sensibilisation et d'éducation à la sécurité, et les logs sont les points de contrôle les plus souvent référencés dans nos signalements. Néanmoins, si nous examinons les échecs relevés dans des brèches de sécurité, l'account monitoring, la sécurité des configurations, la protection des données et la segmentation réseau se démarquent comme les principaux points de contrôle. Les deux perspectives placent toutefois la gestion des vulnérabilités dans leurs listes des cinq points les plus importants.

Il est également intéressant de constater une différence entre les recommandations émises par les analystes en réponse à des vulnérabilités et menaces et les défauts de contrôle enregistrés quand nous étudions des brèches de sécurité rendues publiques. Il est certain que nous sommes toujours appelés à considérer et gérer les points de contrôle de base du cadre établi par le CIS (Center of Internet Security), mais les brèches que nous avons à analyser peuvent être attribuées à des défaillances concernant des points de contrôle plus avancés des exigences du CIS. Cette notion est très nettement explicitée dans les précédents graphiques.

Ces graphiques montrent que, dans nos signalements commentant des vulnérabilités, nous sommes très susceptibles d'émettre des recommandations que le CIS estimerait basiques. Quand les signalements renvoient à des menaces auxquelles nous pensons que nos clients doivent répondre ou pour lesquelles il leur faut se préparer, les recommandations sont bien plus réparties sur les différents niveaux de contrôle du CIS. Enfin, lorsque nous commentons des défaillances en matière de contrôles de sécurité qui ont effectivement induit des brèches, nous citons les points de contrôle fondamentaux et avancés bien plus souvent que les bases.

En d'autres mots, bien qu'il soit clair que les entreprises doivent maîtriser les bases de la sécurité pour devancer les menaces et vulnérabilités, ce n'est pas suffisant. Elles doivent aussi maîtriser des pratiques plus avancées pour éviter les brèches de sécurité et ne surtout pas faire les gros titres.

Conclusion

Les compromissions de données continuent à se multiplier, sous l'impulsion de forces systémiques puissantes.

Les ransomwares servant d'arme utilisée pour une « double extorsion » ainsi que « le big game hunting » sont des sujets majeurs de la cybercriminalité cette année. Les ransomwares doivent être contrés en tant que business, ce qu'ils sont désormais, et non en tant que technologies.

Le groupe criminel Maze, derrière cette approche novatrice, est devenu l'acteur le plus notable ces derniers mois. Maze pourrait, toutefois, ne pas conserver cette avance puisque d'autres modèles économiques et alliances se constituent. Les rançons et menaces d'extorsion pèseront néanmoins encore dans un futur proche. Les techniques utilisées ne sont pas nouvelles, mais l'automatisation et l'orchestration ont conduit à des vitesses d'exécution impressionnantes. Les frameworks des logiciels malveillants polyvalents permettent à l'attaquant d'exploiter une faille de plusieurs manières différentes, avant de lancer finalement le chiffrement des données.

Les vulnérabilités jouent un rôle tout aussi important dans la formation de la menace émergente, figurant presque deux fois plus souvent dans nos signalements. La sécurité de Microsoft (et Windows, en particulier) façonne toujours le paysage, non seulement par son rôle pivot dans grand nombre de technologies d'entreprise, mais aussi du fait d'une augmentation considérable des vulnérabilités critiques au fil des 12 derniers mois.

Cependant, cette année, le principal sujet sécurité aura été la présence de vulnérabilités dans des plates-formes majeures de sécurité périmétrique – surtout, celles garantissant l'accès distant sécurisé d'une armée de télétravailleurs générée par la pandémie de COVID-19. Après des mises en place et redimensionnements hâtifs, les correctifs et mises à jour pour ces plates-formes prennent bien trop de temps. Et ce problème semble s'accentuer…

Les hackers étatiques et cybercriminels ont saisi ces opportunités. Les changements drastiques opérés pour les explorer ont eu des effets dévastateurs. Plusieurs compromissions et brèches majeures exploitaient des vulnérabilités au sein de produits de sécurité, les attaques par ransomware notamment. Ces vulnérabilités sont une constante dans l'arsenal des pirates étatiques.

Par conséquent, l'inventaire des logiciels, la découverte des vulnérabilités et les correctifs sont les recommandations les plus fréquemment citées dans nos signalements (36% d'entre eux).

La maîtrise des contrôles de sécurité de « base » est indispensable pour toute organisation souhaitant devancer les menaces, et ce, bien que ces bases ne soient plus suffisantes. Chaque entreprise, quelle que soit sa taille, est désormais une cible. Les chances sont bonnes pour les attaquants : les compromissions sont donc plus courantes que jamais.

© Orange Cyberdefense

Unwetterartige Schauer und Gewitter sind am Samstag über große Teile Deutschlands hinweggezogen. Mit Ausnahme der Gebiete westlich des Rheins seien alle Regionen betroffen gewesen, teilte der Deutsche Wetterdienst (DWD) in Offenbach mit. Zwischen Schleswig-Holstein und Braunschweig gingen Hagelkörner mit einem Durchmesser von bis zu zwei Zentimetern sowie Regen von bis zu 20 Liter pro Stunde und Quadratmeter nieder. In Nordhessen kamen innerhalb von zwei Stunden sogar 30 Liter Regen pro Quadratmeter herunter. Am Sonntag besteht vor allem im Südosten des Landes Gewitterrisiko.

Koons neben seinem Kunstwerk

GETTY IMAGES/MARC COPPOLA

KUNSTWERK

Aufblasbare Ballerina von Koons enthüllt

Der Meister des Kitsches, Jeff Koons, hat in New York sein neues Kunstwerk vorgestellt: eine aufblasbare Ballerina. Bis zum 2. Juni dominiert die 14 Meter hohe Tänzerin den Platz vor dem Rockefeller Center, auf dem der 62-jährige Koons schon zwei Mal zuvor Werke präsentiert hat. Die Installation soll auf [illegible] der vermissten Kinder [illegible]achen, der im Mai

Mut [illegible] entdeckt

[illegible] in Mittelägypten [illegible]funden worden. [illegible]legten Kata- [illegible] Minja ent- [illegible]he Antiken- [illegible]rst Anfang [illegible]nahe Luxor [illegible] symboli- [illegible] der Zeit der

Wap-bap, ba-da

Abseits der Aufmerksamkeit der Erwachsenen prägt Bibi H. seit Jahren die Jugendkultur. Jetzt sorgt sie mit einem Song für Aufsehen. Ein Besuch

Gleich treffe ich Bianca Heinicke, besser bekannt als Bibi H., was ich normalerweise locker runterreiten würde, hätte ich nicht den Fehler gemacht, meinen Töchtern davon zu erzählen. Ich gebe zu, ich wollte etwas angeben, als ich beim Abendessen sagte: „Übermorgen treffe ich Bibi." Das hab ich jetzt davon. Jetzt begleiten mich die Autogrammwünsche und investigativen Erwartungen von zwei halben Berliner Schulklassen. Leistungsdruck, verdammt.

VON KATHRIN SPOERR

Bibi ist nicht mehr so ganz meine Alters- und ich bin nicht ihre Zielgruppe. Ihre Zielgruppe sind Mädchen ab sagen wir acht Jahren. Wo die Zielgruppe endet, hängt sehr vom einzelnen Mädchen und seiner Bereitschaft ab, Mädchen bleiben zu wollen. Einige finden sich schon mit elf zu alt für Bibi, andere sind schon so alt wie Bibi selbst, aber immer noch klein genug für sie.

Wap-bap, ba-da-di-da-da

Nicht wundern über dieses „Wap-bap". So heißt der neue Song von Bibi. Es ist schwer, ihn aus dem Kopf zu kriegen, wenn er einmal drin ist. In dem Song geht es um nicht viel. Um ein Mädchen, das gerade Pech hat, was aber nichts macht, weil es mit „Wap-bap" alles in den Griff kriegt. Der Song kam vor einer Woche raus, und es gab Riesengemecker deswegen. Außerdem riss er alle erdenklichen Rekorde. Das Gemecker ist der Grund, warum ich Bibi gleich treffe.

Sie werden dieses Lied wahrscheinlich nicht kennen, wenn Sie nicht zufällig minderjährige Töchter haben. Oder andersrum: Wenn Sie minderjährige Töchter haben, werden Sie wahrscheinlich sowohl diesen Song als auch Bibi kennen; Bibi vielleicht schon seit Jahren, wenn auch möglicherweise eher vom Weghören, wie ich.

Weghören ist die einzige Möglichkeit, wie Eltern die Vorliebe ihrer Töchter für Bibi aushalten können. Bibi betreibt seit fünf Jahren den YouTube-Kanal „Bibis Beautypalace". Mehrmals pro Woche stellt sie hier Videos ein, in denen es um nichts geht und um alles: Wie Bibi einkauft, verreist, wohnt, schläft und wieder aufwacht. Darum, wie sie gerade die Haare trägt, die Wimpern tuscht, die Lippen, die Wangen, die was auch immer schminkt. Es handelt sich um die hochnarzisstische Bespiegelung des Privatlebens der Kunstfigur Bibi, die vielleicht in Wahrheit gar keine Kunstfigur, sondern wirklich so ist, wie sie sich darstellt, aber wer weiß das schon.

Ihre Videos beginnen immer mit den gleichen Worten, nämlich mit „Hallihallo, meine Lieben", herausgepiepst mit einer zu den Worten passgenauen Stimme. Vielmehr als diese drei Worte kriegte ich bisher selten von Bibi mit, weil ich meine Kinder dann stets sofort und sehr deutlich aufforderte: „Bitte hört den Schwachsinn in euren Zimmern."

Letzte Woche kam dann Bibis Song heraus, seitdem interessieren sich auch Menschen jenseits der elf für Bibi. Der vollständige Titel ihres Liedes lautet: „How it is (Wap-bap ...)" Er brach mehrere Rekorde.

Und nun steht Bibi da, und sofort tut es mir leid, dass ich ihretwegen bereits das Wort Schwachsinn in den Mund genommen habe. Bibi trägt etwas sehr enges Schwarzes und sieht total hübsch aus. Sie sagt: „Hallo, ich bin Bibi", und ich erkenne den Sound in ihrer Stimme, und es ist völlig in Ordnung. Auf dem Fußboden hockt Julian, Bibis Freund, der ab und zu lächelt und ansonsten mit seinem Handy beschäftigt ist. Wir gehen rüber zum Sofa und setzen uns nebeneinander, und trotz der „good vibrations" kriege ich kurz einen heftigen Gehirnkrampf, weil ich mich frage, über was ich um Gottes Willen 20 Minuten lang mit Bianca Heinicke reden soll!? Über Schminktipps vielleicht oder über die lustigsten Pranks (für die älteren unter

© Orange Cyberdefense

Charl van der Walt
Head of Security Research
Orange Cyberdefense

Ce qui a bouleversé 2020

COVID-19 : L'impact caché

Afin d'examiner les problématiques liées à ce qui a véritablement et fondamentalement changé dans le paysage sécuritaire du fait de la pandémie et de la progression du télétravail, les trois questions suivantes se posent :

- Qu'avons-nous observé dans le comportement des attaquants ?
- Qu'avons-nous observé de la part de nos utilisateurs, quel a été leur comportement en matière de sécurité ?
- Qu'avons-nous observé en matière de résilience technologique, en particulier des technologies d'accès distant ?

Pour répondre à ces questions, nous nous aidons de données provenant de nos experts — CyberSOC, Vulnerability Intelligence, World Watch et Managed Services — ainsi que de certaines recherches menées par nos confrères d'autres entités.

Enfin, nous proposons des orientations pratiques quant à la manière de gérer cette crise — et des crises semblables si elles advenaient.

Que constatons-nous dans le comportement des attaquants ?

Nombreux sont ceux qui ont admis que les attaquants exploiteraient la pandémie pour augmenter et améliorer leurs attaques en recourant à trois attributs de la crise, à savoir :

1. La pandémie, ce «leurre» parfait : prétexte infaillible pour atteindre des victimes stressées, confuses, anxieuses et coincées chez elles.
2. Les utilisateurs, des cibles plus vulnérables : avides d'informations, désireux d'aider et psychologiquement plus vulnérables.
3. Des utilisateurs qui travaillent de chez eux, avec leurs équipements personnels : sans la sécurité offerte par un périmètre réseau d'entreprise, mal protégés et, donc, des cibles pour les cybercriminels.

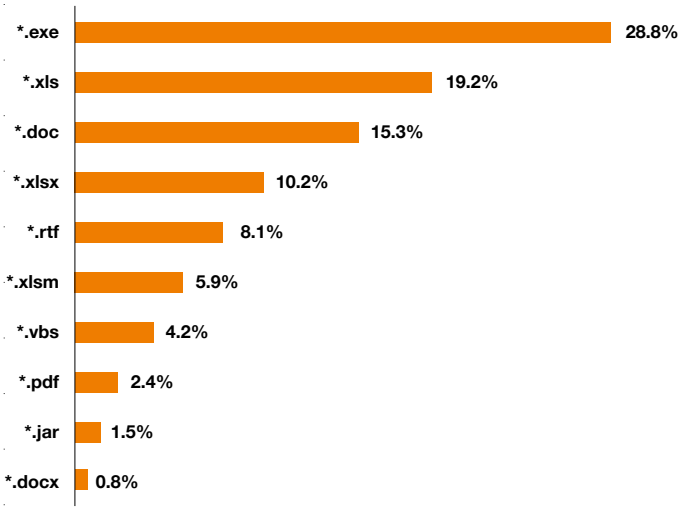
Les attaquants se sont-ils hâtés, comme prévu, d'exploiter la crise ? Voici ce que nous avons constaté…

Une bascule, mais brève, de la part des attaquants

Un rapport publié par Microsoft conclut que l'augmentation passagère des attaques liées au COVID-19 étaient des attaques connues. Il s'agissait d'infrastructures et malwares existants, apposés simplement à de nouveaux leurres. La tendance en matière de détection de malwares de par le monde (ligne orange des chiffres ci-dessous) n'a pas grandement varié durant ce laps de temps. Les attaques utilisant le COVID comme objet représentaient moins de 2 % des attaques relevées durant cette période.

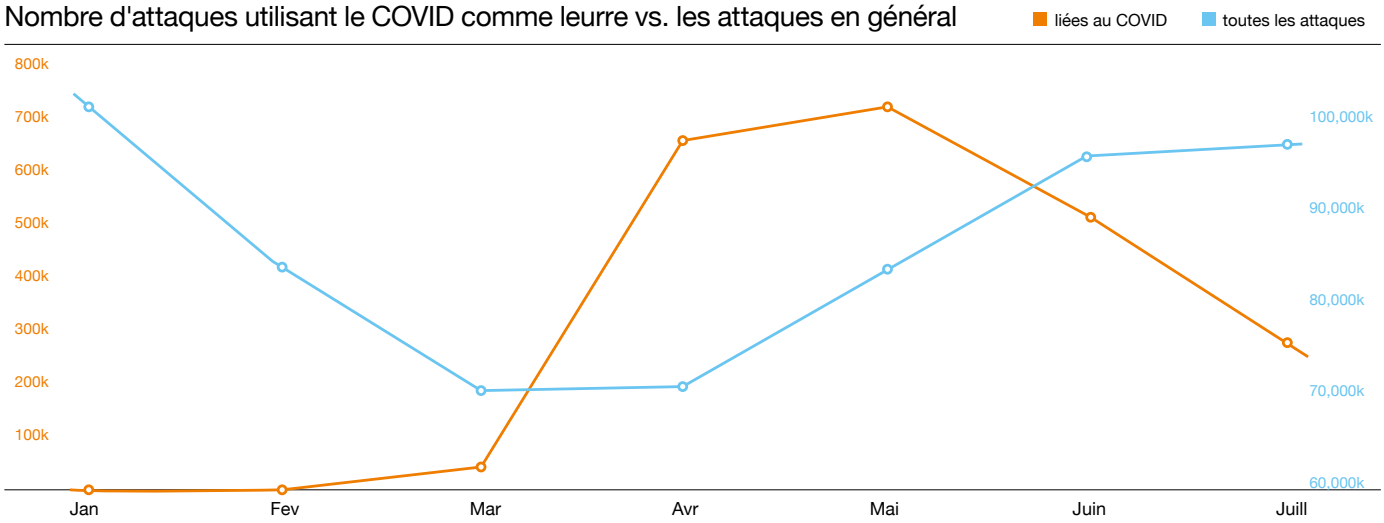
Nos propres données, retraçant l'enregistrement de nouveaux domaines DNS, montrent que les enregistrements inspirés par le COVID (avec des termes comme «covid», «corona» et «mask») ont rapidement chuté de début mai à fin juin. Parallèlement, nous avons vu émerger d'autres sujets, dont «Black Lives Matter», reflétant une réorientation de l'intérêt des médias, bascule aussi traitée par Microsoft dans son rapport.

Le tableau plus bas, par Check Point, relate la même histoire. Un changement de comportement est visible du fait de la crise sanitaire. Toutefois, la plupart des pièces jointes utilisées pour propager les malwares reste très «old school» (.exe, .xls et .doc) : le comportement des attaquants n'a donc que superficiellement et temporairement été modifié pendant la crise.



Attaques liées au COVID vs. toutes les attaques

Nombre d'attaques utilisant le COVID comme leurre vs. les attaques en général



© Orange Cyberdefense

En résumé :

- Les attaquants ont opéré une bascule rapide, bien que, pour l'essentiel, superficielle. Il est fréquent de voir de nouveaux leurres, thèmes et modèles, mais il est rare de leur voir appliquer des changements majeurs.
- Les cybercriminels ont eu recours au thème du COVID-19, mais pas longtemps. Les attaquants sont vite passés à d'autres sujets, ou à d'anciens sujets fiables. Le COVID-19 ne s'impose donc pas comme l'unique leurre.
- Les tactiques, techniques et procédures de l'écosystème cybercriminel conventionnel n'ont pas grandement été modifiées du fait du télétravail.
- Davantage d'indicateurs de «moralité» et «d'honneur» ont été observés chez les attaquants, bien que pas assez pour ralentir la montée des ransomwares et du «big game hunting».

Les acteurs étatiques : des personnes aussi

Le service World Watch d'Orange Cyberdefense œuvre pour ses clients à collecter, analyser, prioriser, contextualiser et résumer les menaces mondiales, par géographie et par secteur. Il fournit aussi des informations avancées sur les vulnérabilités, autant de données exploitables et pertinentes pour chaque métier, infrastructure, processus et application.

L'un des indicateurs de suivi que nous appliquons permet d'identifier les évènements de sécurité majeurs en lien avec des acteurs étatiques. Cet indicateur est utilisé pour suivre les travaux ou investissements gouvernementaux, les pirates soutenus par des Etats, les outils et capacités financés par des Etats (ainsi que les prestataires associés). Il permet aussi de savoir si nos signalements sont susceptibles d'être exploités par des acteurs étatiques au cours d'opérations offensives.

Un autre indicateur de tendance est appliqué aux scams, malwares, vols d'IP, à la désinformation, etc. en lien avec la pandémie.

Il nous sert à appuyer tout signalement centré sur la recherche en matière de COVID-19, dont la teneur est susceptible d'affecter les efforts de réponse à la crise, ou qui exploite le battage médiatique et l'anxiété générés par l'épidémie pour alimenter d'autres attaques, compromissions ou campagnes de désinformation.

En comparant la prévalence, au fil du temps, de ces deux types d'indicateurs dans nos bases, nous obtenons un aperçu du comportement des acteurs étatiques au cœur de la crise pandémique.

Nous indiquons les signalements labélisés «COVID-19» avec des barres bleues et ceux renvoyant à des acteurs étatiques au moyen de lignes orange.

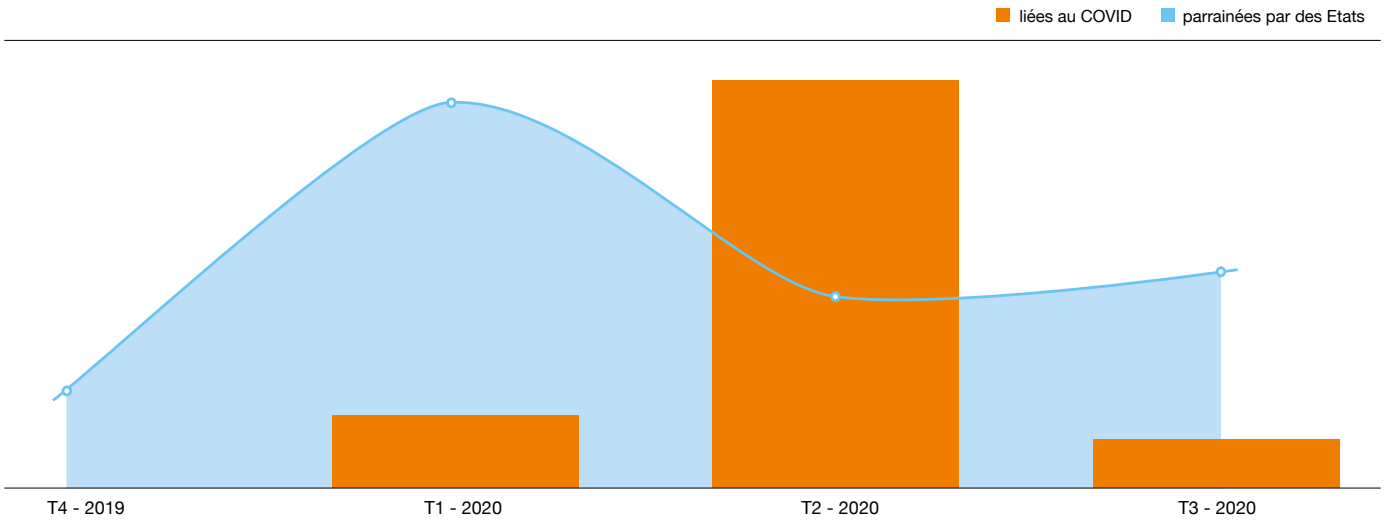
Le tableau ci-dessous montre l'émergence du COVID-19 comme thème dans d'importantes actualités sécurité en mars, avec un pic en mai, et une perte de vitesse après juillet. Ce constat est cohérent avec nos précédents commentaires sur la bascule des attaquants vers le sujet «COVID».

La ligne représentant les évènements en lien avec les Etats suit, néanmoins, une trajectoire bien différente. Selon nos données, le volume d'actualités ayant trait à des piratages étatiques connaît une légère progression au cours du premier trimestre, avant de retomber au second trimestre alors que la pandémie et les confinements étaient au plus haut, puis de remonter quelque peu au troisième trimestre.

Nous estimons que le creux d'activité au second trimestre tient autant à un malaise général dans l'industrie de la sécurité, qu'à des schémas d'activité de piratage étatique. Nous ne voyons pas de raison de penser que le piratage étatique a progressé du fait de la pandémie, ni même pendant la crise.

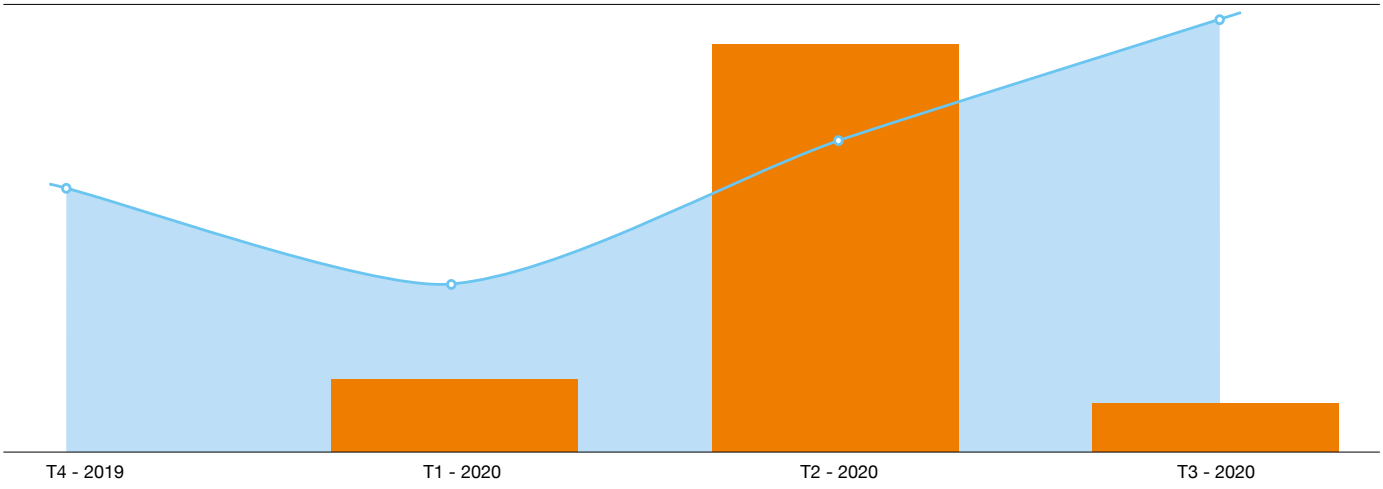
Nous pensons que les acteurs étatiques «formels» travaillent pour des gouvernements et se comportent donc comme la plupart des employés gouvernementaux (horaires fixes, congés et autres contraintes et avantages salariaux). En effet, l'activité imputable aux Etats pourrait avoir un peu diminué pendant la crise du COVID, puisque ces hackers auraient aussi été impactés par la pandémie et les confinements, à l'instar des autres départements gouvernementaux.

Attaques liées au COVID vs. parrainées par des Etats



Attaques liées au COVID vs. ransomwares

Nombre d'attaques utilisant le COVID comme appât vs. ransomware et extorsion



Ransomwares et perspectives

La trajectoire d'un autre indicateur de tendance — les ransomwares — s'impose comme parfait contrepoint et fournit des informations précieuses.

Après un léger recul au cours du premier trimestre 2020, une progression importante des incidents majeurs en lien avec des ransomwares a été observée dans nos données les mois suivants. Le recours aux ransomwares est soutenu par une combinaison de leviers systémiques, dont une demande insatiable, une offre de services limitée et des échanges monétaires fluides. Les monnaies virtuelles permettent des paiements peu chers, plus fiables, faisant des rançongiciels un modèle économique cybercriminel viable. Les sociétés proposent des assurances «cyber», ce qui fait du règlement des rançons l'option la moins coûteuse pour récupérer les données volées.

La différence de trajectoire entre piratage étatique (supposé s'intensifier pendant la crise, bien que ce ne fut pas le cas) et ransomwares (peu envisagés dans le contexte épidémique, mais ayant progressé régulièrement) tient dans des différences dans leurs facteurs systémiques sous-jacents.

Les activités de piratage étatique sont contraintes par les politiques, budgets, gouvernances, compétences et autres limites. Les priorités et cibles peuvent varier, et la pratique de ces activités peut augmenter au fil du temps. Un État ne peut cependant pas subitement produire davantage de ressources pour de nouveaux objectifs (par exemple : cibler les recherches liées au coronavirus) sans soustraire les compétences et ressources d'autres priorités. Nous estimons que, pour cette raison, les activités soutenues par les États n'ont pas changé comme beaucoup l'attendaient pendant la crise.

L'écosystème des ransomwares n'est pas contraint de la même manière et poursuivra inexorablement sa progression jusqu'à ce que lesdits leviers systémiques soient affectés d'une façon ou d'une autre.

La comparaison de ces deux tendances exemplifie l'importance de considérer et comprendre les facteurs systémiques à la base des problématiques de sécurité, plutôt que de réagir à des messages de la presse et des éditeurs sur le court terme.

En résumé :

- Comme les criminels, les acteurs gouvernementaux peuvent changer de cibles ou d'objectifs politiques.
- Cependant, ils sont contraints par leurs ressources et leurs opérations sont de plus en plus «formalisées». Le fait qu'ils basculent vers une nouvelle cible ne veut donc pas dire qu'ils augmentent leur activité.
- Il existe d'autres facteurs et forces systémiques majeurs que la pandémie ou le télétravail, et dont l'influence sur le comportement des attaquants est bien plus grande.

© Orange Cyberdefense

Que constatons-nous dans le comportement des utilisateurs ?

En général, les prévisions (voire aussi les analyses) des retombées sur la sécurité de la pandémie et des confinements spéculaient sur l'idée que les télétravailleurs seraient davantage ciblés et plus vulnérables aux arnaques du fait de la distance et du stress psychologique.

Nos données suggèrent que les attaques visant des individus (phishing, water holing et scams) ont été plus nombreuses que l'an dernier, mais n'ont pas fait les gros titres, peut-être du fait du confinement. Les lignes bleues soulignent les évènements liés au COVID-19, alors que les lignes orange indiquent des évènements de sécurité majeurs impliquant le facteur humain. Un examen plus approfondi des données suggère que ces types d'incidents diminuent en début de crise et augmentent légèrement par la suite.

Attaque ne veut pas dire compromission

Nous ne pensons pas non plus qu'il est possible de prouver que les attaques par ingénierie sociale se sont avérées plus fructueuses pendant la crise COVID.

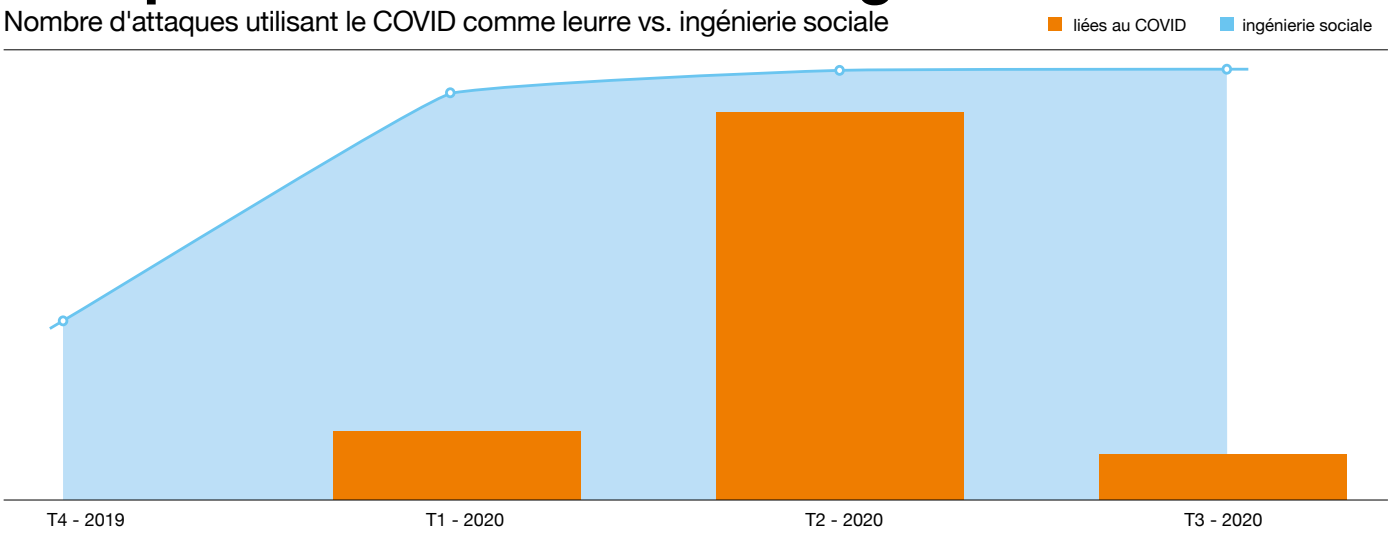
Des données open source très utiles, en provenance de l'université Temple (Critical Infrastructures Ransomware Attacks – CIRWA), listent les attaques par ingénierie sociale qui ont été rendues publiques (donc, fructueuses et pertinentes pour ce propos). Cet ensemble signale 623 compromissions pour les quelques dernières années. Les 70 attaques par ingénierie sociale communiquées sur les douze mois précédant le rapport CIRWA impliquent des techniques d'hameçonnage et de spear phishing. En portant une plus grande attention aux modèles sur cette période, nous observons une trajectoire similaire au volume d'incidents listés dans nos données.

Il existe des fluctuations dans les volumes mensuels, non visibles dans la présentation ci-dessus, mais nous ne pensons pas que les données soient suffisamment granulaires pour donner du sens à ces fluctuations. Les données CIRWA illustrent des pics d'activité en mars et en juin 2020, séparés par un important fossé en avril et en mai. Nous observons le même impact disruptif de la crise sur les industries informatique et sécurité, mais nous ne constatons pas de corrélation directe entre volumes de scams et crise COVID.

Compromis Compte BEC	2.86%
BEC - Fausse facture	2.86%
Compromis sur les courriels d'affaires	2.86%
Faux logiciels	5.71%
Phishing (hameçonnage)	52.86%
Robocall	2.86%
Spear Phishing	15.29%
Vishing	8.57%
Whaling	2.86%
Autres	4.29%

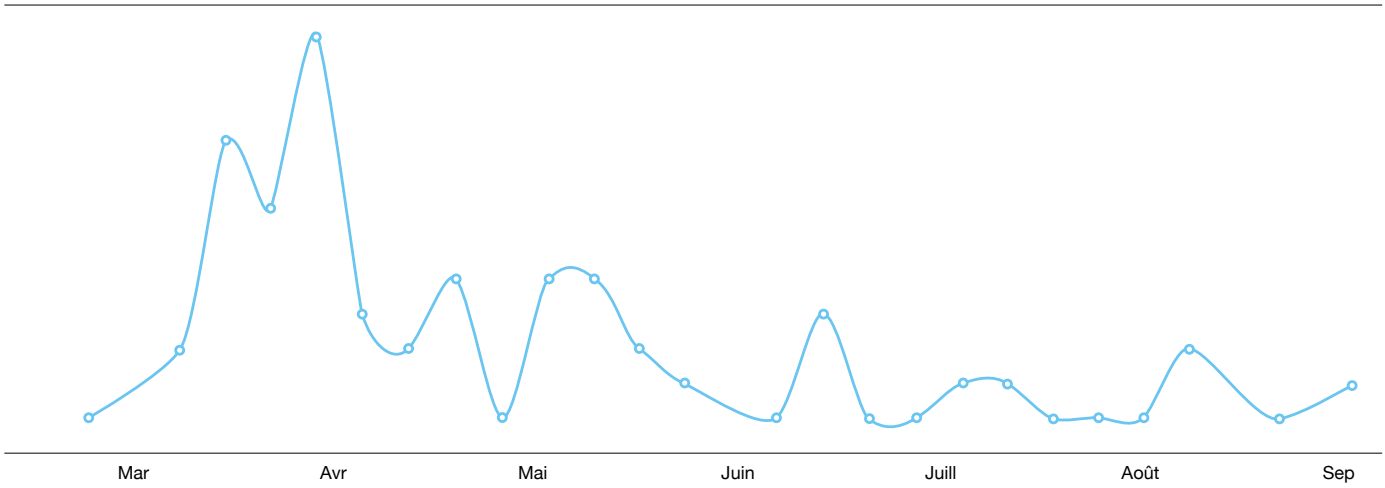
Attaques liées au COVID vs. ingénierie sociale

Nombre d'attaques utilisant le COVID comme leurre vs. ingénierie sociale



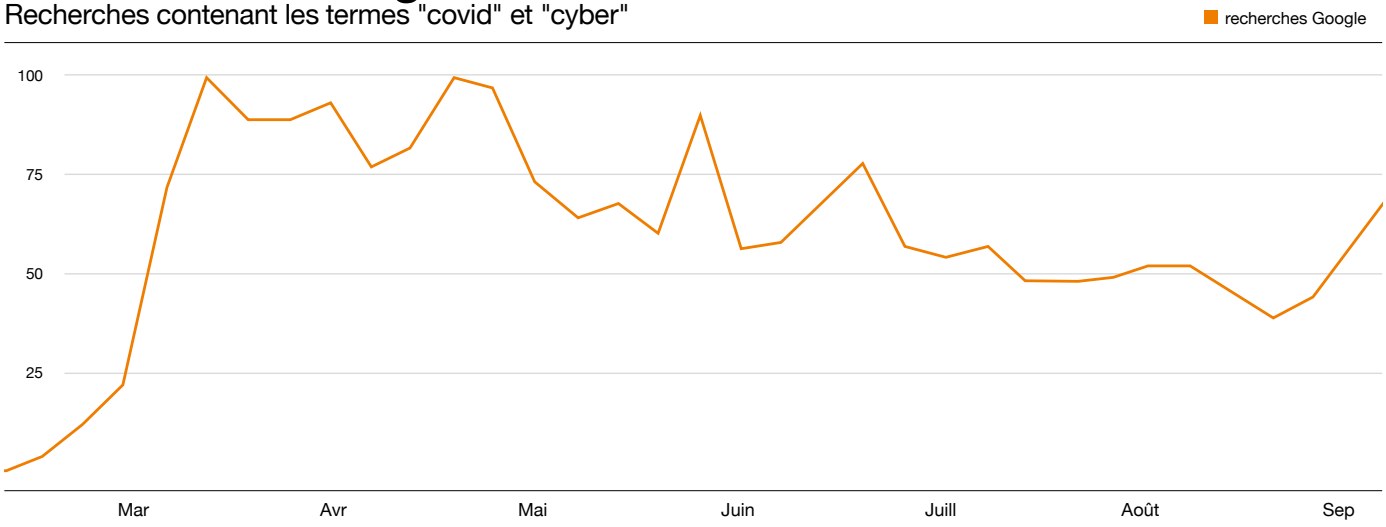
News de sécurité liées au COVID

Articles de presse sur la sécurité contenant les termes "covid" ou "corona" dans le titre



Recherches Google liées au COVID

Recherches contenant les termes "covid" et "cyber"



Couverture presse et intérêt

Dernière considération sur ce thème : le possible impact qu'auraient eu la couverture presse, la formation d'entreprise et les efforts communautaires proactifs sur la sensibilisation des utilisateurs et leur préparation à affronter les scams. Deux sources peuvent mettre cette question en lumière.

Le premier graphique illustrant nos données suit les articles de presse traitant de sécurité dans une sélection de publications majeures, où l'on trouve les termes «covid» ou «corona» en titre. Le second, de Google Trends, montre les recherches contenant les termes «covid» et «cyber». Il est clair dans ces deux ensembles que l'intérêt pour les problématiques de cybersécurité dans le contexte pandémique a augmenté en mars, s'est maintenu jusqu'à juin, avant de s'estomper.

Il se peut que les niveaux exceptionnels de couverture presse aient induit une sensibilisation suffisante du public comme des entreprises, évitant des conséquences bien pires que celles observées. De nos modèles d'expertise, nous voyons que beaucoup d'entreprises ont rapidement ajusté leurs programmes de sensibilisation et d'éducation à la sécurité en réponse au virus, et qu'elles sont parvenues à des niveaux satisfaisants de réponse de la part de leurs utilisateurs.

En résumé :

- Vulnérabilité des utilisateurs :
  - Pas de preuve que les utilisateurs ont véritablement été plus vulnérables aux scams qui recourraient à la thématique COVID.
  - Possible résultat d'importants efforts proactifs.
  - Existence d'une proportion d'utilisateurs invariablement vulnérables au phishing et aux scams, mais visiblement pas du fait de l'impact du COVID-19.
- Réponse des utilisateurs :
  - Assimilation rapide des utilisateurs qui ont appris comment identifier et répondre aux escroqueries inspirées du thème COVID.
  - Préférence des attaquants pour des modèles «traditionnels», par exemple, des e-mails de phishing ciblant des portails de banque en ligne ou Office 365.
- Recettes des attaquants :
  - Pas d'augmentation notable des volumes de transactions illégales en BTC au cours de la période de confinement.
  - Pas de preuve d'augmentation des profits des attaquants durant la période de confinement.

© Orange Cyberdefense

Quid des technologies de sécurité ?

Du fait de déploiements rapides et à grande échelle de technologies d'accès distant (dont les VPN), ces systèmes seraient mal configurés et maintenus, donc plus souvent ciblés par les attaquants, et permettraient plus de compromissions pour ces types de systèmes.

Plus d'accès

Les données de notre entité Managed Services Operations sur les requêtes de service concernant les technologies VPN montrent à quel point l'adoption de technologies d'accès distant sécurisées a progressé dans le monde entier.

Ce graphique montre les niveaux de demande issus de notre SOC MSSP pendant la crise COVID. L'augmentation du nombre de demandes d'installation, d'assistance et de service pour des technologies de sécurité périmétrique au début du confinement est évidente, reflétant ce que les données externes nous disent.

Une de ces sources, top10vpn.com, rapporte que :

1. La demande globale de solutions VPN a augmenté de 41 % au cours de la seconde moitié du mois de mars, et reste 22 % supérieure aux niveaux pré-pandémie.
2. Dans 75 pays, d'importantes augmentations de demandes de solutions VPN ont été enregistrées depuis que les restrictions sociales imposées par la crise sanitaire ont commencé à être appliquées.
3. Dans 21 pays, la demande de solutions VPN a plus que doublé.
4. Plus forts volumes en matière de demandes de solutions VPN : États-Unis (+ 41 %), Royaume-Uni (+ 35 %) et France (+ 80 %).
5. Plus fortes augmentations en matière de demandes de solutions VPN : Égypte (224 %), Slovénie (169 %) et Chili (149 %).
6. Plus importantes augmentations continues : Égypte (154 % — sur 14 jours depuis le pic initial), Pérou (119 % — sur 28 jours depuis le pic initial), Afrique du Sud (105 % — en cours, depuis mi-mars).

Plus de vulnérabilités

Comme illustré dans une autre section du rapport de cette année, nous observons une anomalie dans nos données concernant les vulnérabilités au cours de la crise COVID : en conjonction avec l'accroissement des déploiements de technologies de sécurité, nous constatons une augmentation exceptionnelle du nombre de vulnérabilités remontées (pas nécessairement des attaques) pour ces types de systèmes (dont les technologies de Check Point, Cisco, F5, Fortinet, Juniper, Palo Alto, Pulse & Symantec-Bluecoat, entre autres).

Nous estimons que cette progression spectaculaire du nombre de vulnérabilités dans des produits de sécurité est fonction des facteurs suivants :

1. Le «succès» évident de la vulnérabilité CVE-2019-11510 dans Pulse, datant de mai l'an dernier, qui a été exploitée dans de multiples attaques notoires.
2. L'adoption ou l'expansion rapide, voire irréfléchie, des accès distants sécurisés pour faciliter le télétravail, faisant de ces technologies des cibles de choix.
3. Un effet domino par lequel la découverte d'une vulnérabilité procure connaissance, expérience et idées, menant à la découverte d'autres vulnérabilités dans le même produit, ou de vulnérabilités similaires dans des produits différents.

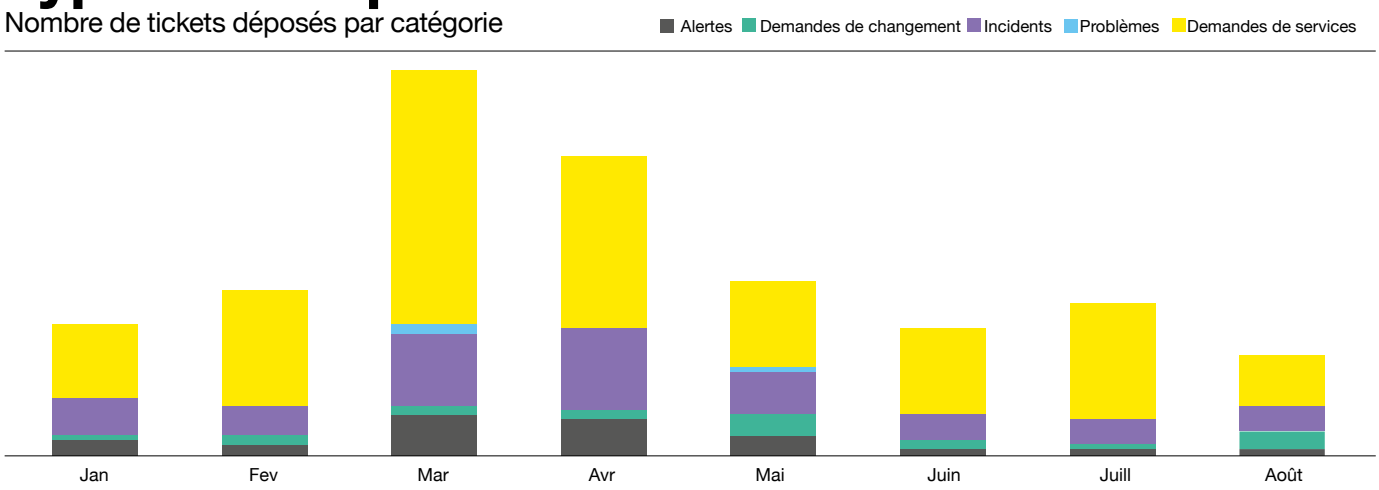
Plus d'attaques

Plusieurs vulnérabilités découvertes récemment dans des produits de sécurité périmétrique sont devenues des cibles répandues d'attaque pour les cybercriminels, comme REvil, et ont joué un rôle pivot dans quelques-unes des principales compromissions l'an passé.

Elles sont aussi répandues chez les acteurs étatiques. Dans un récent bulletin (Advisory) publié par la NSA (intitulé State-Sponsored Actors Exploit Publicly Known Vulnerabilities), 25 vulnérabilités connues et activement utilisées par des acteurs étatiques sont listées. Six de ces 25 vulnérabilités impliquent des technologies de sécurité périmétrique.

Types de requêtes

Nombre de tickets déposés par catégorie



Gérer la crise

À la lumière des menaces et préoccupations décrites précédemment, les recommandations suivantes s'appliquent aux entreprises et professionnels forcés de faire face à la composante cyber de la crise sanitaire. Le virus impacte la cybersécurité, mais ses conséquences ne sont pas inévitables.

Ne pas paniquer

Nos recommandations sont les suivantes :

1. Comprendre que vous faites face à un **niveau de menace plus élevé, mais que le niveau de vulnérabilité n'a que légèrement augmenté.** Nous ne pouvons contrôler la menace, mais nous maîtrisons la vulnérabilité. Il convient donc de se concentrer sur ce point.
2. **Identifier ce qui a changé et ce qui demeure inchangé.** Votre modèle de gestion des menaces peut, ou non, s'avérer très différent aujourd'hui de ce qu'il était hier. S'il est inchangé, votre stratégie et vos opérations n'ont pas, non plus, besoin d'être modifiées.
3. **Maintenir le contexte.** Aujourd'hui, la crise est médicale et humaine. Ne laissez pas le battage médiatique autour de la cybersécurité vous distraire de cette réalité. Internet survivra.
4. **Concentrer vos efforts.** Vous ne serez en mesure d'accomplir que peu de choses en mode dégradé. Consacrez temps et énergie à identifier vos préoccupations premières : concentrez-vous sur ces priorités.
5. **Prendre le temps de s'améliorer.** Si certains points de votre infrastructure ou de vos processus n'étaient pas prêts quand la crise s'est déclarée, il est temps, à présent, de les passer en revue et de les améliorer.

Surveiller vos prestataires

Pour beaucoup d'organisations, il existe un lien direct entre le niveau de sécurité des prestataires et le leur. Cette corrélation a récemment été illustrée par des incidents dont ceux liés à la campagne notPetya. Par temps de risque accru, les entreprises doivent se préoccuper du niveau de sécurité de leurs fournisseurs et partenaires autant que du leur.

Les équipes sécurité et de gestion des risques devraient envisager l'ouverture et la maintenance de canaux de communication avec les fournisseurs, prestataires, consultants et partenaires susceptibles d'avoir accès à des systèmes ou données sensibles. En ce moment, elles doivent s'enquérir de leurs réponses à l'élévation du niveau de risque, s'assurer qu'elles sont adaptées et conformes à leurs attentes.

Définir les priorités

Comme énoncé plus tôt, il faut concentrer nos maigres ressources sur les menaces qui nous préoccupent le plus aujourd'hui. Définir quelles sont les plus « importantes » n'est, toutefois, pas chose aisée. Ce défi, nous en avons déjà parlé. Nous estimons que l'éventail des menaces cyber (même hors crise mondiale) est de loin trop complexe et coulant pour être réduit à une simple liste ou fiche-mémoire. Malgré tout, au risque de tomber dans ce piège, nous recommandons d'envisager les priorités en temps de crise au prisme de deux réalités : ce qui a changé et ce qui n'a pas changé.

Ce qui a changé

Il doit paraître clair à la lecture de ce document que nous pensons que seule une part limitée des cybermenaces a considérablement changé du fait de la pandémie, à savoir :

1. Vos employés sont plus vulnérables à l'ingénierie sociale qu'à l'accoutumée.
2. Vous disposez de moins de contrôle et de visibilité que d'habitude sur les systèmes informatiques que vous protégez.
3. Vos utilisateurs peuvent se connecter depuis des systèmes et environnements fondamentalement peu sûrs ou mal configurés.
4. Vous vous êtes empressés de mettre à disposition des systèmes d'accès distants sans pour autant disposer de temps pour les planifier ou les exécuter comme vous l'auriez souhaité.
5. Vos prestataires, vos équipes et vous-mêmes êtes amenés à fonctionner en mode dégradé, en effectif réduit.

Ce qui n'a pas changé

Au regard de l'Histoire récente, nous traversons une période sans précédent, mais du point de vue des menaces cyber, rien de fondamentalement nouveau n'est observable. Nos priorités cyber n'ont donc pas besoin de différer de trop de ce qui avait été défini avant la crise :

1. Les attaques par ingénierie sociale, dont les compromissions d'e-mails professionnels (Business Email Compromise – BEC), ne sont pas nouvelles. Les réponses n'ont pas non plus changé en dépit d'un niveau de risque plus élevé.
2. Les attaques portant sur les interfaces cloud, systèmes d'accès distants et passerelles VPN se sont multipliées au fil du temps. Bien que peut-être plus poussées, ces tentatives ne sont pas nouvelles.
3. Le télétravail et la facilitation des accès distants sécurisés pour travailleurs nomades sont des problématiques bien comprises. Nos boîtes à outils comptent diverses technologies et approches adaptées à presque tous les budgets et niveaux de sophistication technique.
4. Depuis deux décennies, l'espace de travail est devenu mobile. Les éditeurs et équipes informatiques peuvent fournir plusieurs méthodes de suivi, de maintenance et de gestion des terminaux distants (endpoints). Il est aussi aisé de répondre à des exigences plus complexes, dont l'isolation et du tri à distance, même sans un budget conséquent.

Instituer des procédures et systèmes de réponse d'urgence

La préparation est essentielle. Prenez le temps d'organiser une séance de planification en présence d'acteurs informatiques et sécurité, afin de penser vos capacités de réponse en cas de suspicion de compromission ou de fuite. Les points à considérer sont notamment les suivants :

- Comment détecteriez-vous une fuite ? De quels indicateurs disposeriez-vous outre les éléments traditionnels (à savoir, les notifications d'utilisateurs ou de prestataires externes) ?

© Orange Cyberdefense

- Qui doit être informé et mis à contribution en cas de crise ?
- Comment une équipe de réponse à incident doit-elle communiquer et collaborer, même dans le pire des scénarios, où les systèmes de confiance pourraient avoir été impactés ?
- Comment communiqueriez-vous avec les autres parties prenantes : les utilisateurs, régulateurs, clients, membres du conseil d'administration et actionnaires ?
- Êtes-vous en mesure d'isoler un poste ou un serveur, à distance ou sur site ?
- Avez-vous accès à une équipe de réponse à incident apte, en interne ou par le biais d'un partenaire ?
- Disposez-vous d'une politique de sauvegarde et d'un plan de reprise d'activité ? Quand ont-ils été testés pour la dernière fois ? Pourraient-ils être testés aujourd'hui ?
- Disposez-vous d'une politique de réponse en cas d'attaque par ransomware ou d'extorsion ? Si vous pensez que vous paieriez une rançon, avez-vous les moyens financiers et systèmes requis pour vous en acquitter ? Il vous faudrait aussi penser à une stratégie de négociation et désigner par avance une équipe dédiée.
- Comprenez-vous les exigences règlementaires (RGPD, LPM…) ? Êtes-vous prêts à vous y plier en cas de fuite d'informations ?

Mettre à disposition une hotline d'assistance sécurité

Vos utilisateurs éprouvent en ce moment une grande anxiété, sans doute aggravée par les menaces cyber.

Il serait opportun de leur fournir, voire même aux clients, un numéro ou une adresse leur permettant de discuter avec quelqu'un de façon raisonnée des attaques techniques et cognitives qu'ils pourraient suspecter, ou de leurs propres systèmes et comportements. Il s'agit d'un puissant moyen de réduire les niveaux d'anxiété, tout en améliorant votre sécurité. Si vous disposez déjà d'une ligne directe d'assistance, préparez-vous (au moins au début) à une rapide augmentation des volumes d'appels, d'e-mails ou de tout autre moyen de communication disponible.

Revoir les procédures de sauvegarde et de reprise d'activité

Les ransomwares et dénis de service sont des menaces avérées, antérieures à la crise, qui semblent s'être accentuées du fait de la pandémie.

Prenez le temps de vérifier l'état de vos sauvegardes ainsi que la disponibilité de vos données et de vos procédures de reprise d'activité.

À cette étape, il vous faut penser aux employés en télétravail et aux données avec lesquelles ils pourraient travailler en local. Si vous ne disposez pas déjà d'un système de sauvegarde dédié aux utilisateurs distants, des solutions cloud publiques clé en main type Google Drive, Dropbox ou Microsoft OneDrive sont des alternatives viables au vu des circonstances.

Garantir un accès distant sécurisé

La fourniture d'un accès distant sécurisé et fiable à Internet et aux systèmes d'entreprise s'impose aujourd'hui comme le plus grand des défis pour nos clients. Les principes suivants devraient servir à guider la conception de toute architecture d'accès distant :

1. Bien comprendre votre modèle de gestion des menaces. Nous estimons qu'à ce point le premier défi est de mettre en place des procédures d'authentification et de contrôle d'accès adaptées aux données et systèmes d'entreprises.
2. S'assurer de sécuriser les DNS. Plusieurs attaques impliquent aujourd'hui des redirections de requêtes DNS pour afficher des sites d'hameçonnage (phishing) ou mener à bien des attaques de type Person-in-the-middle. Contrôlez les serveurs DNS que vos employés utilisent, soit par le biais de configurations VPN, soit, simplement, en imposant de coder en dur les résolveurs DNS au niveau des terminaux.
3. Mettre en place des mécanismes d'authentification multi-facteurs. Vérifiez tous vos systèmes d'accès distants (dont les interfaces Web, VPN et passerelles d'accès distant) et demandez-vous comment des procédures d'authentification forte peuvent être mises en place. Les solutions d'envoi de notifications sur mobile — disponibles auprès de sociétés comme Okta, Duo, Google ou Microsoft — peuvent être de bonnes options en termes d'ergonomie, de sécurité, voire aussi de simplicité de déploiement.
4. Rendre sa politique de mots de passe claire et communiquer sur les bonnes pratiques. À nouveau, nous insistons, les attaques à l'encontre des technologies d'accès distant comptent parmi les menaces principales. Si vous n'êtes pas en mesure de mettre en œuvre des procédures d'authentification multi-facteurs fortes, réfléchissez à comment pousser vos utilisateurs à choisir des mots de passe forts. Ils devraient être encouragés à :
   - Changer leur mot de passe.
   - Choisir un mot de passe qu'ils n'ont jamais utilisé ailleurs.
   - Choisir une phrase de passe suffisamment longue, mais facile à retenir, plutôt qu'un mot de passe court et complexe.
5. Gérer vos équipements de sécurité. Certaines campagnes ciblent activement des systèmes d'entreprise spécifiques comme les serveurs Citrix Application Delivery Controller (NetScaler ADC) et Citrix Gateway (NetScaler Gateway), Zoho ManageEngine Desktop Central, Cisco RV320 et les routeurs RV325. Les serveurs VPN Pulse Secure non-patchés comptent aussi parmi les cibles communes. Ces attaques exploitent des vulnérabilités connues et corrigées. En d'autres termes — elles sont avérées, mais elles ne sont pas difficiles à corriger. Assurez-vous de savoir où se trouvent vos systèmes d'accès distant, et qu'ils sont tous correctement patchés et configurés.

Rendre visibles les terminaux distants

Avec le développement du télétravail, les entreprises ne présentant pas de dispositifs robustes de détection et de protection de leurs terminaux ou de remédiation aux incidents se retrouvent dans le noir à la veille d'une crise. Elles doivent désormais se pencher sur les options qui s'offrent à elles. Les voies suivantes sont évidentes et s'appliquent à la majorité des configurations de terminaux :

1. Microsoft Sysmon : Le logiciel gratuit System Monitor (Sysmon) de Microsoft est constitué d'un service et d'un pilote Windows qui, une fois installé, persiste au fil des redémarrages pour surveiller et journaliser l'activité système au sein d'un journal d'évènements. Il fournit des détails sur les créations de processus, les connexions réseau, les modifications d'horodatage de création de fichiers, etc. En collectant ces évènements avec Windows Event Collection ou un agent de gestion des incidents et évènements sécurité (SIEM), puis en les analysant, vous pouvez identifier des activités malveillantes ou anormales. Sysmon est relativement sûr et simple à déployer ; il supporte la majorité des versions Windows actuelles. Il existe un grand nombre de projets commerciaux et open source pouvant vous assister dans les tâches de configuration, de gestion, de collecte et de reporting.
2. Les EDPR professionnels : Divers éditeurs, dont Crowdstrike, Cybereason, Cylance, Palo Alto Traps, SentinelOne et bien d'autres, proposent des outils de détection, de protection et de réponse à appliquer au niveau des terminaux (Endpoint Detection, Protection and Response). Beaucoup de ces solutions sont très fiables et se sont montrées efficaces. Certaines présentent aussi des fonctionnalités d'« isolation » permettant de mettre un terminal en partie hors-ligne le temps de trier les incidents et d'enquêter. Ces solutions sont aussi disponibles en infogérance pour en accélérer la mise en œuvre.

Outre ces solutions évidentes, il existe d'autres options permettant d'arriver au même but. Par exemple, des agents VPN peuvent être utilisés pour isoler un réseau virtuel, et des produits open source, comme Remote Response de Google (GRR), présentent des options de tri et de forensics.

Ne pas oublier les applications mobiles malveillantes

Nous avons remarqué que le nombre d'applications mobiles malveillantes a quintuplé entre février et mars 2020. Nous pensons que cette tendance persistera à mesure que la crise se propagera.

Face aux applications malveillantes, les options pour les sociétés sont, par exemple :

- D'interdire l'installation de toute application tierce.
- D'établir des listes blanches permettant l'installation d'applications autorisées uniquement.
- De s'assurer que les applications n'obtiennent que les permissions strictement nécessaires sur l'outil mobile.
- D'implémenter un conteneur sécurisé pour isoler les données de l'organisation des autres données et applications sur l'outil mobile.

Pour la majorité des entreprises, la seule solution technique concrète est de doter leurs utilisateurs d'un antivirus mobile, ou de leur procurer des outils mobiles d'entreprise sur lesquels sont installés des logiciels de gestion de terminaux mobiles (Mobile Device Management – MDM).

Penser à patcher et durcir la sécurité des terminaux distants, dont les outils mobiles

Le 25 mars, nous avons émis une alerte sécurité (Security Advisory) portant sur deux vulnérabilités zero-day critiques dans les systèmes Windows. Microsoft a averti que des attaques limitées et ciblées avaient été détectées sur le terrain.

Avant encore, le 11 mars, nous avons averti nos clients de l'existence d'une vulnérabilité d'exécution de code à distance (Remote Code Execution) dans le protocole Microsoft Server Message Block 3.1.1 (SMBv3). Cette vulnérabilité permettait à un attaquant d'exécuter du code sur le serveur ou le client SMB cible.

Des vulnérabilités de ce type sur les serveurs et postes Windows continuent à voir le jour et sont activement exploitées. Le même risque s'applique aux terminaux mobiles, outils tant personnels que privés. Bien que nous ne pensions pas qu'il s'agisse du vecteur d'attaque le plus probable à ce jour, ces terminaux ne peuvent être ignorés. Les négliger exposerait votre entreprise à des risques évitables.

Une fois ces priorités adressées, des efforts doivent être investis dans la manière dont les terminaux distants peuvent être patchés aujourd'hui. Une option viable (au lieu d'une solution de correction centralisée) pourrait être d'informer les utilisateurs des correctifs essentiels par biais de communications d'entreprise et de leur demander de les appliquer directement.

Cette réponse est loin d'être idéale, mais, comme indiqué plus tôt, en ce moment chaque endpoint compte.

Un enseignement à tirer

Enfin, nous pensons que l'impact de cette pandémie et notre réponse collective sont riches en enseignements pour les spécialistes de la sécurité. Le virus montre à quel point nos sociétés et nos économies sont interconnectées, et jusqu'où une catastrophe dans un domaine se répercute sur les autres secteurs. En répondant à la crise, nous apprenons à évaluer l'impact que peut avoir notre comportement sur la société entière, et non simplement sur nous en tant qu'individus, familles ou entreprises. Cet enseignement est essentiel pour la communauté de la sécurité.

© Orange Cyberdefense

Les priorités que nous proposons

Sur la base de la répartition détaillée plus haut, nous proposons aux entreprises de prendre en compte les priorités suivantes au regard de l'état actuel des menaces.

Si vos priorités sécurité ne sont pas encore clairement définies, nous vous suggérons de vous concentrer sur les réponses suivantes, par ordre d'importance :

1. Définir des procédures et systèmes de réponse d'urgence.
2. Mettre en place une hotline dédiée à l'assistance sécurité.
3. Vérifier vos sauvegardes et votre plan de reprise d'activité.
4. Doter vos utilisateurs des informations requises pour prendre de bonnes décisions.
5. Fournir des accès distants sécurisés.
6. Rendre visibles les terminaux distants.
7. Prendre en compte les applications mobiles malveillantes.
8. Penser à corriger et durcir la sécurité des terminaux distants, mobiles inclus.
9. Vérifier votre assurance.

Conclusion

Au plus fort de nos constatations : le progrès spectaculaire d'une dépendance à des technologies jusque-là sous-considérées (dont la visioconférence et les outils collaboratifs), une bascule des systèmes d'entreprise vers le cloud, et une augmentation sans précédent du commerce en ligne.

Le vrai impact de la crise COVID et des confinements sur la cybersécurité ne tient donc pas dans des conséquences vives et évidentes (comme une augmentation des cas de phishing ou le ciblage de l'industrie de la santé par les attaquants), mais dans des conséquences plus larges encore, systémiques, pouvant être résumées comme suit :

- L'adoption massive ou l'expansion de capacités d'accès distant, menant à une augmentation des frais de gestion pour les équipes sécurité et l'élargissement de la surface d'attaque pour les adversaires.
- L'importance croissante des technologies d'accès distant pour les entreprises, faisant d'elles des cibles plus attractives et plus difficiles à maintenir, mettre à niveau ou corriger.
- L'intérêt croissant des attaquants pour ces technologies d'entreprise du fait de leur exposition sur Internet et du niveau élevé des accès qu'elles permettent si compromises.

D'autres facteurs systémiques — pour certains liés à la pandémie, d'autres indépendants — continuent de façonner l'environnement des menaces. L'impact systémique de la pandémie sur la cybersécurité n'est pas encore manifeste, mais une incroyable transition vers le cloud, l'accélération sans précédent du e-commerce et une soudaine dépendance à des technologies antérieurement sans importance (visioconférence, par exemple) influeront sans doute sur l'impact déjà visible du progrès des accès distants, pour garnir les emplois du temps des attaquants, comme des RSSI.

© Orange Cyberdefense

© Orange Cyberdefense

Charl van der Walt
Head of Security Research
Orange Cyberdefense

Tech insight :

Au cœur de la cybercriminalité

Notre métier est de détecter d'éventuelles attaques et de défendre nos clients. Notre mission : protéger leurs essentiels. Pour ce faire, nous analysons attaques et vulnérabilités et tâchons de prédire les actions des attaquants pour garder un temps d'avance. Si nous répondons souvent à cette question : « Que font les attaquants et comment ? », il en temps de se demander :
« Pourquoi attaquent-ils ? ».

Jetons donc un œil du côté obscur de la force… Certaines attaques, pourtant communes, gagnent en sophistication même si les menaces avancées et persistantes (APT) de premier ordre restent rares. Le nombre d'attaques décroit considérablement en période de vacances : la cybercriminalité est devenue un métier. Comment fonctionne-t-elle ? Quels en sont les modèles économiques ? Comment les criminels travaillent-ils ensemble ? Quels usages font-ils des biens numériques, propriétés intellectuelles, identifiants, numéros de carte, données médicales… qu'ils dérobent ? Comment ces éléments sont-ils monétisés?

De nouvelles réalités

Il est désormais admis que la cybercriminalité est devenue une industrie majeure. Selon le Global Risks Report 2020 du Forum économique mondial (FEM), d'ici 2021, les dommages qu'elle cause pourraient atteindre 6 000 milliards de dollars. Toujours selon l'enquête, les cyberattaques s'imposeront comme le second risque le plus préoccupant pour le commerce mondial les dix prochaines années.

Les cybercriminels ne disposent pas tous de compétences très techniques. De nos jours, il existe des services de Crime-as-a-Service (CaaS) leur permettant de mener des opérations. Ce type de services a vraisemblablement déjà induit une augmentation des volumes de cybercriminalité. Les criminels n'ont plus besoin de disposer de plusieurs années d'expérience en piratage ou de connaissances en matière de malwares pour se lancer. Selon le rapport du FEM, les deux services les plus populaires sont les attaques par ransomware et par déni de service (DDoS). Cette professionnalisation se reflète aussi dans les chiffres. Les attaques hautement critiques restent relativement rares. Toutefois, ces dernières années, nous avons observé une évolution importante : de plus en plus d'incidents ne sont, non pas faiblement, mais moyennement critiques.

Les Ransomwares et DDoS : ces menaces les plus communes

Selon le FEM, les vecteurs d'attaques les plus prisés sont les ransomware et les DDoS. Les cybercriminels s'allient pour former des groupes spécialisés, collaborer et constituer un réseau interconnecté. Ils s'organisent comme des entreprises et font usage de pratiques courantes : service client, assistance après-vente, etc.

Cette « sagesse commune » est fréquemment citée et souvent partagée, sans que beaucoup comprennent vraiment les réalités qu'elle sous-tend. Un élément critique en matière de cybercriminalité — peut-être moins bien compris qu'il le devrait — réside au cœur du problème, à savoir : les flux monétaires et la valeur partagés par différents acteurs dans l'écosystème cybercriminel.

Cet écosystème abrite une myriade d'acteurs, chacun ayant ses expertises propres et ses façons de monétiser des produits tels que malwares, botnets, informations volées par exemple. Une pleine compréhension de cet écosystème et de ses leviers systémiques est essentielle pour atteindre le cœur de la problématique cybercriminelle et développer une stratégie qui nous permettrait de l'attaquer à la racine.

Dans cette section, nous nous concentrerons sur les principaux acteurs de cet écosystème ainsi que sur leurs liens possibles pour dépeindre leurs interactions plus clairement.

Les places de marché

Le Dark Web est cette partie d'Internet où les serveurs utilisent Tor, I2P, GNUNet, ZeroNet ou Freenet pour cacher leurs adresses IP. Le Dark Web le plus fréquenté est accessible depuis le navigateur Tor, où les sites disposent de noms de domaine se terminant en .onion. Comme il n'est pas simple de se rappeler des noms de domaine (3g2upl4pq6kufc4m.onion est, par exemple, l'adresse .onion de DuckDuckGo), plusieurs moteurs de recherche font de leur mieux pour indexer ces sites.

Parmi ces moteurs de recherche : Torch, Kilos, Candle, notEvil, Haystak, entre autres. Il existe aussi des moteurs sur le Clearnet pour les services cachés de Tor, comme Ahmia, ou simplement des pages Web intégrant des liens vers des sites sur le Dark Web, comme Hidden Wiki.

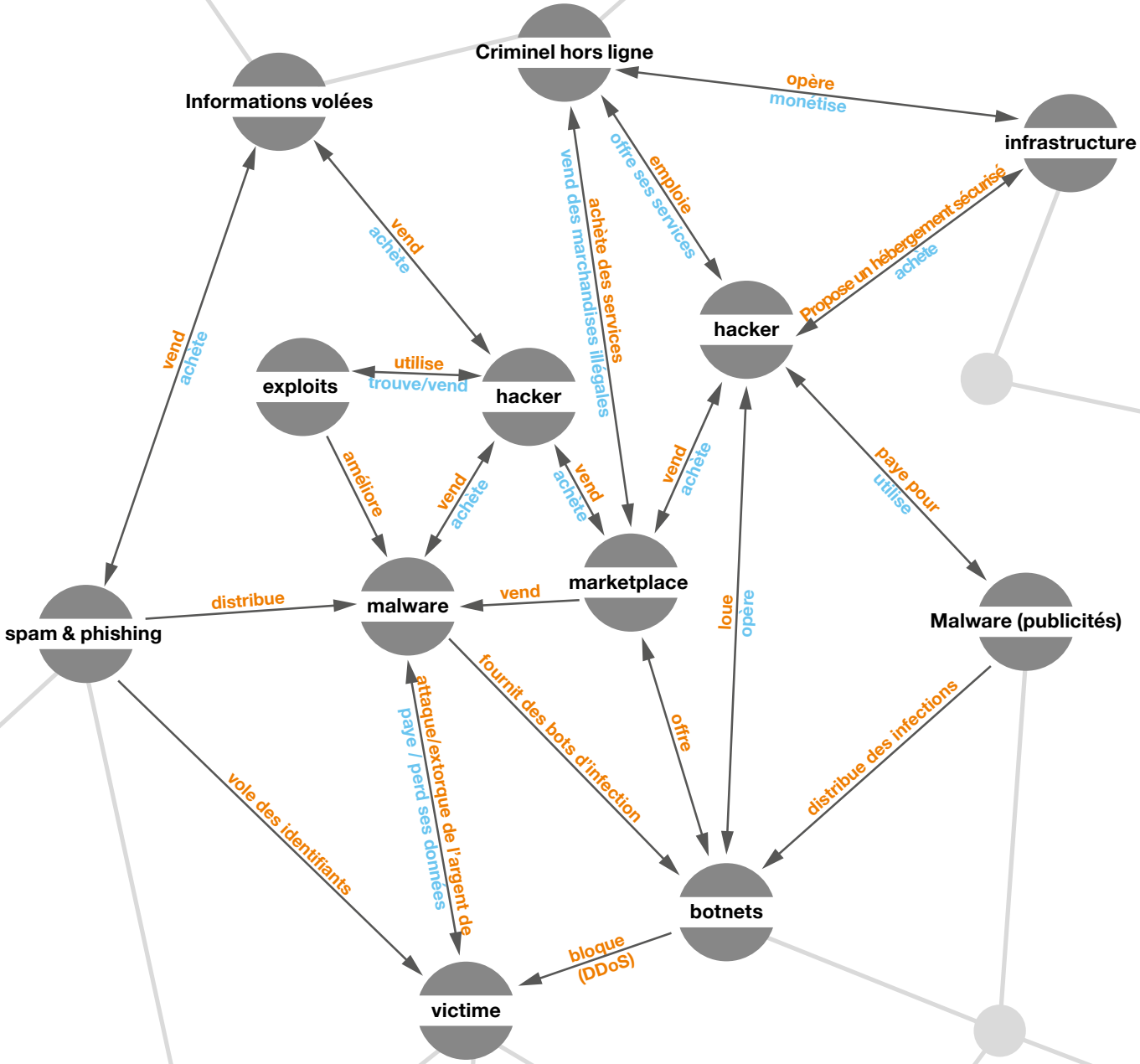
Il faut préciser que le Dark Web est différent du Deep Web, une partie d'Internet non indexée par les moteurs de recherche, et notamment les pages Web accessibles uniquement après authentification sur un site. Le Dark Web lui-même est une partie du Deep Web. C'est sur le Web profond que foisonne le côté obscur d'Internet.

Par ailleurs, il existe sur le Dark Web des sites dont les intentions ne sont pas malveillantes. Et plusieurs sites légitimes sont également présents sur le Dark Web.

Du côté le plus sombre du Dark Web, on observe bon nombre de places de marché, forums et communautés Internet Relay Chat (IRC) se concentrant sur des biens illicites : drogue, armes, identités volées et, bien sûr, produits et services cybercriminels. La plupart de ces places de marché arborent des notations, des descriptifs, des revues, voire, une assistance technique et un support client. Ils disposent de vendeurs, d'acheteurs et d'administrateurs (tout comme eBay). S'agissant de l'acquisition en ligne de biens et services illégaux, ces places de marché ont amélioré l'expérience client en facilitant l'accès aux "escrow services". Ils imposent souvent des frais et une procédure de contrôle pour se faire une place en tant que vendeur ou sur un forum.

Le rapport d'Europol, Internet Organised Crime Threat Assessment, sur la cybercriminalité en 2019, suggère que le Dark Web se fragmente : davantage de magasins sont gérés par des vendeurs seuls et des marchés fragmentés de plus petite taille répondant parfois à des besoins dans des langues spécifiques. Ces marchés et forums tâchent de cacher l'identité de leurs utilisateurs ; ils recourent à l'anonymat pour protéger leurs clients des forces de l'ordre aussi bien que pendant leurs transactions. Ils impliquent généralement des cryptomonnaies et des "escrow services". Ce type de service assure que les transactions sont menées à bien entre deux parties. Ils sont particulièrement utiles sur le Dark Web, où les parties en question peuvent ne pas être dignes de confiance.

© Orange Cyberdefense


Criminel hors ligne
Informations volées
infrastructure
opère
monétise
vend
achète
vend des marchandises illégales
achète des services
offre ses services
emploie
Propose un hébergement sécurisé
achète
hacker
vend
achète
exploits
utilise
trouve/vend
hacker
améliore
vend
achète
vend
achète
vend
achète
paye pour
utilise
spam & phishing
distribue
malware
vend
marketplace
loue
opère
Malware (publicités)
fournit des bots d'infection
attaque/extorque de l'argent de
paye / perd ses données
offre
vole des identifiants
distribue des infections
botnets
bloque
(DDoS)
victime

Le malvertising

Le malvertising s'entend par la présence de publicités malveillantes sur des sites légitimes ou piratés, par le biais de réseaux publicitaires tiers. Pour simplifier l'industrie de la publicité en ligne, on trouve des éditeurs (sites vendant des espaces publicitaires), des annonceurs (personnes souhaitant promouvoir leurs produits, etc.), des bourses d'annonces (plate-formes en ligne sur lesquelles des éditeurs peuvent vendre des espaces publicitaires) et des revendeurs de réseaux publicitaires (achat d'espace publicitaire, mise en relation des éditeurs et annonceurs). Les éditeurs légitimes peuvent proposer de l'espace publicitaire sur leurs sites, qu'un réseau peut acheter, puis vendre à un annonceur malveillant.

Des services de malvertising peuvent agir comme moyen de propagation des campagnes de malwares. Côté utilisateur, la publicité malveillante paraît légitime, mais l'infrastructure qui la fournit en arrière-plan est sophistiquée. Les annonceurs malveillants injectent du code dans des publicités que des réseaux légitimes poussent vers les sites des éditeurs. Ces annonces peuvent rediriger les utilisateurs sur des pages présentant des kits d'exploit, par exemple.

Les exploits

Par exploit, on entend la découverte, le développement et la vente d'exploits. Une vulnérabilité consiste en une faiblesse dans un logiciel et l'exploit est utilisé au cours d'une attaque mettant à profit cette vulnérabilité pour atteindre un certain but. Il existe plusieurs types d'exploits : des simples lignes de code aux scripts complexes. Diverses vulnérabilités et exploits peuvent aboutir à différentes résultantes : faire planter un serveur, faire tourner du code sur un serveur, contrôler totalement un serveur, etc.

Les exploits dépendent des vulnérabilités que les chercheurs découvrent et pour lesquelles ils produisent des exploits. Certains chercheurs responsables choisissent d'informer les éditeurs s'ils découvrent une vulnérabilité, d'autres la gardent secrète et vendent l'exploit correspondant. Aussi, lorsqu'un éditeur remédie à une vulnérabilité dans un de ses produits, des chercheurs peuvent créer des exploits une fois la vulnérabilité rendue publique.

Ces exploits ne sont généralement pas vendus directement par les chercheurs : des prestataires facilitent les négociations auprès de clients potentiels. Les vulnérabilités non publiques, les plus onéreuses, sont appelées « zero-day ». Les profils des clients intéressés par ces exploits 0-day varient : société de sécurité « White Hat », gangs cybercriminels, hackers à la solde d'États.

Les malwares

Par malware on entend la création, l'achat et la vente de logiciels nuisibles ainsi que des postes infectés. Les groupes cybercriminels conçoivent, développent et publient eux-mêmes les malwares. Ils proposent parfois des services à valeur ajoutée : assistance après-vente et maintenance évolutive pour répondre aux besoins changeants de leurs clients. On parle de Malwares-as-a-Service. Ce principe place la barre très bas pour les criminels non techniques souhaitant lancer leurs propres campagnes de malwares.

Les groupes cybercriminels se spécialisant dans les malwares comptent des auteurs chargés du développement de logiciels malveillants. Ils s'assurent qu'ils ne seront pas détectés par les solutions anti-malwares et que leurs performances sont satisfaisantes. Ces groupes peuvent mener des campagnes de malware, ou vendre à d'autres des accès pour qu'ils en utilisent.

Les campagnes par malware impliquent diverses techniques visant à infecter des postes. Elles nécessitent plus que l'achat ou le développement de malwares, à savoir la distribution, la mise en place d'infrastructures de serveurs C&C, l'identification de points d'infection, le blanchiment d'argent, etc. Ces différentes activités peuvent, ou non, être externalisées par le biais d'autres groupes sur le Dark Web. L'aspect distribution est communément externalisé, par exemple, via des services de Pay Per Install (PPI), de spams (courriels indésirables), de phishing (hameçonnage), de drive-by-download (téléchargement furtif) et de malvertising.

L'infrastructure

Quand des criminels cherchent à héberger un site ou contenu malveillant à des fins de phishing, d'escroquerie, pour alimenter des sites de carding, ou à louer un serveur C&C, ils peuvent privilégier un service d'hébergement qui passe outre les plaintes des visiteurs et autres hébergeurs. Ces sites malveillants comptent de faux sites de vente en ligne, des torrents et sites de streaming, des outils de bruteforce, des sites publicitaires, etc.

Ce qui amène à l'infrastructure… le bulletproof hosting (littéralement, hébergement pare-balles) est une industrie criminelle lucrative, bien que souvent négligée. En général, les clients ont le choix entre trois types d'hébergement :

1) un serveur dédié, où le fournisseur sait qu'il héberge du contenu malveillant et s'en accommode ;
2) des serveurs dédiés, ayant été compromis, sont loués, sans que le propriétaire légitime soit au courant ;
3) des serveurs cloud loués à des fins malveillantes.

Par exemple, un article de SpamHaus indique qu'une opération récente louait des serveurs virtuels privés (VPS) légitimes au moyen de fausses identités.

© Orange Cyberdefense

Les spams et le phishing

Les spams et cas de phishing sous-entendent la création, la vente et l'envoi d'e-mails malveillants à des fins publicitaires, de vols d'informations sensibles ou de propagation de malwares. Les clients peuvent acheter des campagnes de spams. Ils rémunèrent des groupes spécialisés pour chaque e-mail envoyé. Une fois achetés, les e-mails sont souvent envoyés par un botnet, loué ou géré par un « spammeur ». Emotet illustre ce type de malwares, initialement diffusé via des e-mails malveillants.

Les campagnes de spam ne sont pas toujours utilisées pour propager des malwares, elles promeuvent souvent des sites et des produits. Si un destinataire fait un achat sur le site d'un de leurs clients, les gestionnaires de ces campagnes perçoivent une commission sur la vente.

Les groupes cybercriminels se spécialisant dans le phishing proposent parfois de louer des services visant à simplifier les attaques par phishing (Phishing-as-a-Service). Des abonnements mensuels s'appliquent. Les débutants achètent donc des modèles d'e-mails, des infrastructures et des manuels d'utilisation sur des forums et places de marché, sur le Dark Web. Le seuil d'accessibilité pour les criminels s'en trouve, là aussi, abaissé. De la même manière, les kits de phishing comportent tous les outils dont les criminels ont besoin pour lancer une attaque : pages Web de connexion usurpées, modèles d'e-mails de phishing, etc.

Les informations volées

Le vol d'informations s'entend par le vol et la vente de données. Ces informations peuvent provenir de l'une ou l'autre des sphères ici évoquées (phishing, malware ou piratage). Les informations susceptibles d'être vendues sont des données sensibles, comme des identifiants VPN, des données de connexion à des sites d'e-commerce ou des médias sociaux, à des domaines Windows, des identifiants bancaires.
Ces informations sont monétisées de diverses manières. Les identifiants de connexion sont vendus individuellement ou proposés par lots. Ils incluent parfois des hashs de mots de passe ou des mots de passe en clair. Les données bancaires et informations issues de cartes de paiement peuvent être vendues par lots sur des forums de carding, ou les comptes peuvent être vidés par divers moyens.

Les autres informations susceptibles d'être vendues vont du numéro de sécurité sociale (SSN) ou numéro de carte d'identité, à des ensembles de données médicales. Ceux qui dérobent des identités achètent, par exemple des informations médicales, car elles contiennent des dates et lieux de naissance, des numéros de sécurité sociale, des adresses, e-mails, voire aussi des informations relatives aux mutuelles souscrites.

Les pirates

La composante piratage englobe les produits et services vendus par des pirates sur le Dark Web. Les hackers disponibles à l'« embauche » promeuvent de multiples services : vol d'informations sensibles, piratage de mobile, piratage de compte sur les réseaux sociaux, cours de piratage, modifications de résultats scolaires, effacement de contenu sur Internet, attaques par DDoS, embauche à plein temps, etc.

De plus en plus, les pirates font la promotion d'accès à des réseaux d'entreprise sous la forme d'identifiants VPN. Ces accès peuvent s'avérer utiles à des groupes se spécialisant dans les ransomwares, en quête de moyens simples de s'introduire dans ces réseaux. En septembre 2020, des accès réseau à des organisations se sont vendus 500 000 dollars sur certains forums de piratage. Sur ce marché, considéré comme « initial », se vendent et s'achètent identifiants VPN, RDP ou accès via des botnets.

Les botnets

Les botnets impliquent la création et la monétisation de réseaux d'ordinateurs, smartphones ou autres objets connectés infectés, capables de recevoir et d'exécuter des ordres (donnés par l'opérateur du botnet). La création d'un botnet demande que soit développé ou acheté un malware dédié, et de trouver ou acheter un service pour distribuer ce malware. Les opérateurs de botnets sont considérés comme les meilleurs clients des auteurs de malwares.

Ils peuvent être monétisés de différentes manières : vendus à profit, ou loués pour divers services. Les services de location incluent notamment les campagnes de spams et de phishing, le vol de données sensibles, des serveurs proxy, l'installation d'autres malwares et les attaques par DDoS.

Le blanchiment

Une fois que les malwares, l'extorsion ou autres arnaques ont généré un revenu, ou si les escrocs s'attendent à un profit, le blanchiment est une étape clé pour garder une longueur d'avance face aux autorités.

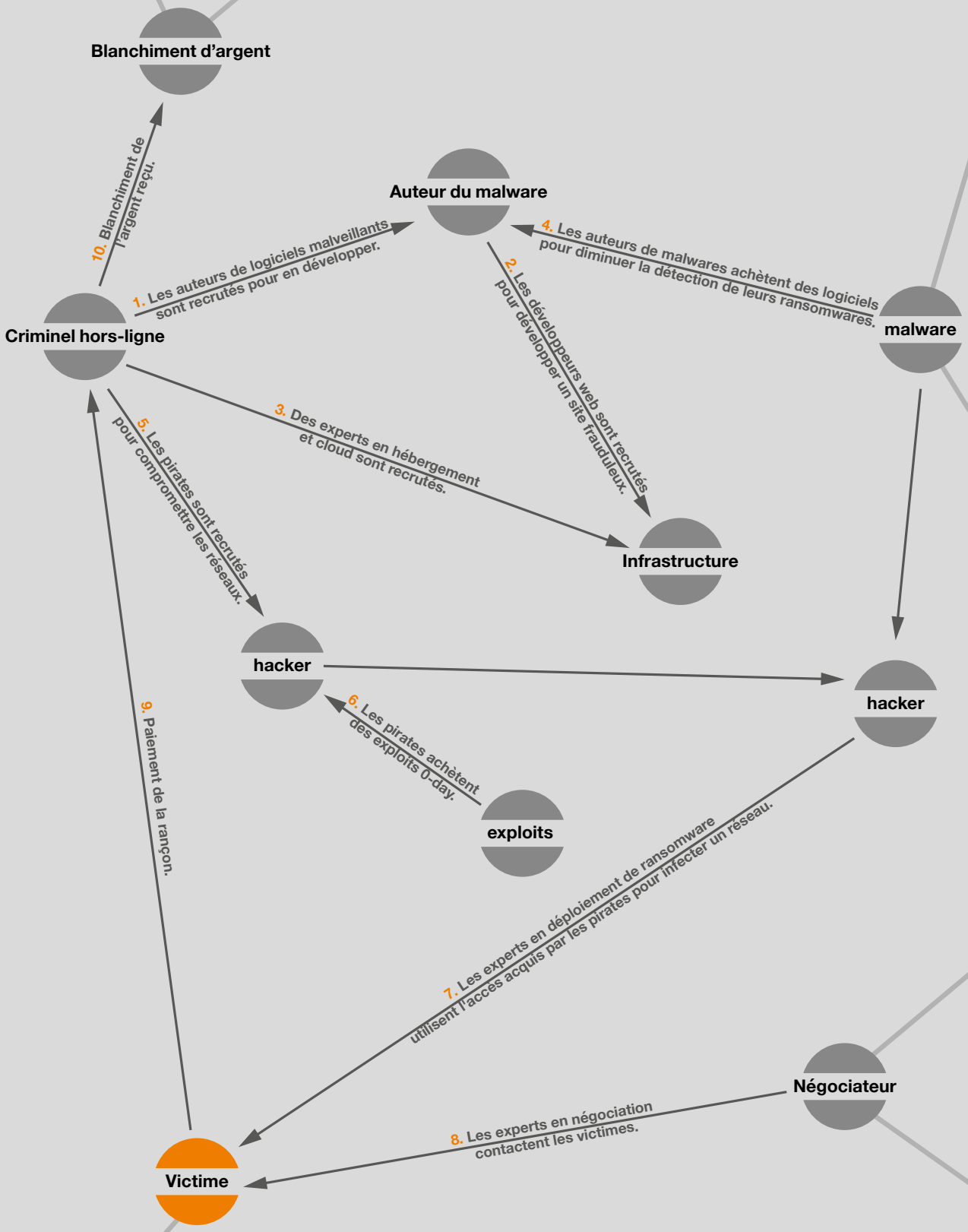
Des groupes cybercriminels se spécialisent dans le blanchiment d'argent. Plusieurs des membres du groupe qqaazz, par exemple, ont récemment été accusés de fournir des services de blanchiment à des opérateurs de malwares connus (dont Dridex, Trickbot et GozNym). Leurs opérations reposaient sur des sociétés-écrans dont le rôle était d'ouvrir des comptes bancaires avec de faux documents, de recevoir l'argent et de le retirer des comptes.

Exemple : Une histoire de ransomwares

1. Les auteurs de ransomwares sont recrutés pour en développer.
2. Les développeurs web sont recrutés pour développer un site frauduleux.
3. Des experts en hébergement sécurisé et en stockage de données dans le cloud sont recrutés.
4. Les auteurs de logiciels malveillants achètent ou fournissent des logiciels pour réduire la détection de leurs malwares.
5. Des hackers sont recrutés pour compromettre les réseaux.
6. Les hackers achètent des exploits "zero-day".
7. Les experts spécialisés en déploiement de ransomwares utilisent l'accès volé par les pirates pour infecter un réseau.
8. Des experts en négociation contactent les victimes.
9. La victime paye la rançon.
10. L'argent de la rançon est blanchi.

© Orange Cyberdefense

Les réseaux criminels : Une histoire de ransomwares



Conclusion

Dans « cybercriminalité », la composante « criminelle » domine sur l'aspect « cyber ». Au fil des années, nous avons observé des changements dignes d'intérêt bien que sans conséquences dans les outils, technologies et techniques des criminels pour mener à bien leurs attaques dans le cyberespace. Dans le même laps de temps, nous avons constaté des changements conséquents au sein de l'écosystème métier de la cybercriminalité. Ces changements ont, quant à eux, impacté la façon dont les criminels gagnent de l'argent et façonné le paysage des menaces de manière significative.

Un exemple récent de transition : le passage des cybercriminels usant de ransomwares à ce que l'on peut appeler la « double extorsion » – pratique consistant à voler (et chiffrer) les données d'une victime pour les lui revendre contre rançon, tout en la menaçant de diffuser des informations sensibles en cas de refus de paiement. Cette pratique a vu émerger des tactiques de « big game hunting » – des attaques sophistiquées, de longue haleine contre des sociétés d'envergure visant à leur faire payer des rançons de plusieurs millions de dollars. Ces jackpots ne sont pas dilapidés sitôt encaissés : ils sont investis dans un cycle d'amélioration et d'innovation donnant lieu à une criminalité encore plus efficace.

Aujourd'hui, le recours aux ransomwares est devenu un business. Et, comme tout business, il évolue au sein d'un écosystème, qui implique des acteurs aux rôles spécifiques, allant de l'exécution du crime, à l'extraction ou la répartition des gains illégaux. Certains acteurs clés agissent sur le fil du rasoir, aux limites de la légalité, et se mettent (plus ou moins) directement en danger. D'autres opèrent en arrière-plan, parfois, même, sans le savoir. Ils fournissent des technologies, des services et l'assistance nécessaires pour la conduite d'actes criminels, afin que les attaquants puissent s'échapper sans être détectés, ou pour déplacer et blanchir des fonds obtenus.

Spams pharmaceutiques, ransomwares, menaces de DDoS contre extorsion, carding et autres formes de cybercriminalité sont des défis métier, et non technologiques.

Bien sûr, comprendre et gérer les vulnérabilités humaines, organisationnelles et technologiques exploitées est une composante importante de la lutte contre la cybercriminalité. Mais, il est tout aussi important de disséquer les modèles économiques qui sous-tendent chaque forme de criminalité, comprendre ce qui les fait fonctionner, leurs interactions, et tenter de déstabiliser cette industrie en son sein.

Dans cette section, nous faisons référence à l'une de nos initiatives visant à cartographier les composantes clés de l'écosystème cybercriminel pour mieux comprendre les liens et flux entre ses acteurs. Au cœur de cette initiative : un site interactif sur l'écosystème des réseaux cybercriminels doit prochainement voir le jour et être mis à disposition de nos clients. Comprendre la nature interconnectée de l'écosystème cybercriminel permet d'appréhender la manière dont il fonctionne, comment il peut être ciblé pour entraver son fonctionnement fondamental, au lieu de, simplement, s'adapter à ses stratagèmes techniques changeants.

Par le passé, notre industrie a prouvé que nous pouvons combattre avec succès la cybercriminalité. Cette approche doit devenir la norme plutôt que l'exception. Nous pensons donc que comprendre les réseaux de l'écosystème cybercriminel est la première étape, cruciale, de cette approche.

© Orange Cyberdefense

© Orange Cyberdefense

Robinson Delaugerre
CSIRT Investigations Manager
Orange Cyberdefense

Les récits du CSIRT et du pentest

Patrouiller avec les cybersauveteurs

Les attaquants progressent rarement en ligne droite, mais sont, malgré tout, assez directs. Ils lancent leurs scans à la recherche de possibles vulnérabilités, typiquement, des faiblesses pour lesquelles ils disposent d'exploits. Si cette voie ne peut être empruntée, ils en cherchent une autre. Le principe se répète jusqu'à l'ennui, jusqu'à manquer de temps ou jusqu'au succès.

La vie des défenseurs, quant à elle, s'avère bien plus complexe. Tiraillés entre de multiples vulnérabilités, correctifs et vecteurs d'attaques, entre évaluer les dernières technologies et éduquer des utilisateurs prompts à réagir : il n'est pas simple de rester à la pointe en matière de sécurité. Généralement, tous font du bon travail, mais il n'existe pas de sécurité absolue. Par moment, même les politiques de prévention les mieux préparées peuvent échouer : une zero-day, de la malchance, une vulnérabilité matérielle non patchée, ou ce boîtier VPN dont vous aviez oublié l'existence et que vous n'avez pas corrigé… Les attaquants trouvent des portes d'entrée.

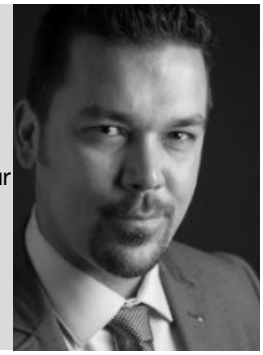
Et… quand les problèmes commencent, qui faut-il appeler ?

Découvrez les récits du CSIRT, mais aussi de nos équipes pentest, qui permettent d'agir en amont et d'éviter bien des déconvenues !

Un doux parfum de ransomware

Un client a fait appel à Orange Cyberdefense car l'une de ses filiales vietnamiennes subissait une attaque par ransomware. En coopération avec Orange Business Services, qui a dépêché un ingénieur sur site, les experts du CSIRT (Computer Security Incident Response Team) ont pu intervenir quelques heures à peine après l'identification de l'incident.

Robinson Delaugerre, CSIRT Investigations Manager, **Orange Cyberdefense**



1 Démarrage en fanfare

L'attaquant a eu accès au serveur RDP (Remote Desktop Protocol). Là, il a largué sa caisse à outils : il scanne le réseau, extrait les mots de passe du navigateur, explore la mémoire des processus et désactive les antivirus sur le serveur.

2 Le « roi du Texas »

Dix minutes après l'intrusion, il a déjà procédé à la reconnaissance du réseau et obtenu les identifiants de l'administrateur de domaine. Il se connecte au contrôleur de domaine et extrait les identifiants du serveur. Il obtient alors les identifiants de l'ensemble des utilisateurs, ou presque, en clair.

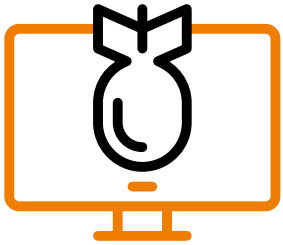
3 Vu d'en haut

Connecté au serveur de domaine, l'attaquant monte plusieurs partages, découverts sur le contrôleur de domaine. Il témoigne un intérêt particulier pour les sauvegardes. Il est déjà là depuis une heure et demie.

4 Brouiller les pistes

Une fois la majorité du réseau atteinte et la cible principale sous contrôle, tous les logs Windows sur toutes les machines compromises sont effacés pour tenter de rendre plus ardue l'enquête scientifique du vecteur d'attaque. Cependant, comme vous pouvez le constater, les journaux ne sont pas l'unique source d'information forensics.

© Orange Cyberdefense



5 Déploiement d'un ransomware

Quatre heures après sa première connexion au serveur RDP, l'attaquant déploie une variante de Phobos sur l'ensemble des machines.

6 Restaurer proprement les sauvegardes

En étudiant l'historique de l'attaque, le ransomware utilisé et son mode opératoire, il a été possible de restaurer proprement des sauvegardes des systèmes infectés, puis de les remettre en ligne. Pour les besoins de l'enquête criminelle et afin d'éviter des attaques ultérieures, un rapport complet et détaillé a été fourni au client.

Enseignements :

Ce qui se tapit dans l'ombre

L'histoire commença avec un attaquant surgissant sur un serveur RDP, sans qu'on vous dise comment… Comme les logs ont été effacés, nous ne saurons jamais vraiment comment l'attaquant s'est emparé du compte. Néanmoins, le fait que deux heures après la suppression, plus de huit-mille tentatives de connexion étaient enregistrées depuis le monde entier, il est cohérent de penser à une attaque par force brute.

- Comme énoncé, un réseau non segmenté n'est guère plus solide que son terminal le plus faible. La défense et la détection appliquées aux terminaux sont centrales pour identifier les attaques au plus tôt et minimiser les dégâts.
- La segmentation réseau peut aider à contenir une attaque en la limitant à une partie séparée du réseau. Les équipements importants, comme les serveurs RDP, doivent de surcroit être protégés au sein du segment.
- Les attaques par force brute sont relativement faciles à détecter et gérer. Plusieurs milliers de tentatives de connexion ont probablement échoué avant qu'une réussisse. En amont, un mécanisme de détection aurait pu déclencher une alerte et des contre-mesures automatisées, si des mécanismes de protection ou un SOC (Security Operation Center) avaient été mis en place sur site ou en externe.
- Enfin, dissimuler la procédure d'attaque et l'activité en supprimant les logs est inefficace si les journaux d'évènements sont collectés au sein d'un SIEM. Non seulement, les logs sont sauvegardés efficacement, mais ils permettent aussi des enquêtes détaillées pour identifier les vecteurs d'attaque et, préventivement, supprimer les vulnérabilités exploitées.

« Bonjour, je suis AD\steve-admin, pouvez-vous me laisser accéder à VLAN2 ? »

En tant que pentesteur, nous sommes confrontés à divers environnements, que certains comparent à des flocons de neige. De loin, ils semblent tous similaires, mais intrinsèquement, à leur manière, ils sont tous uniques. Parfois, nous tombons sur seulement l'un de ces flocons, si particulier qu'il nous invite à l'examiner à la loupe, l'étudier, voir ce qu'il se passe si on y touche. Voici l'histoire d'un de ces flocons.

Justin Perdok, Security Specialist Operations, **Orange Cyberdefense**

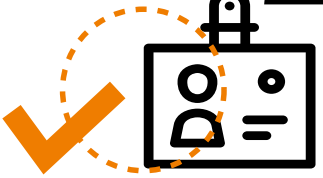
1 Attends, qu'est-ce qu'il se passe là ?

Lors d'audits internes, nous exécutons parfois des services, comme des serveurs de fichiers pour déplacer des éléments sur le réseau. Après avoir fait tourner un de ces services, nous avons constaté que quelqu'un cherchait à s'y authentifier. Il s'agissait d'un compte administrateur du domaine, qui s'authentifiait de manière répétée. Nous avons ainsi pu récupérer le hash de son mot de passe, le casser ou, éventuellement, relayer ces identifiants et compromettre d'autres systèmes sur le réseau. Au lieu de nous en tenir à cela, nous avons souhaité savoir « qui » se connectait et pourquoi.

3 Et… si ?

Comme le réseau fait confiance aux données issues d'un poste pour appliquer les règles du pare-feu, que se passe-t-il si nous disons au système que nous sommes un utilisateur doté de droits d'administration ? Pouvons-nous faire appliquer d'autres règles, qui nous permettraient d'accéder à d'autres systèmes au sein d'autres réseaux ? Est-ce que nous pourrions alors compromettre plus de systèmes métier critiques auxquels nous n'aurions pas accès pour l'instant ? Des outils publics nous permettent-ils d'y parvenir ?

Spoiler : les réponses sont oui, oui, oui et « en quelque sorte ».



2 Qui vient de se connecter et pourquoi ?

Après avoir inspecté le trafic réseau généré par ce mystérieux admin, il est apparu qu'il tentait de collecter des informations sur les utilisateurs connectés. Il s'est avéré que ce réseau disposait d'un système permettant au pare-feu d'identifier les utilisateurs connectés à un poste. Ces informations servaient ensuite à appliquer au niveau du pare-feu des règles spécifiques à l'IP du poste de travail. Ce comportement nous a suffisamment interpellés pour que nous nous demandions « Et… si ? ».

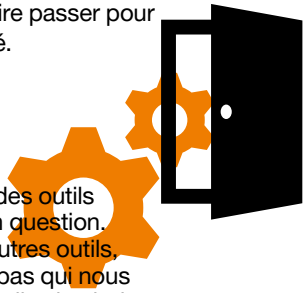
© Orange Cyberdefense

5 Collecter les informations

Précédemment, nous avions analysé des informations issues du réseau interne. Nous opérions depuis un segment réseau que, pour l'instant, nous nommerons VLAN1. Nous avons trouvé un système dans un autre réseau virtuel local segmenté, que nous appellerons VLAN2. À ce stade, nous ne pouvions pas accéder à ce système dans VLAN2, supposément, du fait des règles de pare-feu. Nous avons aussi remarqué qu'un utilisateur, disons « steve-admin », avait accès à ce système. Cet utilisateur devenait alors une cible idéale pour se faire passer pour un utilisateur connecté.

6 Se faire passer pour l'administrateur

Nous avons lancé notre outil, renseigné « steve-admin » et attendu que le système interroge notre liste d'utilisateurs connectés – en nous demandant toujours si cela allait fonctionner. Après que le système nous ait interrogés et vu que « steve-admin » était l'utilisateur connecté, il nous a octroyé ses règles de pare-feu. Ce procédé nous a donné accès au système dans VLAN2 d'un point de vue réseau. Avec des identifiants collectés précédemment, nous nous sommes connectés et avons compromis le système cible.



4 Construire l'outil

Pour réaliser ces tests, il nous fallait des outils qui reproduiraient la fonctionnalité en question. Après avoir étudié le protocole et d'autres outils, nous avons conclu qu'il n'en existait pas qui nous permettraient d'atteindre ce but, mais il existait des briques utilisables. Nous avons donc enrichi un outil existant avec ces briques et avons pu répondre à ces requêtes avec des informations arbitraires que nous contrôlions totalement. Nous avons donc pu nous faire passer pour n'importe quel utilisateur comme s'il était connecté sur notre système et, potentiellement, obtenir ses règles de pare-feu.

Enseignements

- Lire et appliquer les bonnes pratiques émises par l'éditeur : la mise en œuvre de la fonctionnalité que nous avons exploitée est indiquée comme non sûre par l'éditeur, mais elle est toujours supportée et peut être configurée.
- Appliquer le principe de moindre privilège à vos environnements d'Active Directory : les comptes de services ne doivent pas se voir remettre les clefs du royaume. Assurez-vous qu'ils ne sont autorisés à accéder qu'aux ressources dont ils ont réellement besoin dans l'intérêt de leurs fonctions. L'éditeur a décrit ce cas dans un guide de bonnes pratiques.
- Savoir ce que l'on implémente : le fait qu'un éditeur de logiciels supporte certaines fonctionnalités ne veut pas systématiquement dire qu'elles sont sûres. Il n'est jamais dommageable de vérifier ce qu'elles font, de se demander « si… ».

Alerte rouge

Ce récit récapitule une opération Red Team menée en 2020 pour l'un de nos clients. L'objectif était de simuler une menace externe pour accéder à une application interne spécifique, sans être détecté ou bloqué par les équipes de sécurité interne. Pour atteindre ce but, de multiples vecteurs d'intrusion pouvaient être utilisés.

Elias Issa, Head of Red Team France, **Orange Cyberdefense**

1 Enquête téléphonique

Après avoir mis la main sur le numéro du service presse (souvent exposé), l'équipe a composé des numéros suivant le même format. Les appels passés hors des horaires de travail visaient à lister des boîtes vocales du type « Vous êtes sur la boîte vocale de <prénom nom>, veuillez laisser un message ».

2 Analyse

Quelques noms ont pu être collectés et une enquête a été menée sur chaque personne identifiée pour construire les scénarios les plus adaptés.

3 Ingénierie sociale

Une plate-forme d'appel a été utilisée pour falsifier le numéro de téléphone « appelant ». L'accueil a été contacté en usurpant le numéro d'un employé. L'arrivée de deux « consultants » dans la matinée leur a été indiquée. L'employé ne pouvait pas aller les chercher, prétextant un problème : « Pourriez-vous créer deux badges pour eux ? Ils sont déjà venus, ils connaissent la maison ».

4 Déploiement de la porte dérobée

Une fois dans les locaux et munis de leurs badges, l'exploration des lieux les a menés à une pièce qui semblait parfaite pour dissimuler un implant physique. Une fois l'implant connecté au réseau et caché derrière une imprimante, un accès Wi-Fi était fourni à l'équipe qui attendait dehors dans une voiture. Elle avait alors accès au réseau interne.

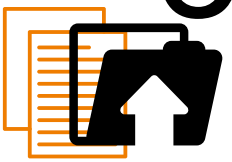
© Orange Cyberdefense

5 Exploitation du périmètre

Un peu plus tard, un compte utilisateur valide leur a permis d'exploiter une mauvaise configuration du contrôleur de domaine et de collecter les mots de passe en clair des comptes admin locaux. Quelques actions après, le compte d'administrateur de domaine était compromis.

7 Compromission totale

La sécurité a été mise à mal, avec succès, par la Red team.



6 Accès aux données

Le but principal était d'avoir accès — en étant authentifié — à un client lourd utilisé par certains employés. Après avoir identifié les personnes qui avaient accès à l'application, des recherches approfondies ont été effectuées sur leurs ordinateurs. Ce procédé a permis d'accéder directement au client lourd pendant que les employés déjeunaient.

Enseignements

- Sensibiliser les employés aux risques liés à l'ingénierie sociale.
- Appliquer des procédures robustes et strictes de limitation des accès aux locaux.
- Imposer des contrôles d'accès au réseau (Network Access Control – NAC).
- Segmenter le réseau et appliquer des filtres.
- Durcir la configuration des serveurs, des postes et de l'Active Directory.
- Ne jamais stocker des mots de passe en clair !

© Orange Cyberdefense

Business Unit Conseil & Audit,
France et Maroc
Orange Cyberdefense

Tech insight :

Quel service de visioconférence choisir ?

L'épidémie de COVID-19 a fait du télétravail l'une des seules alternatives à la présence physique dans les locaux pour de nombreuses entreprises. L'appel vidéo est ainsi devenu incontournable pour collaborer efficacement lorsque l'on travaille depuis chez soi. Teams, Jitsi, Zoom et d'autres outils collaboratifs se sont inscrits dans notre quotidien.

Réunions de travail à plusieurs, visioconférences avec des partenaires ou des clients, webinars, formations ou encore simples conversations entre collègues, ces outils proposent de nombreuses fonctionnalités. C'est usages ne se font pas sans risques.

Si l'application Zoom a été sous le feu des critiques, que valent ses concurrents ? Nous proposons aujourd'hui d'analyser les différentes solutions qui peuvent être utilisées pour la visioconférence. Les solutions grand public comme Skype, Discord ou Ventrilo n'entrent pas dans le panorama de l'analyse.

Visioconférence : entre sécurité et fonctionnalités

Le choix d'une solution de visioconférence est toujours le résultat d'un compromis entre les usages (fonctionnalités telles que audio/visio, partage de documents, tableau blanc, questionnaire…) incluant les différents terminaux utilisés (smartphones, ordinateurs, connexion depuis une salle de réunion, via un téléphone…), les contraintes techniques telles que la bande passante disponible (connexion haut débit ou plus limitée) d'un côté et la confidentialité des données et la protection de la vie privée de l'autre (chiffrement, contrôle d'accès, conformité…).

Une solution efficace est un savant mélange de tout ceci : il est déconseillé d'utiliser une solution extrêmement sécurisée si les collaborateurs éloignés de l'IT n'y trouvent pas leur compte. De même, il est déconseillé de déployer une solution très fonctionnelle mais ne présentant aucune garantie de sécurité.

Pour vous aider objectivement à choisir la solution qui vous convient le mieux, nous commençons par vous présenter un « modèle de sécurité cible » qui, selon nous, devrait résumer les besoins de sécurité pour un utilisateur de l'entreprise.

En gardant ce modèle à l'esprit, nous avons ensuite entrepris d'installer, de configurer et de tester chacune des solutions dont nous rendons compte ci-après. Toutefois, lorsque cela n'était pas possible, nous avons également intégré :

- Les informations publiées par les éditeurs ou d'autres sources tierces
- Les retours d'utilisateurs qui ont déjà utilisé les solutions

Modèle de sécurité cible

Nous avons basé notre analyse des solutions sur les exigences de sécurité présentées ci-dessous :

Authentification

Un système robuste doit permettre d'identifier, de confirmer les utilisateurs légitimes d'une plateforme et d'empêcher l'accès aux personnes non autorisées. Pour les entreprises, cela repose notamment sur l'annuaire utilisateurs et l'authentification unique (Single Sign On, SSO). Nous portons également un intérêt aux systèmes qui prennent en charge l'authentification multi-facteurs (MFA).

Chiffrement

La confidentialité de la donnée est essentielle (textes, vidéo, etc.) lorsqu'elle traverse notamment un réseau local.
Il y a deux modèles à considérer :

Les données « en transit » : ce sont des informations qui se déplacent d'un endroit à un autre sur un réseau, par exemple entre le poste de l'utilisateur/son navigateur Web et le service de visio-conférence.

Le chiffrement de bout en bout : (en anglais, End-to-End Encryption ou E2EE) c'est un système de communication où seules les personnes qui communiquent ensemble peuvent lire les messages échangés. Il est conçu pour résister à toute tentative de surveillance ou de falsification, puisque personne n'est en mesure de déchiffrer les données communiquées ou stockées. Autre atout : les entreprises qui offrent un service de chiffrement de bout en bout sont dans l'incapacité de remettre une version déchiffrée des messages de leurs clients aux autorités.

Règlementation et juridiction

Pour le fournisseur, la localisation géopolitique et la juridiction légale jouent un rôle important dans la détermination du risque.

Le fournisseur d'un service de conférence est une personne morale qui relève de la juridiction (et donc de la règlementation) d'un État souverain. Tenant compte de cet aspect, cela pourrait avoir une incidence sur le type de normes de sécurité que le fournisseur met en œuvre. De plus, cela peut avoir des répercussions importantes sur la sécurité des données qui pourraient être stockées ou traitées par le fournisseur, compte tenu des possibilités légales pour un gouvernement d'accéder à ces données (Patriot Act par exemple).

Caractéristiques et gestion de la sécurité

La complexité est « l'ennemi » de la sécurité et nous nous attendons donc à ce qu'un système critique fournisse aux administrateurs des outils clairs et complets permettant de comprendre, de mettre en œuvre et de contrôler les caractéristiques de sécurité.

Vulnérabilité et historique d'exploitation

Les dispositifs de sécurité et les contrôles qu'une plate-forme prétend mettre en place ne sont utiles que si ces contrôles ne peuvent pas être détournés par des pirates exploitant les vulnérabilités de la technologie. Nous devons donc tenir compte des antécédents du fournisseur en matière de sécurité technique, de son niveau de transparence et de sa capacité à réagir rapidement et efficacement lorsque des bugs/erreurs de sécurité sont signalés. Notre analyse portera davantage sur les aspects sécurité et fonctionnalités de l'outil.

Zoom

Zoom Video Communications est une entreprise basée à San Jose, en Californie. Elle connaît un grand succès depuis sa création en 2011, succès d'autant plus important depuis

© Orange Cyberdefense

l'épidémie de COVID-19. Le but du service proposé par Zoom est d'interagir avec une solution cloud pour assurer une meilleure qualité. Zoom est utilisé comme une solution audio et vidéo collaborative pour les utilisateurs (sous licence) de salles de réunion permettant de travailler en interne comme avec des partenaires en externe, en proposant un mécanisme interactif innovant.

L'application permet également le partage d'écran afin de collaborer via le partage de notes, visibles par tous les participants. Il est possible d'envoyer des messages sur tous les appareils d'un seul clic. Zoom permet également d'enregistrer les conférences, en local ou sur le cloud.

Zoom : analyse technique

Zoom s'intègre avec les clients de messagerie et fonctionne également sur mobile (iOS et Android) ou sur écrans tactiles afin de permettre le plus d'intégrations possibles. Elle est raccordable à de nombreux points de terminaison audio et vidéo. L'installation d'un client lourd (ndlr : d'un logiciel exécutable sur l'ordinateur) ou d'une application mobile est nécessaire, sous Windows, Android et iOS, afin de pouvoir créer et gérer une réunion. La connexion ou la planification d'une réunion peut également se faire via un navigateur.

Zoom, à la différence de nombreuses solutions présentées ici, n'utilise pas le standard WebRTC mais fait appel à une technologie propriétaire. A titre informatif, le WebRTC est une interface permettant la communication en temps réel sur le web. Ce standard permet aux navigateurs de supporter de la voix, ou du partage de données directement depuis le navigateur, en s'affranchissant donc de logiciels spécifiques ou d'extensions à installer dans ces navigateurs.

En mai 2020, Zoom 5.0 a annoncé des mesures de sécurité améliorées qui comprennent un chiffrement plus robuste, la protection des réunions avec par défaut un mot de passe ainsi qu'une nouvelle icône pour un accès facile aux paramètres de sécurité. Le service utilise désormais la norme de chiffrement AES 256 bits GCM. En octobre, Zoom a annoncé tester la mise en œuvre du chiffrement de bout en bout avec les clients lourds.

Avantages

- Un outil très fonctionnel et facile à prendre en main, qui facilite la collaboration en entreprise et avec les partenaires.
- Un outil disponible sur une vaste majorité de plateformes, accessible via un navigateur et qui, de par son fonctionnement SaaS, ne demande pas de configuration spécifique du système d'information.
- Une solution qui s'interconnecte avec de nombreuses autres.
- La prise en compte de l'accessibilité pour tous les participants : l'application permet par exemple, via des API Rest, d'implémenter des sous-titrages.
- Effort important depuis mai sur la sécurité avec la correction des failles remontées, l'apport récent du chiffrement de bout en bout des communications.

Inconvénients

- La solution est complexe à administrer, même sur des postes de travail correctement gérés.
- Présence de fonctionnalités telles que le transfert de fichiers ou le contrôle d'écran à distance qui pourraient être interdites dans le cadre de la politique de sécurité d'une entreprise
- Solution exclusivement en SaaS, sur les serveurs de Zoom.

Zoom : quelle sécurité ?

Depuis le début de la pandémie de COVID-19 et la mise en place de mesures de confinement à l'échelle planétaire, Zoom a vu son usage croître de façon exponentielle (+535% d'usage, rien qu'aux Etats Unis). Sous le feu des projecteurs, de nombreuses failles et vulnérabilités sont venues mettre à mal la sécurité de Zoom et la confiance portée à l'entreprise. Voici notre analyse :

- L'entreprise a, pendant un temps, partagé certaines de ses données avec Facebook, sans en avertir ses utilisateurs. Ce transfert de données a été arrêté, suite aux découvertes.
- Zoom déclarait il y a peu que ses communications étaient chiffrées de bout-en-bout (parfois écrit end-to-end ou E2EE), ce qui s'est avéré ne pas être le cas. Cette fonctionnalité n'a été ajoutée que fin octobre.
- Zoom permet de générer automatiquement des annuaires d'adresses : pour les personnes travaillant dans la même compagnie, Zoom génère un annuaire permettant de se regrouper. Seul hic, Zoom a fait de même avec des adresses mail personnelles, telles que Gmail, exposant des centaines de milliers d'adresses e-mail à d'autres personnes tierces.
- Une précédente version de Zoom installait un serveur web secret sous les appareils Mac des utilisateurs, la désinstallation de l'application ne supprimait pas le serveur.

Tout n'est pas négatif pour autant, pour Zoom : l'entreprise semble avoir compris les enjeux de sécurité de son application et prend les mesures nécessaires pour stopper ses agissements discutables et corriger au plus vite les failles dont elle a connaissance. Nous vous recommandons donc la plus grande précaution avec Zoom et la nécessité de mettre à jour le client dès qu'une mise à jour est disponible.

Tixeo, la référence française

Créée et basée à Montpellier, Tixeo propose un ensemble de solutions de téléconférence sécurisées. L'entreprise

compte de nombreuses références et a fait de la sécurité des communications un enjeu prioritaire. La technologie et le savoir-faire de Tixeo sont certifiés et qualifiés par l'ANSSI : TixeoServer est ainsi certifié CSPN (Certification de sécurité de premier niveau), gage de sécurité des solutions proposées. Tixeo permet d'organiser des visioconférences, de partager son écran ou encore, de donner le contrôle à distance, ce qui peut s'avérer utile pour le travail collaboratif sur des documents.

La solution Tixeo est une solution payante qui propose plusieurs modes de fonctionnement

- en cloud mutualisé, via deux offres (standard et premium, permettant l'interconnexion d'autres systèmes de visioconférence traditionnels),
- en cloud privé, opéré par Tixeo,
- en version serveur – on premise.

L'entreprise propose également une offre de fourniture de matériels (caméras, écrans, …) nécessaires aux visioconférences.

La solution est disponible sur les plateformes les plus utilisées (Android, iOS, Windows, MacOs et Linux). On s'y connecte via un compte et un mot de passe spécifique qui sont gérés en amont.

Tixeo : analyse technique

La solution s'intègre facilement dans un système d'information car elle ne nécessite pas de configuration ou de ports spécifiques à ouvrir, l'ensemble des communications passant par du HTTPS.

L'utilisation des solutions Tixeo requiert l'installation d'une application côté client et côté serveur, dans une configuration on-premise. A la différence de beaucoup d'autres solutions, l'ensemble des communications de Tixeo sont chiffrées de bout-en-bout par l'algorithme AES 256, tout comme les communications entre le client et le serveur par HTTPS. Traditionnellement, les solutions de visioconférence chiffrent uniquement les flux entre le client et le serveur via le protocole SRTP, les échanges sont alors déchiffrés sur le serveur de vidéoconférence qui a donc accès à la communication audio et vidéo.

Avantages

- Solution sécurisée reconnue par l'ANSSI.
- Offre commerciale qui pourra répondre à la grande majorité des besoins.
- Facilité de déploiement, pas de configuration spécifique (règles firewall, ...) à mettre en place.
- Chiffrement end-to-end sur l'ensemble des communications, y compris à plusieurs participants.

Inconvénients

- Il est nécessaire d'installer un client lourd pour bénéficier de la solution.
- Ne conviendra pas nécessairement aux petites organisations ou aux besoins ponctuels en raison de son modèle économique.
- Pas d'accès possible à la conférence via le réseau téléphonique.

Google Meet

Google Meet, connu sous le nom Meet by Google Hangouts jusqu'au 09 avril 2020, est la plateforme de vidéoconférence à destination des entreprises développée par Google et mise en service en mars 2017. La solution est intégrée dans l'écosystème Google Suite (Gmail, Docs, Drive…). Côté fonctionnalités, Meet permet d'organiser des réunions à distance (grâce à des appels audio, vidéo), offre un partage de documents et un système de messagerie instantanée. Le service est accessible en ligne à travers la plupart des navigateurs Internet ou via des applications mobiles disponibles sur Android ou iOS.

L'authentification se fait via un compte Google servant également à accéder aux autres applications G Suite. La licence de G Suite intègre les coûts d'utilisation de ce service. Le niveau de licence détermine le nombre maximum de participants à une visioconférence. Par ailleurs, Meet offre une fonctionnalité permettant de rejoindre une réunion vidéo planifiée via la saisie d'un code unique.

Google Meet : analyse technique

Les flux vidéo et audio en transfert sont chiffrés en AES-128 mais les conversations ne sont pas chiffrées sur les serveurs Google. Ce dernier est donc, techniquement, en mesure de les capter et les observer. La solution est disponible sur les technologies principales du marché : Windows, Mac OS, Chrome, Linux ainsi qu'au format applications sur les plateformes iOS et Android. L'application est disponible uniquement en mode SaaS via la suite G Suite.

Avantages

- L'outil est intégré à la suite Google, l'usage des autres services est facilité.
- L'interface du produit est simple à prendre en main.
- Accès possible depuis n'importe quel terminal et possibilité de rejoindre la réunion par téléphone.

Inconvénients

- Google se situant aux USA et étant soumis aux règlementations du pays, la possibilité d'interception des communications existe. Google a déjà été accusé de récupérer les informations personnelles et préférences des utilisateurs par ses outils pour ensuite pouvoir faire du marketing ciblé.
- L'interfaçage avec d'autres produits comme la suite Microsoft Office n'est pas très fluide et cette solution est clairement destinée en priorité aux utilisateurs des outils Google (Gmail, Chrome, Google Calendar...).

© Orange Cyberdefense

- L'application souffre de certaines limitations sous un autre navigateur que Google Chrome.

Microsoft Teams

Microsoft Teams est une application de communication collaborative propriétaire, fonctionnant uniquement en mode SaaS, officiellement lancée par Microsoft en novembre 2016. Le service s'intègre à la suite Microsoft Office 365 et à Skype for Business (il est d'ailleurs annoncé comme le remplaçant de ce dernier, qui sera abandonné en juillet 2021) et propose des extensions pouvant être intégrées à des produits autres que Microsoft.

Depuis le 13 juillet 2018, Microsoft Teams est disponible en version gratuite, limitée à 300 membres (certaines fonctionnalités d'Office 365 sont absentes). La solution revendique aujourd'hui plus de 44 millions d'utilisateurs actifs, avec une accélération exponentielle depuis le début du recours massif au télétravail dans de nombreux pays. Côté fonctions, la solution permet le travail collaboratif (co-édition et stockage de documents, accès aux e-mails et à un système de messagerie instantanée…), allant bien au-delà des fonctions de visioconférence classique.

Teams : analyse technique

La solution est disponible sur la plupart des technologies Microsoft Windows, MacOS, Android, iOS et GNU/Linux. L'authentification s'appuie sur Office 365 avec notamment Microsoft Azure.

L'authentification multi-facteurs, combinée au chiffrement des données en transit et au repos assure la connexion des équipes et la possibilité de travailler, à distance, dans un espace sécurisé. Teams impose pour toute l'organisation et ses utilisateurs une authentification à double facteur et peut être intégrée à un single-sign-on (SSO) basé sur l'Active Directory (AD). Les fichiers sont stockés dans SharePoint appuyé par le chiffrement SharePoint, les notes sont gérées via OneNote appuyé par le chiffrement OneNote, lui-même hébergé sur un SharePoint.

Avantages

- Solution sécurisée s'appuyant sur les moyens de sécurisation d'Office 365.
- Une solution 100% intégrée à la suite Office, facilitant l'usage et la modification de documents.
- Un chiffrement des données qui transitent et lorsqu'elles sont stockées sur la solution Office 365.
- Une gestion de l'authentification et de l'identification qui se connecte aisément à Azure.
- Solution 100% utilisable via un navigateur, sans nécessité d'installer un client (sauf pour accéder à des fonctionnalités, comme celle du partage de contenus).
- Une version gratuite existe pour les PME (jusqu'à 300 utilisateurs), même si elle propose des fonctions très limitées.

Inconvénients

- Solution extrêmement complète et pouvant être un peu lourde pour des besoins très basiques ou ponctuels.
- Solution en SaaS, reposant sur des technologies tierces : il faut faire confiance à Microsoft, qui dépend de la juridiction des Etats-Unis.
- Les clefs de chiffrement sont, par défaut, à la main de Microsoft, qui peut donc procéder au déchiffrement de vos données.

Skype for Business

Skype for Business (anciennement Microsoft Lync et Office Communicator) est un outil de messagerie instantanée propriétaire, développé par Microsoft en tant que composant de la suite Microsoft Office. Il comprend les fonctionnalités d'appels audio, vidéo, chat et de transfert de fichiers. Skype for Business s'intègre dans la suite Microsoft Office notamment avec Exchange et SharePoint.

Cette solution nécessitait initialement l'installation d'un serveur Skype on-premise chez le client, ainsi que l'installation d'un client sur le poste de travail. Elle est aujourd'hui intégrée à la suite Office 2019 ou 365 et est disponible sur le cloud en mode SaaS, via Teams. La solution est disponible sur les plateformes les plus utilisées (Android, iOS, Windows, MacOs) sauf Linux.

On s'y connecte via un compte AD interne. Skype est interfacé avec Exchange pour pouvoir gérer les aspects de calendrier, les réunions, les indicateurs de présence ou encore le partage de documents.

Skype for Business : analyse technique

Skype for Business Server comprend une authentification serveur à serveur par le protocole OAuth. Grâce à un ensemble de mécanismes de sécurité (usage de Kerberos, TLS, SRTP...), pratiquement toutes les données de Skype Business Server sont protégées une fois sur le réseau.

Par défaut, les communications réseaux dans Skype entreprise Server sont chiffrées entre les clients et le serveur. Les communications ne sont pas chiffrées en end-to end. Il est cependant possible de chiffrer ses communications en end-to-end, en contactant une seule personne via une demande d'appel sécurisé.

Skype for Business est payant et sa licence est incluse dans les différents packages de licences proposés par Microsoft. En septembre 2017, Microsoft a annoncé que cette solution serait abandonnée au profit de Microsoft Teams, une nouvelle plateforme collaborative basée sur le cloud, il ne s'agit donc pas d'une solution d'avenir.

Avantages

- Solution largement éprouvée par le marché.
- Solution disponible on-premise ou en mode SaaS.
- Solution intégrée à la suite Office offrant de nombreuses possibilités pour les utilisateurs utilisant déjà Exchange notamment.

Inconvénients

- La version on-premise nécessite le déploiement de plusieurs composants et serveurs.
- Ne conviendra pas nécessairement aux petites organisations ou aux besoins ponctuels en raison du modèle économique.
- Faible valeur ajoutée si les utilisateurs n'évoluent pas sur Exchange.
- Usage de solutions de chiffrement end-to-end possible mais limitées à une personne et non-activées par défaut.

Cisco WebEx Meetings

WebEx est une société américaine spécialisée dans les services de logiciels de visioconférence. La solution se présente sous plusieurs licences dont une version gratuite (limitée à 100 participants). Cette solution est disponible :

- En mode SaaS (cloud public) ou sur un cloud privé.
- En mode on-premise sur un serveur dédié ou intégré à un système de téléphonie Cisco.

Selon Gartner, WebEx est aujourd'hui le leader historique sur le marché et est encore considéré comme un acteur visionnaire dans les technologies de communication visio (avec Zoom et Microsoft).

La solution se décline en deux applications, WebEx Teams pour le travail collaboratif et les réunions en audio ou visio et WebEx Meetings pour les réunions audio et vidéo. WebEx propose également du matériel pour réaliser les visioconférences comme des téléphones IP, des écrans et des caméras.

Cisco WebEx Meetings : analyse technique

L'utilisation de la solution WebEx Meetings se fait à travers un navigateur Web avec un plug-in. Il est également possible d'utiliser un logiciel à installer, disponible pour Windows, Android et iOS, qui facilite l'accès aux réunions organisées.

WebEx Meeting propose deux modes de sécurité : par défaut, les communications sont chiffrées entre le serveur et les clients (hop-by-hop). Les données transitent donc en clair sur le serveur. Il est possible d'activer un chiffrement end-to-end, cependant, il est nécessaire d'utiliser un client lourd WebEX CISCO. Cela restreint certaines fonctionnalités, comme le partage d'écran et le téléchargement de fichiers partagés dans l'espace de réunion à la fin d'une session WebEx Meetings.

Avantages

- Leader historique et actuel sur le marché de la visioconférence.
- Une offre commerciale complète qui pourra répondre à la grande majorité des besoins.
- Solution disponible on-premise ou en mode SaaS et sur tous les terminaux.

Inconvénients

- L'installation du client lourd nécessite les droits administrateurs sur le poste.
- La solution ne sera pas forcément adaptée aux TPE et PME, ses capacités étant orientées pour un gros nombre d'utilisateurs.
- Coût de la solution.

Cisco WebEX Teams

Webex Teams est une application qui permet de travailler en équipe en continu à l'aide des réunions vidéo, de la messagerie de groupe, du partage de fichiers et des tableaux blancs. Cisco annonce que la solution fournit un chiffrement de bout en bout de toutes les données. A minima, elles sont transmises et stockées de façon chiffrée.

WebEx Teams permet également aux clients de détenir leurs propres clés de chiffrement et d'éviter de les transmettre dans le cloud. Les données stockées dans le cloud seraient donc uniquement accessibles aux utilisateurs définis. Enfin, Cisco offre la possibilité de fédérer des instances WebEx, éliminant ainsi les risques liés aux comptes invités qui peuvent représenter un risque de confidentialité et de fuite de données.

Cisco WebEX Teams : analyse technique

L'utilisation de la solution WebEx Teams requiert l'installation d'une application coté client, côté serveur (comme WebEx Meetings). Comme évoqué précédemment, les communications et fichiers sont chiffrés avant envoi, et stockés chiffrés également. Il est possible d'autoriser Cisco à accéder aux données, mais selon la documentation technique mise à disposition, sans accord, ils sont dans l'impossibilité de le faire. La solution, comme la plupart des entreprises du marché, permet de connecter l'Active Directory de l'entreprise, afin de faciliter l'authentification, via un SSO (Single Sign-on). Des mécanismes qui s'apparentent à de la DLP sont présents au sein des infrastructures de stockage, ce qui renforce encore un peu plus la protection des données stockées. Les données partagées ne le sont que dans des espaces de réunion, fermés, où seuls des personnes habilitées peuvent ajouter des collaborateurs. Enfin, comme WebEx Meetings, il est possible d'interconnecter la solution à de nombreux services (Google Calendar, Zekdesk, Trello, Twitter…).

Avantages

- Une offre vaste avec des options de messagerie instantanée, de vidéo, tableau blanc, d'EDT, d'échanges de fichiers, etc.
- Facilité de déploiement.
- Combiné aux autres services fournis par l'éditeur, c'est l'une des solutions les plus complètes actuellement existante.

© Orange Cyberdefense

Inconvénients

- La fonction des mémos vocaux semble instable et les messages ne s'envoient pas souvent.
- La solution est très complète mais pourra s'avérer démesurée pour des TPE/PME.
- La solution, comme expliqué précédemment, est payante.

Et dans le monde du libre ?

Le monde du libre n'est pas en reste ! Il existe des applications Open Source qui permettent de pouvoir communiquer sur Internet. Nous avons décidé de présenter trois solutions assez complètes et proposant des fonctionnalités équivalentes aux solutions présentées ci-dessus.

BigBlueButton

Initialement développée pour la formation à distance, BigBlueButton est une solution de visioconférence. Elle permet de réaliser des appels, du partage d'écran, d'images et de présentations et, formation oblige, met à disposition des outils collaboratifs comme un tableau blanc, des systèmes de chat et la possibilité d'utiliser des documents type PDF ou Microsoft. L'outil est proposé gratuitement et publié sous licence générale limitée, autrement appelée GNU, une licence libre.

Techniquement

L'installation d'un serveur BigBlueButton n'est possible que sous Ubuntu, un système spécifique du monde Linux. Il reste possible de l'utiliser au travers d'une machine virtuelle, sous Windows. L'installation ne sera pour autant pas totalement aisée ; la solution requiert un serveur dédié et l'ouverture de nombreux ports de communication ainsi que l'assignation d'un nom de domaine et la génération d'un certificat SSL.

La connexion entre le client et le serveur de BigBlueButton est chiffrée et les informations transitent en HTTPS, dès lors que ce paramètre est activé et que le certificat SSL est configuré correctement. Si un utilisateur partage de l'audio ou de la vidéo, son navigateur utilise la technologie WebRTC, la solution est sécurisée par l'usage du DTLS et du SRTP.

En termes plus simples, les communications ne sont pas chiffrées de bout-en-bout, mais du client vers le serveur. Elles sont ensuite déchiffrées, puis chiffrées à nouveau, vers l'autre client. Le passage sur le serveur s'effectue en clair. Attention donc à la sécurité de la machine qui héberge la solution.

Avantages

- Une solution très complète répondant à de nombreux besoins et usages ;
- Une solution permettant la maîtrise technique totale ;
- La solution est entièrement personnalisable.

Inconvénients

- L'installation et le maintien en conditions opérationnelles et de sécurité de BigBlueButton pourra rebuter plus d'un administrateur.
- L'usage de la solution nécessite un serveur dédié.

Jitsi Meet

Anciennement SIP Communicator, Jitsi est une application Open Source, gratuite, de messagerie instantanée, d'appel audio et de visioconférence. Cette application fait partie du socle interministériel des Logiciels Libres (SILL) qui représente la liste des logiciels libres plébiscités par l'Etat depuis 2016. La solution est multi-plateformes et peut être connectée à d'autres systèmes, comme Google Hangouts par exemple, permettant ainsi d'échanger avec des personnes présentes sur d'autres systèmes de messagerie. Elle permet de passer des appels sur Internet mais aussi des appels vers des fixes et des téléphones mobiles.

Techniquement

Jitsi offre deux modes de fonctionnement :

- A deux personnes, la configuration par défaut est l'usage du Peer-to-Peer, le lien étant établi directement entre ces deux personnes, la connexion est en end-to-end.
- Dès qu'on dépasse deux utilisateurs ou si le Peer-to-Peer est indisponible, on bascule dans du chiffrement des communications en "hop-by-hop" : les communications du client vers le serveur sont chiffrées, tout comme celles du serveur vers le client, mais elles passent en clair sur le serveur.

La sécurité de la machine hébergeant la solution doit être assurée, sous peine d'une rupture de confidentialité au sein des systèmes. Il est également possible d'héberger Jitsi Meet en SaaS mais le risque ne sera que déporté : la sécurité des communications dépendra de celle des serveurs hébergeant la solution.

La solution offre une qualité audio et vidéo plus que satisfaisante, sans latence constatée. Côté utilisateur, Jitsi Meet repose sur une solution WebRTC et HTML5. Ces technologies fonctionnant au travers des navigateurs web classiques, il n'est pas nécessaire d'installer un logiciel pour pouvoir utiliser Jitsi, même si des logiciels sont disponibles pour iOS et Android.

Côté serveur, les dépôts Ubuntu et Debian intègrent les packages de Jitsi Meet avec une installation en partie automatisée. Il est également possible d'installer le côté serveur sur des machines Windows ou MacOS.

Avantages

- Solution gratuite et OpenSource.
- Ne nécessite pas d'installation de client lourd par l'utilisateur.
- Interopérabilité de la solution avec les autres systèmes de communication.

Inconvénients

- Besoin d'un serveur dédié pour la solution car la charge monte très rapidement avec le nombre d'utilisateurs.
- Installation au sein de votre infrastructure, ce qui signifie qu'il faudra maintenir à jour la machine dédiée à Jitsi, ainsi que la configuration de la solution.
- L'installation automatique existe sous certaines distributions, mais pas toutes.
- L'installation manuelle n'est pas à la portée de tout le monde et peut rapidement s'avérer complexe.

Bluejeans

Bluejeans est un service de vidéoconférence qui permet d'organiser des réunions en ligne rassemblant de nombreux participants, via divers appareils et de nombreuses combinaisons de terminaux de vidéoconférence d'entreprise et grand public. Chaque membre de BlueJeans dispose d'une « salle de réunion » privée dans le cloud BlueJeans pour planifier et organiser des réunions.

Sur le marché devenu très concurrentiel de la visioconférence cloud, qui connaît en ce moment un développement fulgurant, l'éditeur BlueJeans Network a été racheté par l'opérateur américain Verizon Communications le 16 avril 2020.

En plus du fait que les réunions n'ont pas de limite de temps, les hôtes peuvent créer jusqu'à 20 sessions en petits groupes et répartir les participants selon les besoins, ce qui est idéal pour collaborer sur des actions. Bluejeans permet de partager son écran, faire des annotations et autoriser l'accès du bureau à distance à un destinataire. Cependant, il n'est pas possible de brouiller l'arrière-plan.

Avantages

- Interopérabilité totale : salles, postes de travail ou appareils mobiles.
- Planification flexible : conférences avec ou sans réservation.
- Gestion Web : planification, hébergement et jonction en quelques clics.
- Pas de nouveau matériel : BlueJeans fournit une infrastructure évolutive et sécurisée.

Inconvénients

- Limitation du nombre de participants entre 100 et 150 ce qui reste encore inférieur comparé aux principaux concurrents.

© Orange Cyberdefense

	Editeur	E2EE*	Déploiement	Mise en place	Fonctionnalités	Tarification	Commentaires
BigBlueButton	Libre	Non		Client Web	+	Gratuit	Attention au maintien en conditions de securité
Meet, by Google Hangouts	USA	Non	SaaS	Client Web	+	Payant (gratuit jusque 10 participants)	Attention à l'utilisation des données utilisa-teurs à des fins marketing
Jisti Meet	Libre	Optionnel en 1:1		Client Web	+	Gratuit	Attention au maintien en conditions de securité
Microsoft Teams	USA	Non	SaaS	Client Web	++	Payant (gratuit jusque 300 participants)	Authentification multi-facteurs
Skype for Business	USA	Optionnel en 1:1	SaaS	Client Lourd	+	Payant	Solution en fin de commerciali-sations
Tixeo	FR	Oui	SaaS	Client Lourd	+	Payant	VISA de sécurité ANSSI
WebEx	USA	Optionnel	SaaS	Client Web (sauf si configuration spéciale)	++	Payant	Approuvé par le FedRAMP (Gouvernement US)
Zoom	USA	En test	SaaS	Client Web/ Client Lourd	+	Payant	Actions prises pour renforcer la sécurité
Bluejeans	USA	Non	SaaS	Client Web	+	Payant	Gartner : Complications potentielles de l'acquisition de Bluejeans par Verizon

*E2EE - End-to-end Encryption : Chiffrement de bout-en-bout

Deploiement On-premise SaaS Déploiement Saas

Conclusion

Comme nous venons de le voir, chaque solution a ses avantages et ses inconvénients. Nous ne donnerons qu'un conseil pour éclairer votre choix : positionnez correctement le curseur entre simplicité d'usage, sécurité et respect de la vie privée.

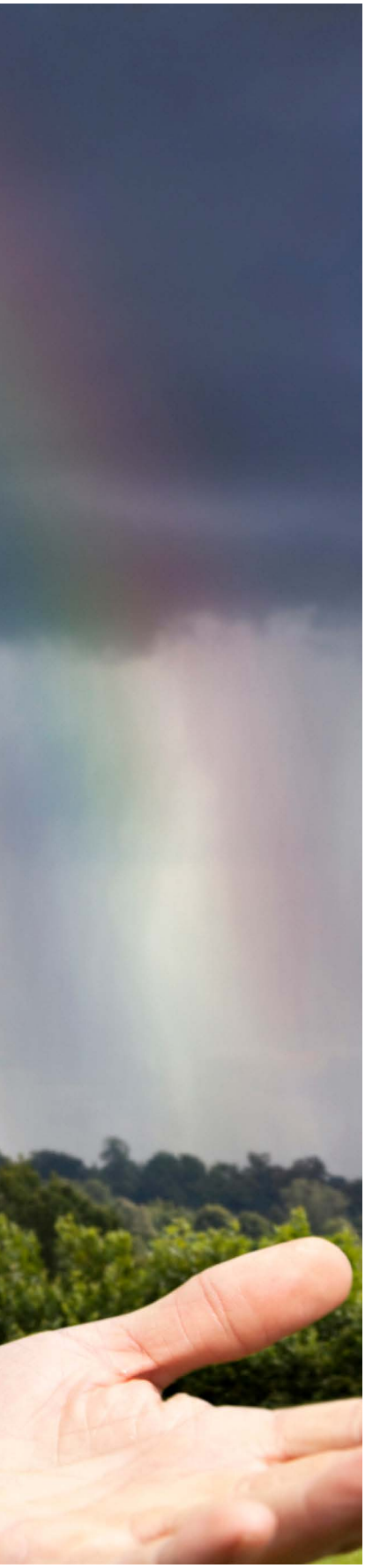
Certaines des solutions présentées sont hautement sécurisées mais nécessitent un abonnement ou des compétences techniques poussées. D'autres sont moins sécurisées mais sont gratuites ou directement disponibles à l'usage. La réflexion doit consister à savoir ce qui doit être protégé d'une part et, de l'autre, à identifier quelles concessions peuvent être faites sur la sécurité.

Peu importe le choix, il doit prendre en compte l'ensemble des risques pris, tant avec la sécurité des données que celles des utilisateurs, clients, élèves... qu'à la conformité juridique des traitements mis en place. Zoom a fait l'objet de nombreuses questions sur sa conformité au RGPD et son usage dans nombre d'organismes, la Direction interministérielle du Numérique allant jusqu'à « déconseiller fortement » l'usage de Zoom. Depuis mai 2020, Zoom a malgré tout nettement renforcé la sécurité de sa solution allant jusqu'à intégrer le chiffrement de bout en bout.

Parce qu'un tableau comparatif est toujours plus parlant, voici ici un comparatif des solutions dont nous venons de parler.

© Orange Cyberdefense

© Orange Cyberdefense



Stefan Lager
SVP Global Service Lines
Orange Cyberdefense

Prédictions de sécurité

Un homme averti…

En vaut deux.

Pour protéger au mieux votre organisation, il faut être au fait des nouveautés les plus importantes en termes de cybersécurité. Nous en avons sélectionné quatre.

1

1 : Cybersécurité VS menace

Les deux facteurs de risques les plus importants pour votre entreprise sont les menaces et les vulnérabilités. Sans vulnérabilité, il est inutile de se soucier de la menace (= rêve). En présence de multiples vulnérabilités critiques, la moindre menace peut avoir un impact considérable.

La menace :

- La commercialisation de produits cyber-offensifs tend à estomper les lignes entre États-nations et acteurs cybercriminels. Des outils de pointe, précédemment réservés à un nombre limité d'acteurs établis, sont désormais généralement disponibles sur le marché noir, ce qui tire vers le bas le niveau requis de la part des cybercriminels pour se lancer.
- Les entreprises paient des sommes importantes aux cybercriminels pour récupérer les clés de chiffrement de données volées ou pour empêcher leur fuite. Cela attire davantage d'acteurs malveillants et permet de financer des attaques plus sophistiquées à l'avenir.

La vulnérabilité :

- Les outils de cybersécurité sont complexes, les compétences et ressources associées sont rares pour déployer ces technologies dans le respect des bonnes pratiques.
- Peu d'organisations cartographient et mesurent leurs capacités de détection. Une stratégie de détection portant sur l'ensemble des cyberattaques s'impose comme une exigence.

Afin de stopper les menaces, il vous faut évaluer l'efficacité de vos solutions de protection. Vous devez vérifier vos capacités de détection pour vous assurer qu'elles sont conformes aux objectifs que vous vous êtes fixés.

© Orange Cyberdefense

2

2 : Cybersécurité VS sécurité des données

La cybersécurité évolue et se concentre de plus en plus sur les données. Cette évolution semble logique puisque, pour les entreprises, les principaux coûts sont liés à des incidents de sécurité impliquant des données.

Indisponibilité des données	Ransomware
Extorsion contre non-divulgation de données	Extortionware
Vol de données	Vol de propriété intellectuelle
Défaut de gestion des données	Défaut de conformité (ex. : RGPD)
Fausses données	Impact sur l'image de marque

Nous estimons que les organisations auront à s'investir davantage dans la compréhension de leurs données et dans leur classification pour appliquer des stratégies de sécurité plus adaptées à leur protection. Cette approche inclut le chiffrement des données (au repos, en transit et en cours d'utilisation).

Il faut aussi permettre l'accès aux données de façon contrôlé. Anciennement, il était coutumier de séparer les individus bienveillants des individus malveillants avec un pare-feu périmétrique, mais, à l'intérieur, peu de segmentation et de sécurité s'appliquaient. Aujourd'hui, les utilisateurs comme les données se trouvent à divers endroits, ce modèle ne convient donc plus.

- **Vérifier :**
  Vérifier l'identité (authentification multi-facteurs), la localisation, la sécurité des équipements…
- **limiter les accès :**
  Limiter les accès au minimum requis et uniquement si nécessaire par application du principe de moindre privilège
- **Assumer les possibles brèches :**
  Créer une infrastructure pour limiter l'impact d'une brèche en segmentant les accès par réseaux et utilisateurs (ex. : micro-segmentation)

Nous prédisons une augmentation des investissements dans des mécanismes de sécurité des données, au détriment d'une sécurité centrée sur les infrastructures.

3

3 : Cybersécurité VS post-COVID

La pandémie de COVID-19 a eu un sérieux impact sur nos vies, comme sur l'industrie de la cybersécurité dans son ensemble. Elle a accéléré la transformation numérique de nombreux clients.

Comme la majeure partie des équipes opère à domicile, les exigences augmentent en matière de solutions de travail collaboratif, d'accès et de sécurité. Nous pensons que même si les choses reviendront à la normale post-COVID, beaucoup d'entreprises ont constaté des avantages dans le télétravail et le poursuivront dans un mode nouveau, plus hybride. Aussi, tous les employés qui, avant, communiquaient localement au sein de réseaux d'entreprise protégés par un pare-feu de qualité professionnelle, connecteront leurs ordinateurs portables à des routeurs bon marché de FAI pour accéder à des données par le biais de connexions VPN.

Ces routeurs à domicile ne présentent généralement pas les mêmes cadences de mise à jour logicielle pour prendre en compte les vulnérabilités nouvellement découvertes ; ce qui accroît leur risque de compromission.

Une fois le routeur sous contrôle, il existe plusieurs moyens d'infecter tous les outils qu'il dessert, dont les postes d'entreprise connectés en permanence au VPN.

Pour limiter les risques liés au télétravail, nous prédisons que les investissements porteront sur :

- Des solutions flexibles d'accès distant : solutions ajustables, à petite et grande échelle, pour répondre à des besoins à l'instant t, sans nécessiter un investissement lourd au départ.
- Des solutions de sécurité nouvelle-génération à appliquer au niveau des terminaux : solutions équipées pour vous prémunir contre des menaces avancées encore inconnues, et reposant sur l'apprentissage machine (Machine Learning) ou des analyses comportementales poussées.
- Des solutions de détection et de réponse à appliquer au niveau des terminaux (Endpoint Detection and Response – EDR). Comme les CyberSOC des entreprises ont beaucoup perdu en visibilité du fait du télétravail, les organisations doivent disposer d'une autre solution leur garantissant non seulement visibilité et détection sur les terminaux distants, mais aussi l'assurance d'une réponse à incident rapide et efficace. Toutefois, il est très probable que beaucoup de ces solutions échoueront pour une de ces deux raisons :
    - L'efficacité des technologies d'EDR est insuffisante, les analystes auront à gérer un gran nombre d'alertes. Le défi ne tient pas dans la détection elle-même, mais bien dans la pertinence de ces détections.
    - Les entreprises n'ont pas les compétences ni les ressources pour analyser les alertes générées par ces outils, d'où des investissements supplémentaires dans des services dédiés, externalisés.

Nous pensons également que, compte tenu des incertitudes qui pèsent toujours sur l'avenir, les clients privilégieront (encore davantage) des modèles récurrents de dépenses d'exploitation plutôt que des investissements de départ lourds.

© Orange Cyberdefense

4

4 : Cybersécurité VS sécurité physique

Lorsqu'il s'agit d'investir dans la cybersécurité, le levier le plus important a toujours été financier. Les clients ont investi dans la cybersécurité pour éviter les ransomwares, se prémunir contre les vols d'IP, etc.

À mesure que tout devient connecté — tant directement (Internet des Objets connectés à des réseaux 5G), qu'indirectement (usines et locaux « intelligents » connectés à des réseaux informatiques internes) — de nouveaux risques sont introduits. Leur impact n'est pas uniquement financier : ils affectent aussi la sécurité des individus.

Les criminels ciblent explicitement des verrous de sécurité

Triton illustre cette menace. Ce malware mis en lumière en 2017 est conçu pour désactiver les systèmes de sécurité physique. Ces systèmes proactifs étaient d'abord faits pour empêcher les dommages physiques dans des environnements technologiques opérationnels (OT) et systèmes de contrôle industriels (ICS), en cas de problèmes mécaniques ou logiciels. La principale mission de ces systèmes est la protection des individus, des environnements et des biens. L'attaque visait à éliminer ces dispositifs de sécurité intrinsèques pour induire des dommages physiques et, éventuellement, nuire aux employés. Il est parfois décrit comme le malware le plus « meurtrier » au monde.

Aux États-Unis, la Cybersecurity and infrastructure Secure Agency (CISA) et la NSA ont émis des alertes spécifiant que des adversaires pouvaient cibler des infrastructures critiques.

Nous jugeons qu'il sera nécessaire de mettre en place des transferts de connaissances entre équipes OT et informatiques. En effet, plusieurs défis sécuritaires en environnement opérationnel peuvent se voir appliquer des solutions informatiques. Par ailleurs, du fait de différents protocoles et de la stricte priorité de disponibilité par opposition à la sécurité, certaines solutions doivent être adaptées ou conçues spécifiquement pour un environnement OT.

Une chose est cependant claire. Le vecteur d'attaque le plus commun contre des usines impliquera des accès par des infrastructures informatiques existantes (ex. : e-mails de phishing, services vulnérables exposés, clés USB infectées, etc.). Et, dans la plupart des cas, les activités de commande et de contrôle des environnements OT doivent aussi traverser les réseaux informatiques.

Les organisations doivent donc investir dans des solutions capables de garantir visibilité et détection des menaces dans les environnements opérationnels comme informatiques, et de corréler ces informations. Aussi, elles pourront répondre rapidement à des menaces susceptibles d'induire des risques financiers et sécuritaires.

Synthèse

Qu'avons-nous appris ?

Etienne Greeff
CTO
Orange Cyberdefense

Difficile de trouver une raison de ne pas lire ce rapport («tl;dr») ! Je l'ai lu et relu un bon nombre de fois.

Il m'a semblé évident que la tâche des défenseurs est particulièrement ardue. Beaucoup de données et d'enseignements doivent être assimilés, puis appliqués pour s'assurer de ne pas voir son nom, ou celui de ses clients, faire les gros titres.

Lorsque l'on tente de démêler des sujets immensément complexes, il peut être opportun de se poser la question «Pourquoi est-ce important ?». Nous considérons souvent la technologie comme un acquis, qu'il s'agisse d'accès distant, d'applications Cloud ou de technologies de communication (dont la visioconférence). Au risque d'énoncer l'évidence, il est important de réaliser que, sans défenseurs dédiés et sans nos modèles technologiques, il serait impossible de faire un usage sécurisé de ces technologies.

Pendant la pandémie, ces technologies sont passées de «souhaitables» ou «complémentaires» à «absolument nécessaires». Ceci se vérifie, qu'il s'agisse de communiquer avec nos grands-parents, un groupe d'amis ou de poursuivre nos activités professionnelles pour permettre à notre économie de fonctionner malgré les changements qui s'opèrent. Du point de vue des défenseurs, la cybersécurité n'a jamais autant compté.

Comme l'expliquait l'oncle de mon super-héros préféré, à grand pouvoir, grande responsabilité. Si ce que nous faisons compte grandement, il est important de prioriser nos efforts sur les sujets pour lesquels notre impact sera le plus grand.

Je ne présumerai pas des priorités de chaque individu ou entreprise. Je conseille, toutefois, de continuer d'établir des priorités, sans être tenté d'appliquer de simples pansements. Étudiez le paysage des menaces pour comprendre les dangers actuels, assurez-vous de comprendre votre surface d'attaque et de connaître vos vulnérabilités, quelles données et procédures causent des insomnies à votre PDG. Appliquez ce savoir pour prioriser vos efforts de protection.

Surtout, assumez que vous n'aurez pas tout juste, tout le temps. Prévoyez les bons plans de secours au cas où le pire adviendrait.

L'un des principaux constats dans ce rapport : la cybercriminalité est désormais une grande industrie. En cause, la confluence de différents facteurs :

- Les monnaies virtuelles ont simplifié la monétisation d'activités de piratage.
- Certaines industries de l'écosystème cybercriminel peuvent rapporter gros et les criminels peuvent se spécialiser dans des activités dans lesquelles ils sont hautement compétents.
- Les sociétés d'assurance sont disposées et aptes à payer des acteurs malveillants, d'où des entrées d'argent régulières dans l'écosystème.
- La majorité des entreprises recourt au numérique pour leurs activités, même des secteurs qui impliquent traditionnellement un face-à-face client/prestataire (les coiffeurs, par exemple).
- Le succès de gouvernements exploitant la cybersécurité à des fins géopolitiques.

Quand une industrie foisonne et brasse de grosses sommes, elle attire rapidement des talents.
Cette tendance est reflétée dans la communauté cybercriminelle. L'exploitation de vulnérabilités iOS, jusque-là dans la nature et tenues secrètes, en est un bon exemple. Ces vulnérabilités valent plus d'un million de dollars sur le marché, on peut donc se demander combien elles ont rapporté aux chercheurs en sécurité pour qu'il ne les dévoile pas et ne réclame pas de primes (bug bounty).

Comment aborder ce nouveau monde dans lequel le piratage est une grosse industrie et où nous sommes confrontés à des adversaires talentueux et motivés ?

© Orange Cyberdefense

Comme indiqué dans ce rapport, il est important de bien maîtriser les bases. En tant que défenseurs, pour l'essentiel, nous nous acquittons de cette tâche. Malheureusement, les données montrent que les attaquants les plus déterminés s'acharnent jusqu'à mettre le doigt sur une faiblesse. Nous avons constaté que les méthodes de certains hackers sont aussi sophistiquées que celles des pirates soutenus par des Etats.

Une différence fondamentale, toutefois : ces derniers sont généralement contraints par les ressources et le temps mis à leur disposition, alors que les premiers sont seulement limités par leurs ressources économiques. Cela fait du hacking un business attrayant et lucratif.

Il est également important de ne pas se baser uniquement sur les technologies, mais aussi sur des processus métier. Nous pensons que les mondes traditionnellement séparés de la cybersécurité et de la fraude doivent davantage converger puisque la cybersécurité n'implique pas seulement des problématiques techniques, mais aussi métier. Sur ce, je vous souhaite de bons vents pour naviguer dans les eaux troubles et parfois périlleuses de la cybersécurité.

« Étudiez le paysage des menaces pour comprendre les dangers actuels, assurez-vous de comprendre votre surface d'attaque et vos vulnérabilités, quelles données et procédures causent des insomnies à votre PDG. Appliquez ce savoir pour prioriser vos efforts de protection. »`
Etienne Greeff, CTO, **Orange Cyberdefense**

Sources

Ce rapport n'aurait pas pu être réalisé sans le travail de nombreux chercheurs, journalistes et organisations du monde entier. Nous avons utilisé avec gratitude leurs publications en ligne à titre de référence ou de contexte.

Sources/liens

https://www.ons.gov.uk/businessindustryandtrade/business/businessservices/bulletins/coronavirusandtheeconomicimpactsontheuk/8october2020
https://media.defense.gov/2020/Oct/20/2002519884/-1/-1/0/CSA_CHINESE_EXPLOIT_VULNERABILITIES_UOO179811.PDF
https://www.cisecurity.org/controls/cis-controls-list/
https://www.microsoft.com/security/blog/2020/06/16/exploiting-a-crisis-how-cybercriminals-behaved-during-the-outbreak/
https://blog.checkpoint.com/2020/08/11/threat-actors-join-in-the-race-towards-a-coronavirus-vaccine/
https://blog.checkpoint.com/2020/08/11/threat-actors-join-in-the-race-towards-a-coronavirus-vaccine/
https://www.top10vpn.com/research/investigations/COVID-19-vpn-demand-statistics/
https://media.defense.gov/2020/Oct/20/2002519884/-1/-1/0/CSA_CHINESE_EXPLOIT_VULNERABILITIES_UOO179811.PDF
https://threat-advisories.secdata.com/threats/viewSignal/SIG-4618
https://threat-advisories.secdata.com/threats/viewSignal/SIG-4467
http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf
https://www.hackread.com/8-best-dark-web-search-engines-for-2020/
https://www.europol.europa.eu/publications-documents/cyber-telecom-crime-report-2019
https://www.fbi.gov/news/stories/alphabay-takedown
https://software.imdea.org/~juanca/papers/ppi_usenixsec11.pdf
https://www.tenable.com/blog/a-look-at-the-vulnerability-to-exploit-supply-chain
https://research.checkpoint.com/2018/malvertising-campaign-based-secrets-lies/
https://www.digitalshadows.com/blog-and-research/the-ecosystem-of-phishing/
https://www.trendmicro.com/vinfo/pl/security/news/cybercrime-and-digital-threats/bulletproof-hosting-services-cybercriminal-hideouts-for-lease
https://www.spamhaus.org/news/article/792/bulletproof-hosting-theres-a-new-kid-in-town
https://www.digitalshadows.com/blog-and-research/the-ecosystem-of-phishing/
https://www.cbsnews.com/news/hackers-steal-medical-records-sell-them-on-dark-web/
https://www.bleepingcomputer.com/news/security/network-intruders-selling-access-to-high-value-companies/
https://www.zdnet.com/article/network-access-sold-on-hacker-forums-estimated-at-500000-in-september-2020/
https://securelist.com/the-botnet-ecosystem/36279/
https://www.europol.europa.eu/newsroom/news/20-arrests-in-qqaazz-multi-million-money-laundering-case
https://docs.microsoft.com/en-gb/MicrosoftTeams/get-clients
https://www.cisco.com/c/en/us/products/collaboration-endpoints/collaboration-room-endpoints/index.html?dtid=osscdc000283#~explore-video-devices
https://cloud.google.com/access-transparency/
https://en.wikipedia.org/wiki/WebRTC
https://en.wikipedia.org/wiki/HTML5
https://www.bleepingcomputer.com/news/security/zoom-will-provide-end-to-end-encryption-to-all-users/
https://www.zdnet.com/article/bluejeans-announces-end-to-end-encryption-for-video-meetings/

© Orange Cyberdefense

Quel outil de visioconférence choisir ?

https://blog.zoom.us/zoom-rolling-out-end-to-end-encryption-offering/
https://www.courrierinternational.com/article/teletravail-la-plateforme-de-visioconference-zoom-utiliser-avec-moderation
https://www.vice.com/en/article/k7e599/zoom-ios-app-sends-data-to-facebook-even-if-you-dont-have-a-facebook-account
https://www.wired.com/story/zoom-security-encryption/
https://www.nextinpact.com/article/30168/108854-zoom-retour-sur-accumulation-failles
https://medium.com/bugbountywriteup/zoom-zero-day-4-million-webcams-maybe-an-rce-just-get-them-to-visit-your-website-ac75c83f4ef5
https://www.tixeo.com/visioconference-securisee/a-propos/
https://www.ssi.gouv.fr/entreprise/certification_cspn/tixeoserver-version-11-5-2-0/
https://www.eff.org/deeplinks/2020/03/google-says-it-doesnt-sell-your-data-heres-how-company-shares-monetizes-and
https://docs.microsoft.com/en-us/microsoftteams/teams-overview
https://fr.wikipedia.org/wiki/OAuth
https://docs.microsoft.com/fr-fr/skypeforbusiness/plan-your-deployment/security/key-security
https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cloudCollaboration/spark/esp/cisco-spark-security-white-paper.pdf
https://fr.wikipedia.org/wiki/Datagram_Transport_Layer_Security
https://fr.wikipedia.org/wiki/Secure_Real-time_Transport_Protocol
https://www.data.gouv.fr/fr/datasets/socle-interministeriel-de-logiciels-libres/
https://www.nextinpact.com/article/30181/108877-la-direction-interministerielle-numerique-deconseille-fortement-application-zoom

Jeu-concours :
Déchiffrez notre énigme !

Les règles du jeu sont simples :

- Déchiffrez la question posée.
- Trouvez la réponse à cette question.
- Envoyez-la, en clair (non-chiffrée) via le formulaire ci-dessous.

A gagner :

- **Une paire d'Airpods (Apple)**
- **Une Nintendo Switch Lite**
- **Un casque à réduction de bruit Sennheiser HD**
- **Un MiniDrone Parrot**
- **Une enceinte portable Ears Wonderboom**

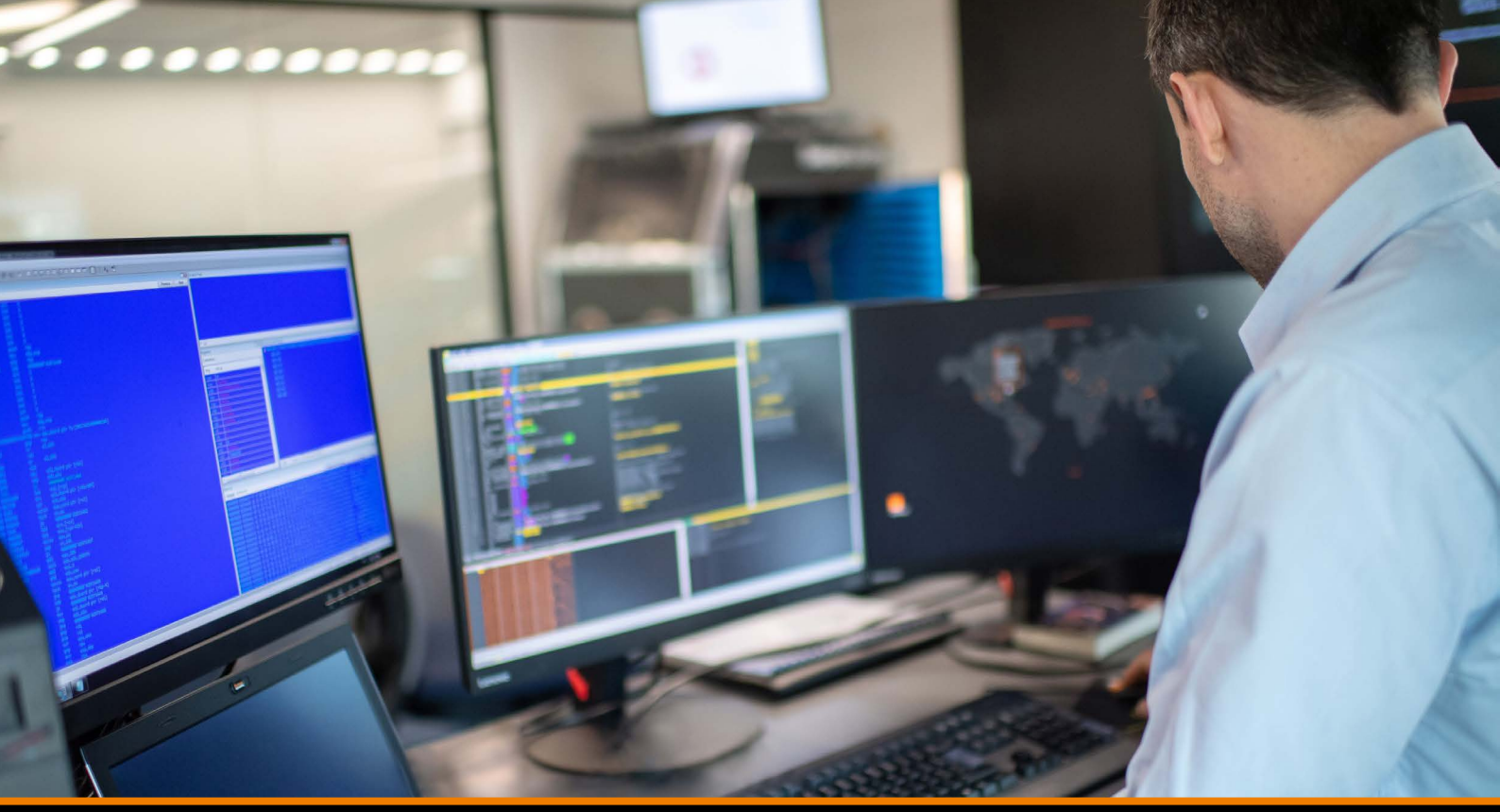
Cinq gagnant.e.s seront tiré.e.s au sort parmi les bonnes réponses le 30 décembre 2020.

Pour envoyer votre réponse, cliquez-ici : orangecyberdefense.com/fr/security-navigator/

DJEIKDUZTREDEKLEJKDNL
KSZLDJFRNKLQPSGFRKLM
DEKALDEKKNNEJNDYALEZ
SJEQ’OMITGXKSKFEDEKLP
ASMEKQAPLEORUNDLHK
KXGKEDLFRMOTGNTLNTL
KKLMLEJDPSSGFFNKLM
FRNFRLEPITLZHQYSBCELF
CFRKLKFRKDORAEEKPR
FKORFOQPOEMLKFXBJR?

Un grand merci à tous.tes nos expert.e.s en sécurité, partout dans le monde.

Clause de non-responsabilité
Orange Cyberdefense met ce rapport à disposition "en l'état" sans aucune garantie d'exhaustivité, d'exactitude, d'utilité ou d'actualité. Les informations contenues dans ce rapport sont de nature générale. Les opinions et les conclusions présentées reflètent un jugement fait au moment de la publication et peuvent changer à tout moment. Orange Cyberdefense n'assume aucune responsabilité pour les erreurs, omissions ou résultats obtenus en cas d'utilisation de ces informations. Si vous avez des préoccupations spécifiques en matière de sécurité, veuillez contacter Orange Cyberdefense pour une analyse plus détaillée et pour obtenir des conseils en sécurité.



Pourquoi Orange Cyberdefense ?

Spécialistes de la cybersécurité
Orange Cyberdefense est spécialisé dans les services et solutions de cybersécurité et dispose de 25 ans d'expérience dans les services managés, notamment pour le compte des plus grandes entreprises du monde.

Une expertise exceptionnelle
Nos 11 SOC et 17 CyberSOC, répartis dans le monde entier, offrent un accès immédiat, 24 heures sur 24, 7 jours sur 7, 365 jours par an, à des spécialistes qui traiteront les incidents et assureront une disponibilité continue.

Nos partenaires
Nos partenariats dans le monde de la cybersécurité nous permettent d'accéder plus facilement à leurs expertises techniques et à leurs feuilles de route.

Une connaissance approfondie de la sécurité
Orange Cyberdefense traite plus de 50 milliards d'événements par mois, ce qui nous donne un accès inégalé aux menaces actuelles et émergentes.

www.orangecyberdefense.com