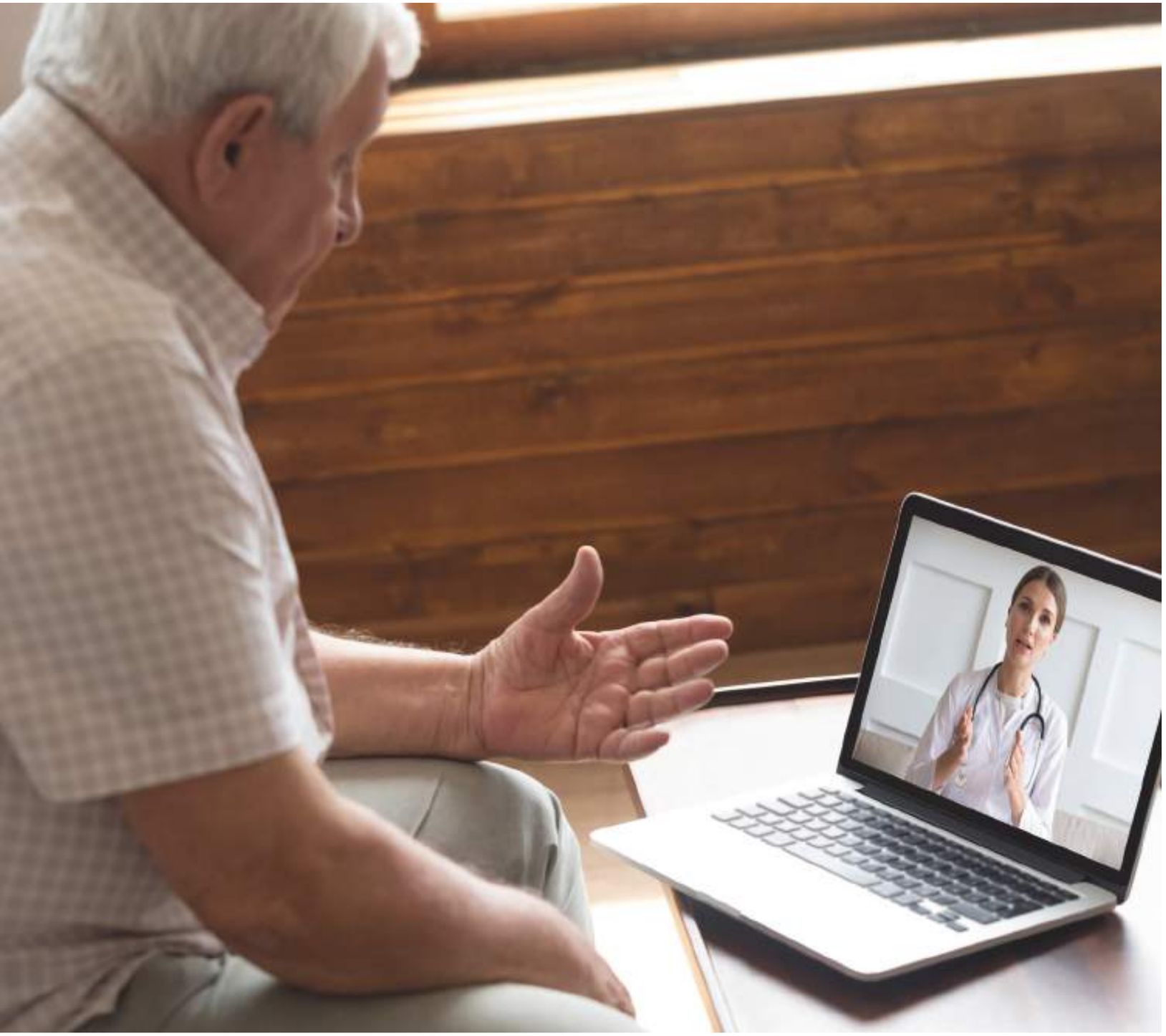
Orange
Cyberdefense

COVID-19:
Quand un risque biologique devient numérique
Analyser la crise dans la crise

Table des matières



Charl van der Walt
Responsable de la recherche en matière de sécurité
Orange Cyberdefense

Contexte:

Une crise mondiale

Alors que la pandémie de coronavirus COVID-19 continue de se propager dans le monde entier, les acteurs de la cybermenace tentent de tirer profit de la crise sanitaire mondiale en développant des logiciels malveillants ou en lançant des attaques sur le thème du COVID-19. Toutefois, ce type de comportement d'exploitation du contexte par le paysage de la cybercriminalité n'est qu'un élément d'un tableau plus vaste de la cybersécurité. Orange Cyberdefense publie ce document afin d'attirer l'attention sur un ensemble de faits qu'il est nécessaire de prendre en compte dès maintenant.

En raison de la nature mondiale de la pandémie COVID-19, cette crise a un impact significatif sur tous les aspects de la vie des particuliers et des entreprises, y compris la cybersécurité. Dans ce climat de peur, d'incertitude et de doute, la conscience de la menace est suffisamment élevée. Cela peut néanmoins générer un niveau d'anxiété exagéré. Dans ce contexte, la présente ressource est le résultat de notre effort collectif, en tant qu'Orange Cyberdefense, qui consiste à partager nos connaissances, nos idées et notre expérience concernant notre conception de la cybersécurité dans le contexte de la crise du COVID-19 et dans le monde post-coronavirus qui, espérons-le, n'est pas trop éloigné.

L'analyse présentée ici comprend les apports :

- du Centre de recherche sur la sécurité (SRC)
- de l'Équipe d'intervention en cas d'urgence informatique (CERT)
- du Malware Epidemiology Lab
- de l'Unité OSINT
- du CyberSOC
- d'Advisory & Architecture
- du Bureau mondial du CISO
- du Bureau mondial des CTO

Résumé des conclusions

Nous pensons que les points principaux suivants doivent être pris en considération par nos clients :

1. Les **logiciels malveillants et le phishing** exploitant le COVID-19 comme un leurre risquent de se multiplier. Nous avons également observé des cas sophistiqués d'attaques par watering holes utilisant des cartes du COVID-19 pour déposer des exploits et des logiciels malveillants. Ce rapport décrit plusieurs exemples spécifiques de ce type, mais la tendance devrait se poursuivre et s'intensifier sous différentes formes.
2. Nous allons observer une recrudescence de **campagnes de désinformation générale** déformant les faits liés à COVID-19 pour servir des programmes politiques divers. Le fact checking est essentiel.
3. Heureusement, plusieurs **équipes de ransomwares se sont engagées à ne pas cibler les établissements médicaux et de recherche**. Il s'agit là d'un répit bienvenu mais on ne peut pas s'attendre à ce qu'il ait un impact substantiel. Les menaces « traditionnelles », comme les ransomwares, persistent.
4. Dans l'intervalle, nous avons assisté à des **attaques ciblées contre des organisations médicales** impliquées dans la recherche, le traitement ou toute autre réponse au COVID-19, en particulier dans le monde occidental, apparemment pour saper la réponse à la pandémie. Nous prévoyons que cette situation se poursuive, car des groupes étatiques et hacktivistes de diverses natures intensifient leurs efforts.
5. La crise du COVID-19 est une crise mondiale. Toutefois, les tensions géopolitiques antérieures à la pandémie vont probablement s'accentuer. Nous nous attendons à voir de **nouvelles vagues de cyber-perturbations parrainées par des États** à mesure que la pandémie se répandra, ce qui pourrait avoir un impact direct sur la gestion de la pandémie.
6. Puisque de plus en plus de personnes travaillent à domicile en utilisant des solutions d'accès à distance mal conçues et mal déployées nous anticipons une multiplication des **attaques contre les technologies d'accès à distance**, les passerelles VPN et les points d'accès Wi-Fi domestiques et partagés mal sécurisés, contribuant à l'apparition de graves compromissions.
7. **La visibilité des SIEM et des équipes d'opérations de sécurité sera réduite** dès lors que les endpoints se connecteront via le VPN ou directement à internet. Ils ne sont donc pas soumis au même niveau de surveillance que lorsqu'ils sont connectés au réseau local de l'entreprise. Cela réduit le niveau global de sécurité sur lequel une entreprise peut compter. Nous prévoyons également que le CIRT et d'autres capacités de réaction aux incidents seront entravées, contribuant à allonger les délais de réaction et les temps d'arrêt par les attaquants, voire à empêcher la détection des attaques.
8. Durant cette période, de plus en plus **d'activités informatiques seront déplacées vers le cloud**, obligeant les programmes de sécurité à prendre en compte les infrastructures locales et en cloud dans leurs stratégies.
9. **La plupart des entreprises accélèrent leur transition vers le commerce en ligne**, lorsque ça n'est pas déjà fait, notamment dans le secteur du commerce de détail. Durant cette course effrénée, nous nous attendons à une accumulation de dettes de sécurité, cette dernière étant sacrifiée au profit de la rapidité de mise sur le marché.
10. Étant donné le nombre croissant de travailleurs à domicile, nous prévoyons que l'infrastructure Internet partagée, cruciale pour les entreprises, sera mise à rude épreuve. **Les performances se dégraderont probablement**, et même s'effondreront dans certains cas. Pour la plupart des organisations, la fonction informatique et le plan de continuité des activités sont devenus des éléments nettement plus stratégiques.

Si vous n'avez que 5 minutes…

La pandémie du COVID-19 a modifié les modèles de menace pour la sécurité de cinq manières importantes :

- **Vos employés sont plus vulnérables qu'à l'accoutumée à l'ingénierie sociale et aux escroqueries.**
- **Vous avez moins de contrôle et de visibilité sur les systèmes informatiques que vous protégez que ce à quoi vous êtes habitué.**
- **Vos utilisateurs peuvent se connecter à partir de systèmes et d'environnements qui sont fondamentalement peu sécurisés ou mal configurés**
- **Vous vous êtes peut-être précipité pour mettre en place des systèmes d'accès à distance sans avoir le temps de les planifier et de les exécuter aussi bien que vous le souhaiteriez.**
- **Vous, votre équipe et vos fournisseurs êtes susceptibles de fonctionner avec des capacités réduites.**

Résumé des recommandations :

Nous vous proposons de vous concentrer sur les réponses suivantes, par ordre d'importance :

- Mettre en place des procédures et des systèmes d'intervention d'urgence.
- Mettre en place une ligne d'assistance téléphonique pour le soutien à la sécurité et se préparer à élargir l'équipe en charge de cette assistance.
- Revoir la sauvegarde et la récupération après sinistre (DR).
- Fournir à vos utilisateurs les informations dont ils ont besoin pour prendre de bonnes décisions en matière de sécurité.
- Fournir un accès à distance sécurisé.
- Organiser la visibilité sur des terminaux distants.

Rester rationnel pendant la crise

Les conseils sont bon marché en temps de crise. Mais chaque entreprise est différente, et nous ne prétendons pas savoir comment chacune doit réagir à la menace particulière qui pèse sur sa sécurité en ce moment. Nous proposons toutefois les lignes directrices suivantes aux entreprises qui évaluent à l'heure actuelle la menace pour la sécurité et planifient leur réponse à cette menace :

1. Comprendre que nous vivons un état de menace accrue, mais que notre vulnérabilité n'a que légèrement augmenté. Nous ne pouvons pas contrôler la menace, mais nous pouvons contrôler la vulnérabilité, alors concentrons-nous sur ce point.
2. Comprendre ce qui a changé et ce qui n'a pas changé. Le modèle de menace de votre entreprise peut être très différent aujourd'hui de ce qu'il était hier, mais il peut aussi très bien ne pas l'être. S'il n'a pas changé, alors votre stratégie et vos opérations n'ont pas à changer non plus.
3. Formez des partenariats mais évitez les foules. Plus que jamais, vos fournisseurs, votre prestataire de services et même vos concurrents sont dans le même bateau. Ils n'ont peut-être pas toutes les réponses non plus, mais il est temps de tendre la main et de trouver des partenaires qui ont des points de vue équilibrés et rationnels et d'éviter les communautés qui font de la publicité et génèrent de l'hystérie.
4. Maintenir le contexte. L'informatique et internet ont survécu pendant vingt ans malgré diverses défaillances de sécurité. Il ne fait aucun doute que la situation actuelle est préoccupante, et que le risque d'une crise fondamentale de la cybersécurité au cours de notre vie est réel et ne peut être ignoré. Cependant, à l'heure actuelle, la crise est d'ordre médical et humain. Ne vous laissez pas distraire par le battage médiatique sur la cybersécurité.
5. Travaillez intelligemment, pas durement. Vous ne pourrez pas faire grand-chose pendant cette période de capacité réduite, alors consacrez du temps et de l'énergie à analyser vos principales préoccupations et à vous concentrer sur celles-ci.

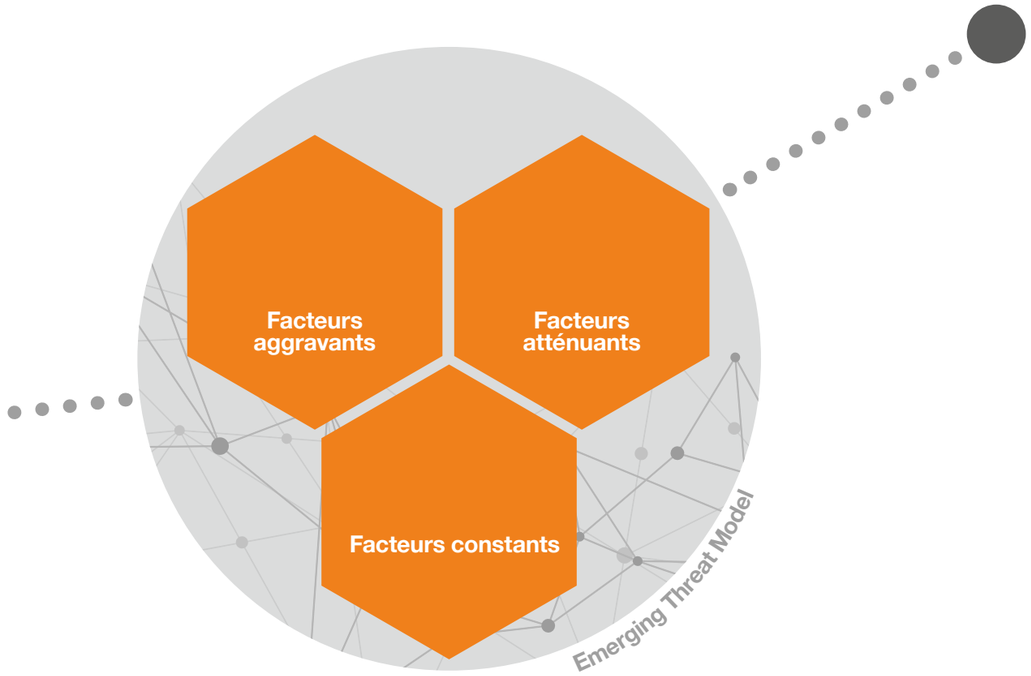
Partie I:

Impact de la pandémie

De nombreuses réalités fondamentales en matière de sécurité ne sont pas vraiment transformées par la pandémie. Cependant, certains défis majeurs, notamment ceux liés à notre propre capacité à surveiller et à répondre aux menaces et aux vulnérabilités, sont devenus considérablement plus difficiles à relever. D'autre part, il convient de noter que l'agresseur est également humain et que les comportements de l'agresseur peuvent également changer en raison de l'impact du virus, voire même réduire le niveau de menace actuel.

Comment évaluer l'impact de la pandémie COVID-19 sur notre niveau de menace actuel ?

Dans cette section du document, nous tentons de décrire et de résumer l'impact de la pandémie COVID-19 sur le modèle de la cybermenace



Facteurs aggravants

Comme tant d'autres dans cette crise, certains des éléments auxquels sont confrontés les praticiens de la sécurité informatique sont, sinon totalement « sans précédent », du moins bien pires que ce que nous avons connu jusqu'à présent. Plusieurs caractéristiques de la pandémie aggravent la situation de la cybersécurité. Nous les examinerons en détail dans la présente section.

Une vulnérabilité accrue à la coercition

A l'heure actuelle, les utilisateurs que nous protégeons sont plus vulnérables à la coercition. Ils sont pour la plupart des travailleurs dont la routine quotidienne a été brusquement interrompu. C'est d'autant plus vrai pour ceux qui ont des enfants en âge d'être scolarisés ou qui s'occupent de parents âgés.

La psychologie suggère qu'en période de crise et d'anxiété exagérée, la vigilance des individus peut être réduite tandis que leur appétit pour d'autres comportements à risque est susceptible d'augmenter

Les individus devraient agir plus prudemment en ce moment, mais nous risquons en réalité d'observer le contraire.

Ces comportements plus risqués, associés à un appétit généralement accru pour l'information et l'actualité, rendent les individus plus vulnérables à l'ingénierie sociale et aux escroqueries de toutes natures.

En outre, les individus sont généralement prédisposés psychologiquement à donner la priorité aux risques aigus à court terme plutôt qu'aux risques vagues à long terme, de sorte qu'ils seront enclins à ouvrir un document Word promettant un vaccin contre les coronavirus quand bien ils le savent potentiellement malveillant.

Mais ce n'est pas la seule raison pour laquelle la psychologie humaine en temps de crise peut s'avérer dangereuse pour la sécurité.

Selon un article paru dans Psychology Today[1], il est entendu que les gens sont susceptibles d'adopter des comportements plus risqués, comme boire et fumer, pour les aider à gérer leur anxiété. Le principe peut s'appliquer également aux personnes qui choisissent de prendre des risques avec leur cyber-hygiène afin de faire face à leur anxiété en temps de pandémie.

D'autres éléments augmentent encore le niveau de risque.

Selon un rapport d'Europol, les facteurs qui provoquent des changements dans la criminalité et le terrorisme comprennent[2]:

- Une forte demande pour certains biens, équipements de protection et produits pharmaceutiques.
- Une diminution de la mobilité et de la circulation des personnes dans l'UE.
- Les citoyens restent à la maison et font de plus en plus de télétravail, en s'appuyant sur des solutions numériques.
- Les limitations de la vie publique rendront certaines activités criminelles moins visibles et les déplaceront vers les lieux d'habitation ou en ligne.
- Une anxiété et une peur accrues qui peuvent créer une vulnérabilité à l'exploitation.
- Une diminution de l'offre de certains biens illicites dans l'UE.

Les criminels sont bien entendu prêts à profiter des faiblesses actuelles des individus.

Alors que des millions de citoyens du monde entier sont totalement ou partiellement bloqués, nous observons dans le monde entier une volonté désespérée d'obtenir des nouvelles et des informations sur la pandémie ainsi qu'un sentiment généralisé de peur et d'urgence. Les attaquants se voient présenter l'appât parfait pour toutes sortes d'attaques, notamment le phishing, le Business Email Compromise (BEC), les watering holes et autres arnaques. Nous devons anticiper à la fois une augmentation du volume des attaques d'ingénierie sociale et la vulnérabilité de nos utilisateurs à tomber dans leur piège.

Le travail à domicile rend l'équipement personnel vulnérable

Afin de ralentir la propagation du virus, de nombreuses organisations qui normalement n'encourageraient pas leur personnel à travailler à domicile ont maintenant été obligées de mettre en place à la hâte des politiques de travail à domicile et des infrastructures d'accès à distance.

Cela introduit plusieurs risques supplémentaires, notamment :

- Une dépendance accrue aux communications « virtuelles » comme le courrier électronique, les réseaux sociaux, la vidéoconférence, les appels et les sms, rendant les utilisateurs plus vulnérables aux attaques d'ingénierie sociale et moins à même de valider les communications en face à face.
- L'ennui et l'isolement social conduisent à une vigilance moindre et à une volonté accrue de prendre des décisions plus risquées.
- Une dépendance accrue à l'informatique domestique et à des appareils personnels dont les configurations et les profils de risque sont inconnus.
- Une utilisation accrue de routeurs Wi-Fi domestiques mal patchés et mal configurés, qui sont également de plus en plus pris pour cible par les attaquants.

Nous anticipons une escalade des attaques contre les passerelles VPN et autres infrastructures d'accès à distance, car les solutions nouvellement mises en œuvre pourraient ne pas être aussi sécurisées qu'elles devraient l'être. Les routeurs et les points d'accès Wi-Fi partagés pourraient également entraîner des attaques et des compromissions supplémentaires. Il est également possible que des dispositifs personnels non sécurisés et qui pourraient potentiellement être déjà infectés, soient utilisés pour se connecter à distance au réseau de l'entreprise, favorisant l'implantation des acteurs de la menace. Cette situation est exacerbée par une diminution substantielle du niveau de visibilité des opérations SIEM et SOC sur les endpoints des utilisateurs, et une génération de solutions de sécurité des endpoints encore très répandue qui n'est pas encore adaptée à contrer les menaces contemporaines.

Utilisation accrue du téléphone portable et des appareils mobiles personnels

Le mobile est, depuis un certain déjà, un problème difficile à résoudre pour le secteur de la sécurité. Les appareils sont difficiles à gérer avec les outils de sécurité classiques, ne se prêtent pas bien au déploiement d'agents et ne sont souvent pas sous le contrôle direct de l'entreprise. Dans le même temps, les attaques directes (comprenant les exploits et les malware) et indirectes (comprenant les applications malveillantes, le phishing et le smishing) sont en constante augmentation et constituent une problématique sérieuse pour toute stratégie de sécurité. Nous devons nous attendre à ce que les travailleurs à distance utilisent plus que jamais leurs téléphones portables personnel et d'entreprise pour accéder en ligne à des données et des systèmes personnels et professionnels.

Nous avons abordé les risques liés aux logiciels malveillants et aux applications mobiles malveillantes dans d'autres parties de ce rapport, mais la gestion des correctifs pour les appareils mobiles risque également de devenir un problème pendant la crise. Comme le montrent les données de 2018 de notre Centre de recherche sur la sécurité, il peut falloir jusqu'à trois mois pour que 40 % seulement du parc d'appareils sous Android adoptent une nouvelle version du système d'exploitation. Grâce à l'approche « walled-garden » d'Apple, les appareils iOS s'en sortent beaucoup mieux. Cependant, entre 5 et 20 % des utilisateurs des deux plateformes ne déploieront jamais de correctifs de sécurité importants.

Alors que la crise pousse les utilisateurs à dépendre plus que jamais des plateformes mobiles des entreprises et des particuliers pour accéder aux données et aux services, les problématiques préexistantes auxquels nous sommes confrontées pour sécuriser l'écosystème mobile sont aggravées. Certaines menaces, comme le phishing, sont traitées avec les solutions existantes. D'autres, cependant, comme les malwares, les applications malveillantes et les patchs pour les systèmes d'exploitation mobiles, continuent de nous mettre au défi et augmentent en raison de la crise.

Les organisations ont réduit leur capacité à mener des opérations de sécurité

Le risque actuel pour la sécurité est encore exacerbé par une réduction de la capacité et de l'agilité opérationnelle des Blue Teams des entreprises :

- Un niveau réduit d'attention et de vigilance des Blue Teams des entreprises, car elles sont personnellement distraites par la crise, ont du mal à se concentrer et peuvent tomber elles-mêmes malades.
- Une capacité réduite à réparer et à renforcer les ordinateurs de l'entreprise qui ne sont pas connectés au réseau local de cette dernière.
- Une capacité réduite à déployer des ingénieurs sur place pour surveiller et effectuer des correctifs sur des systèmes qui ne sont pas accessibles à distance.
- Les solutions VPN et d'accès à distance rapidement déployées et mal sécurisées, qui sont aussi spécifiquement visées par les attaquants.
- Une diminution substantielle du niveau de visibilité que les SIEM et SOC ont sur les endpoints des utilisateurs, ces derniers n'étant plus connectés au réseau local de l'entreprise. Même en utilisant des VPN, les configurations courantes (par exemple, le « split tunneling ») permettent d'accéder à Internet sans les contrôles habituels présents lors de la connexion depuis le bureau.
- L'adoption rapide de solutions basées sur le cloud computing créera encore davantage d'angles morts, les utilisateurs ayant de moins en moins besoin d'accéder au réseau d'entreprise. La détection d'attaques dans le cloud est une tâche difficile qui oblige les Blue Teams à se concentrer sur la surveillance des enpoints.
- Une capacité réduite à répondre aux attaques et aux compromissions suspectes, à renforcer l'isolement des endpoints et à mener des expertises cyber-légales. Cela pourrait générer des délais de réponse et des temps d'arrêts plus longs au profit des attaquants, voire rendre impossible la détection des attaques.
- Une capacité réduite de communication et de coordination face à des crises de cybersécurité comme celles de Wannacry ou de notPetya.

De nombreuses équipes informatiques ont dû faire des pieds et des mains pour répondre à la soudaine migration massive vers un modèle de travail à domicile. Elles doivent maintenir leur activité pendant la crise afin d'assurer la protection, la détection et la réponse des infrastructures informatiques critiques, bien qu'elles-mêmes sont touchées par la pandémie. Nous pouvons nous attendre à ce que les écosystèmes de la cybercriminalité nous laissent un certain répit, étant eux aussi touchés par la crise, mais nos observations à ce jour laissent penser qu'il ne sera pas si important. Les technologies de l'information des entreprises apparaissent donc beaucoup plus vulnérables.

La chaîne d'approvisionnement est également soumise à un niveau de risque accru

Depuis plusieurs années déjà, les menaces pesant sur la chaîne d'approvisionnement constituent un facteur de plus en plus important dans les modèles de risque des entreprises. Pour de nombreuses organisations, il existe en effet une corrélation directe entre le niveau de sécurité des fournisseurs et le leur, comme l'ont illustré des incidents récents tels que la campagne de lutte contre les logiciels malveillants « notPetya ».

Au début de l'année 2020, le Département de la Sécurité intérieure des Etats-Unis a rapporté que les sociétés biopharmaceutiques faisaient partie des dix industries stratégiquement ciblées par les pirates chinois pour voler des secrets commerciaux, et que les pirates exploitaient activement les relations entre les fournisseurs de services informatiques et leurs clients pharmaceutiques pour mener des compromissions à bien[3].

Les tactiques de compromission de la chaîne d'approvisionnement ont également été caractéristiques des plus récentes campagnes d'espionnage de l'APT41. Le groupe chinois aurait accès à des environnements de production pour injecter du code malveillant dans des fichiers légitimes, ces derniers étant ensuite distribués aux organisations victimes.
Les pirates chinois ne sont pas les seuls à cibler la chaîne d'approvisionnement. Le FBI a aussi publié le 30 mars une notification au secteur privé (Private industry notification), mettant en garde contre une campagne de logiciels malveillants baptisés Kwampirs - vaguement liée aux pirates informatiques soutenus par l'État iranien - qui vise spécifiquement le secteur de la santé. Les Kwampirs sont aussi soupçonnés de se déplacer latéralement dans la chaîne d'approvisionnement[4].

Alors que les risques sont élevés en cette période, les entreprises doivent se préoccuper de la sécurité de leurs fournisseurs et partenaires autant que de la leur. Comme c'est le cas pour notre réponse à la pandémie COVID-19, nous sommes directement dépendants les uns des autres dans la maîtrise des menaces de cybersécurité.

Dépendance à l'égard de l'insécurité L'IdO et l'OT vont augmenter

Des préoccupations importantes concernant la sécurité et la confidentialité des diverses technologies de l'IdO, de l'OT et de l'automatisation (les voitures à conduite autonome et les robots de nettoyage par exemple) ont été fréquemment exprimées ailleurs.

Comme les contacts entre humains deviennent moins fréquents et que les travailleurs de toutes sortes sont encouragés à se tenir à l'écart des lieux publics, nous prévoyons que le recours à la robotique, aux véhicules automatisés et à d'autres technologies IdO et OT se développera plus rapidement qu'on ne pouvait le croire auparavant. Cela ne constitue pas une menace en soi, mais exacerbe les préoccupations actuelles concernant la sécurité de ces technologies.

Internet et les infrastructures en cloud sont mis à rude épreuve

C'est une époque sans précédent pour Internet. Nos paradigmes architecturaux sont balayés par les entreprises et leurs fournisseurs qui s'activent massivement pour permettre à tous leurs salariés de se connecter à distance du jour au lendemain.

Avec l'augmentation du volume de travailleurs à domicile, nous nous attendons à ce que l'infrastructure Internet partagée soit également mise à rude épreuve. Cela pourrait se traduire par une dégradation des performances des infrastructures et des services critiques tels que les DNS, Microsoft Office 365, Zoom et WebEx, ainsi que d'autres fournisseurs de services, ou même par une panne qui pourrait avoir des répercussions sur la continuité des activités.

La chaîne d'approvisionnement en TI est mise sous tension

La crise insidieuse à laquelle nous sommes aujourd'hui confrontés atteint tout le monde, y compris les fournisseurs de matériel, de logiciels et de services dont votre entreprise dépend pour ses propres opérations informatiques et dont dépend, par extension, sa capacité à répondre aux cybermenaces exacerbées.

Puisque les entreprises de tous secteurs sont touchées de diverses manières à l'échelle mondiale, leurs chaînes d'approvisionnement fonctionneront elles aussi à capacité réduite. Nous pouvons anticiper que la fourniture de matériel et de logiciels, l'assistance, les services professionnels, l'assurance, la conformité, la réponse aux incidents, la criminalistique et l'application de la loi soient tous affectés négativement, réduisant ainsi davantage la capacité d'une entreprise à faire face à un niveau de cybermenace accru.

Les cyberconflits risquent de s'aggraver

La pandémie de COVID-19 est une crise d'une ampleur sans précédent, et il est juste de dire que le monde entier est en guerre. Si ces crises ont pour effet remarquable de rassembler les populations, elles peuvent aussi, hélas, exacerber et aggraver les conflits existants pour les ressources et les tensions idéologiques.

Nous pensons que l'impact de la pandémie au Moyen-Orient nourrira le sentiment anti-occidental[5] .Parmi les conséquences possibles, une guerre cybernétique est à envisager. Elle pourrait viser les installations médicales et de recherche ainsi que les institutions gouvernementales et les infrastructures importantes.

En outre, divers conflits régionaux en cours dans la région pourraient encore s'aggraver, la BBC rapportant que le COVID-19 pourrait s'avérer être une bombe à retardement dans l'ensemble de la région[6]. Cela pourrait conduire à une nouvelle augmentation de l'hacktivisme et à d'autres formes de cyberattaques.

Notre unité OSINT propose également les observations suivantes spécifiques au piratage informatique parrainé par l'État :

Nos renseignements sur la menace considèrent l'APT41 comme l'un des groupes de pirates informatiques les plus actifs et les plus dangereux à l'heure actuelle (30 mars 2020). Dans le contexte de l'épidémie de COVID-19, les activités d'espionnage vont s'intensifier. Nous pensons que les brevets et les informations exclusives utilisées pour fabriquer des vaccins et des tests de détection rapide ont de forts risques d'être ciblés.

Hacktivisme

Une autre hypothèse porte sur les efforts idéologiques visant à discréditer le secteur pharmaceutique par le biais du « cyber-hacktivisme ». La colère générée par diverses théories conspirationnistes concernant la recherche d'un traitement au COVID-19 pourrait conduire les hacktivistes à lancer des attaques de déni de service.

L'industrie pharmaceutique et les soins de santé sont des secteurs difficiles à protéger. Plusieurs menaces peuvent constituer des risques pesant sur la protection des données : nombre élevé d'activités de fusions-acquisitions, apprentissage machine et intelligence artificielle, nombreuses industries partenaires, mais aussi des menaces provenant de l'intérieur de l'entreprise (ex : attaques de la chaîne d'approvisionnement).

Dans le cas d'une cyber-attaque réussie, les conséquences sont potentiellement désastreuses pour l'entreprise. Le vol de données ou l'espionnage peuvent entraîner la reproduction d'essais cliniques, des pertes financières considérables, des litiges et même des conséquences dangereuses pour la santé des patients : temps d'arrêt, déversement de matières dangereuses, production de médicaments inefficaces ou toxiques, etc.[7]

Nous prévoyons que les attaques politiquement motivées par des acteurs soutenus par les États contre les systèmes associés aux efforts de réponse au COVID-19 se poursuivront à un rythme soutenu, les attaquants et les hacktivistes de divers États-nations intensifiant leurs efforts. Nous pensons, en effet, que l'impact de la pandémie au Moyen-Orient pourrait déclencher des attaques visant à miner les efforts de réponse au COVID-19, retardant ainsi les tentatives de reprise en main de la situation. Les groupes de pirates informatiques parrainés par des États qui ciblent l'industrie pharmaceutique sont actifs et dangereux pour le secteur.

Facteurs constants

De nombreux éléments terribles de la crise actuelle surpassent totalement toute expérience antérieure à laquelle ait pu être confrontée notre génération. Cependant, bien que les criminels et autres pirates informatiques exploitent les tensions que subissent les personnes et les systèmes aujourd'hui, la situation actuelle en matière de cybersécurité n'est pas fondamentalement différente de celle à laquelle nous avons été confrontés dans une réalité antérieure. Comme il s'agit de la première hypothèse sur laquelle nous devrions nous baser, nous ne mettrons ici en évidence qu'un petit nombre de ces réalités antérieures.

L'ingénierie sociale a toujours exploité l'actualité

Alors que la pandémie COVID-19 se propage dans le monde entier, les campagnes de phishing et de logiciels malveillants cherchent à jouer sur les craintes et la faim des individus pour l'information. Ces campagnes ont été observées à travers des cartes en ligne légitimes permettant de suivre la propagation du virus, de fausses applications mobiles et des sujets de courriel et pièces jointes utilisés comme appâts dans des courriers électroniques de phishing. L'idée d'utiliser l'actualité pour attirer l'attention des victimes ou soulever leur intérêt et gagner leur confiance est aussi ancienne que la sécurité sur Internet elle-même. Les réponses sont aussi les mêmes.

L'anxiété généralisée face à la pandémie, combinée au besoin accru d'information des populations et à leur vulnérabilité à la coercition, rendent l'exploitation du thème COVID-19 par l'agresseur particulièrement insidieuse. Cependant, ces menaces ne sont pas, en elles-mêmes, fondamentalement nouvelles et ne nous posent donc pas de nouveaux défis. En effet, au-delà de messages rationnels envoyés à nos utilisateurs visant à les informer, nous voudrions conseiller à nos clients de ne pas se prendre à l'hystérie collective et de se concentrer sur la lutte stratégique contre la crise humaine à laquelle nous sommes confrontés.

Les hackers vont pirater

Un article disponible sur le Bleeping Computer décrit une escalade de l'activité de l'APT41 chinois, en corrélation avec l'apparition du coronavirus : « Le groupe d'État chinois APT41 a été à la tête d'une série d'attaques qui ont utilisé des exploits récents pour cibler les failles de sécurité dans les appareils et dispositifs Citrix, Cisco et Zoho d'entités d'une multitude de secteurs industriels à travers le monde. On ne sait pas si la campagne qui a débuté en janvier 2020 était conçue pour tirer profit du fait que les entreprises devaient alors se concentrer sur la mise en place de tout ce dont leurs travailleurs à distance avaient besoin pendant le confinement ou la quarantaine COVID-19, mais, comme l'ont constaté les chercheurs de FireEye, les attaques sont assurément de nature ciblée »[8].

Comme le suggère l'article, il ne fait guère de doute que les acteurs de la menace, quelle que soit leur nature, vont chercher à instrumentaliser cette crise à leur avantage.

Il convient toutefois de noter que les « failles de sécurité des appareils et dispositifs Citrix, Cisco et Zoho » sont antérieures à la crise, sont bien comprises et auraient dû être corrigées bien avant le déclenchement de la pandémie.

Des problématiques encore moins évidentes, comme les risques posés par le travail à distance via des points d'accès Wi-Fi non fiables ou mal configurés, ont été bien comprises par Orange Cyberdefense et sont largement discutées dans le secteur. Un article du journaliste Geoff White décrit un document que notre centre de recherche sur la sécurité a publié sur le sujet et illustre ce point : « Le problème est que le fournisseur de points d'accès Wi-Fi ne se contente pas de recevoir temporairement le trafic internet de votre machine - il peut aussi potentiellement le manipuler et ainsi causer de graves problèmes de sécurité ».[9]

Bien qu'elles puissent être ciblées de manière plus agressive aujourd'hui, les vulnérabilités de sécurité, aussi bien techniques que procédurales, sont généralement bien connues et comprises par nous et il est généralement dans nos capacités d'y remédier.

Les humains ont toujours été vulnérables

L'attrait pour l'ingénierie sociale que l'on observe au travers de la crise COVID-19 ne constitue que la moitié du problème. Comme nous l'avons déjà dit, l'autre moitié réside dans le fait que les humains sont fondamentalement prédisposés à tomber dans le piège de ce genre d'escroquerie, même dans des circonstances plus « ordinaires ».

Bien que la situation actuelle semble favoriser l'agresseur, nous devons également noter que les préjugés psychologiques fondamentaux dont dépend l'ingénierie sociale sont profondément ancrés dans la condition humaine. Il peut s'agir d'une mauvaise nouvelle dans la mesure où nous n'avons pas réussi à remédier à ces vulnérabilités, même dans des circonstances « ordinaires ». Mais c'est aussi une bonne nouvelle, car il ne s'agit pas d'une nouvelle difficulté à relever mais une à laquelle nous sommes déjà à mi-chemin de répondre.

Les données médicales ont toujours ont été précieuses aux yeux des cybercriminels

Les cyber-attaques ciblant des industries de natures diverses sont devenues de plus en plus courantes ces dernières années. Le secteur de la santé ne déroge pas à la règle. 2015 a été un point culminant, avec de nombreuses entreprises de santé basées aux États-Unis touchées et plus de 113,27 millions de dossiers exposés.

Dans un rapport publié par Orange Cyberdefense en 2019, les chercheurs ont conclu que « les données liées à la santé ont plus d'attrait pour un attaquant dans la mesure où la multitude de données qu'elles contiennent, comme les données financières, les DCPs, les antécédents médicaux, génèrent plus de valeur » et que « les données de santé volées sont vendues à un prix plus élevé en moyenne sur les marchés en ligne par rapport à d'autres données volées telles que les données financières ».[10]

Dans un récent rapport, Reuters a également évalué que la valeur financière de données sur la santé pouvait être jusqu'à dix fois supérieure à celle du numéro d'une carte bancaire. [11]

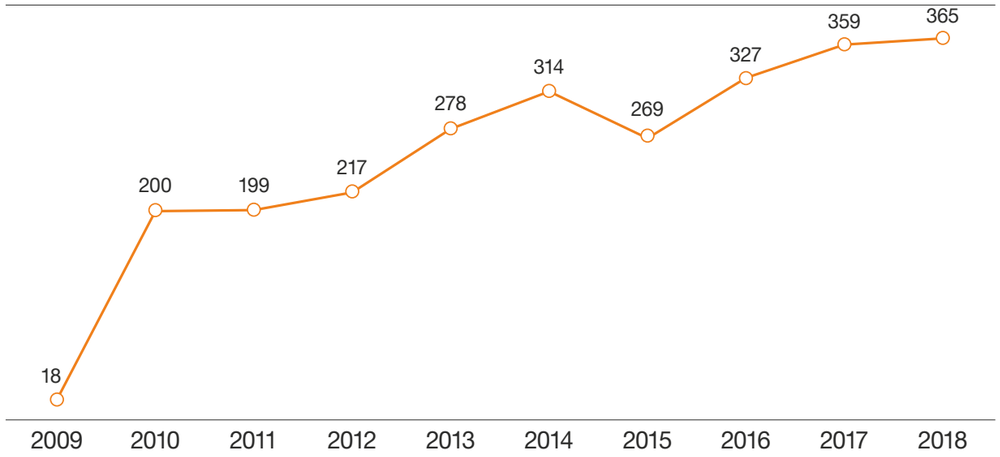
Trois raisons expliquent l'intérêt du hacker pour les groupes de l'industrie pharmaceutique : premièrement, il y a une profusion de propriété intellectuelle. Deuxièmement, la sensibilité des données des patients attire les pirates informatiques potentiels. Troisièmement, le secteur pharmaceutique est un secteur controversé : il superpose les questions de santé publique à une logique commerciale.

Compte tenu des liens étroits qu'entretiennent le monde commercial et le monde scientifique, les grands laboratoires sont régulièrement accusés de conflits d'intérêts. Ce secteur a donc été la cible de dénonciateurs et de cyber-hacktivistes.

Le modèle de menace que les services de santé doivent prendre en compte et adresser pendant la crise du COVID-19 n'est pas vraiment nouveau. Compte tenu de la valeur des données et des systèmes utilisés par les hôpitaux et organisations analogues, les attaques et les compromissions qu'ils subissent aujourd'hui étaient déjà monnaie courante.

Number of reported data breaches

Reported databreaches in the USA



Source: https://www.hipaajournal.com/healthcare-data-breach-statistics/

Les services de santé ont un bilan médiocre en matière de sécurité

Dans un document publié en 2019 par Orange Cyberdefense, nous indiquions que « le nombre de données liées à la santé exposées a augmenté de 73,6 %, avec un total de 3 452 442 dossiers médicaux volés ». [12]

Le secteur des soins de santé, comme tout autre secteur, se numérise massivement afin d'accroître l'accessibilité et de renforcer le partage des informations aux fins d'une meilleure prise en charge des patients. L'effet collatéral de cette évolution en est l'augmentation de la surface d'attaque. Les connaissances, la sensibilisation en matière de sécurité, ainsi que le budget, s'avèrent souvent insuffisants.

Les données ne sont pas la seule préoccupation. Certains dispositifs médicaux, tels que les moniteurs de fréquence cardiaque ou les pompes à insuline, ont été conçus pour servir un objectif médical. Pourtant, leur sécurité n'est souvent pas considérée comme suffisante. Les appareils eux-mêmes n'ont peut-être pas de capacités de stockage de données, mais ils fournissent néanmoins un point d'entrée aux serveurs et aux autres dispositifs de réseau qui stockent des données sensibles et sont souvent essentiels au bon fonctionnement d'un établissement médical.

Les attaques ransomware contre les prestataires de soins de santé ont également augmenté au cours de la dernière décennie. Nombre d'entre eux sont passés du papier à des solutions électroniques d'enregistrement médical qui ne sont pas soumis à des contrôles de cybersécurité adéquats. Cela en fait des cibles de choix pour des attaques intentionnelles ou des dommages collatéraux causés par des campagnes de rançonnement. L'exemple le plus tristement célèbre est celui de l'incident dévastateur qu'a connu le NHS au Royaume-Uni.[13]

Bien qu'il existe des preuves « anecdotiques » selon lesquelles l'activité de divers acteurs, incluant des groupes parrainés par des États, s'accélère actuellement, la réalité est que les industries de santé ont été la cible d'attaques bien avant la crise actuelle. Notre étude de 2019 sur le sujet montre que les dossiers médicaux ont une valeur plus élevée que les autres DCPs sur le marché noir. Les services médicaux ont été ciblés en raison du caractère précieux de la propriété intellectuelle qu'ils détiennent, et pour être totalement honnête, parce qu'ils se sont avérés être des cibles faciles pour les vecteurs d'attaque les plus simples, tels que les ransomwares.

Facteurs atténuants

Il est difficile d'entrevoir une lueur d'espoir dans la situation actuelle, mais certains éléments de cette crise peuvent jouer en notre faveur et contribuer à atténuer les risques de cybersécurité auxquels nous sommes susceptibles d'être confrontés.

Les agresseurs sont aussi des humains

Bien qu'il soit trop prématuré de se prononcer de manière définitive sur ce point, on peut supposer sans risque que les pirates informatiques, les escrocs, les hacktivistes et les opérateurs publics seront, comme le reste d'entre nous, tous touchés par cette crise.

> Les opérateurs de sécurité offensifs, tout comme leurs homologues défensifs, sont dotés de budgets et de patrons. Ils tombent malades comme nous tous, ont des familles dont ils doivent s'occuper et ont besoin de gagner de l'argent pour vivre. Ils ont des besoins en fournitures, équipements et autres ressources pour travailler. Certains ont même une éthique et un code moral. Bien que nous ayons observé les premiers signes d'une escalade des activités criminelles et des activités soutenues par les Etats, il paraît raisonnable de s'attendre à ce que les capacités des attaquants soient également réduites actuellement et qu'elles puissent encore diminuer à mesure que l'impact de la pandémie se fera ressentir et que la vie normale sera encore davantage perturbée.

La communauté de la sécurité se mobilise

« L'enfer n'est rien comparé à la communauté de la cybersécurité pendant une pandémie ».[14]

Comme c'est si souvent le cas lors de véritables crises humaines, les bonnes gens du monde entier se rassemblent pour mettre à disposition leurs compétences et leurs ressources. Il en va de même dans le domaine de la cybersécurité, et plusieurs efforts notables pour développer et appliquer des initiatives communautaires ont déjà été lancées.

CV19 – « un groupe nouvellement formé de professionnels de la sécurité de l'information, comprenant des RSSI d'entreprise, des testeurs d'intrusion, des chercheurs en sécurité, et bien d'autres, ont juré de faire tout ce qui est en leur pouvoir pour aider à fournir un soutien en matière de cybersécurité aux services de santé à travers le Royaume-Uni et l'Europe ».[15]

Selon l'article du magazine Forbes cité plus haut, les cinq principes de cette initiative sont les suivants :

1. Être honnête et disponible
2. Agir toujours avec intégrité
3. Être aimable et respectueux envers les autres volontaires
4. Être flexible et collaborer
5. Faire confiance à tous et utiliser l'expertise de chacun

Ce mode de pensée noble et altruiste est exactement ce dont le monde a besoin en ce moment, et pourrait bien nous aider à renverser la tendance en matière de cybercriminalité.

BBC reporter Joe Tidy has created a web application, in conjunction with a number of corporate sponsors, to track corona-related phishing emails. The site can be found at https:// coronavirusphishing.com/.

The ThreatCoalition is another such global volunteer initiative focused on creating and sharing COVID-19 related threat intelligence.[16]

Nous travaillions déjà à la maison

Une « plaisanterie » répandue dans la communauté technique de la cybersécurité suppose de dire que les membres des Blue Teams et des Red Teams étaient déjà socialement isolés, vivant seuls et ne sortant jamais, avant même que la quarantaine ne devienne la norme.

Chez Orange Cyberdefense, par exemple, nous avons organisé le télétravail et fermé nos bureaux dans le monde entier presque du jour au lendemain, sans pratiquement aucun impact ressenti sur nos opérations.

> Aussi (pas)drôle que cela puisse être, la réalité est pour le moins rassurante : la plupart des entreprises de produits, d'assistance et de services de sécurité informatique ont déjà des structures et infrastructures de travail à distance. Les fournisseurs de services et d'assistance à la sécurité informatique dans le monde entier ont jusqu'à présent conservé un niveau élevé de capacités et devraient continuer à s'adapter aux nouvelles contraintes, quand bien même la crise se poursuit.

Nous savons comment régler le problème

Comme il faut espérer que vous l'ayez compris si vous avez lu notre rapport jusqu'ici, il n'y a pas d'éléments techniques dans le paysage actuel de la cybermenace liée au coronavirus qui ne soit fondamentalement nouveau.

> Même si les conditions deviennent plus difficiles et semblent favoriser l'attaquant plus que le défenseur, chaque faiblesse technique que nous devons contrer a déjà été observée, étudiée et traitée. Nous savons comment résoudre ces problèmes. Le défi qu'il nous reste à relever maintenant est celui de penser clairement, d'agir stratégiquement et de travailler efficacement pour résoudre les problèmes les plus importants en utilisant le peu de ressources dont nous disposons encore.

Partie II:

Répondre à la dimension cybernétique de la crise

À lumière des menaces et des préoccupations soulevées ci-dessus, nous proposons les conseils suivants aux entreprises et aux professionnels qui envisagent le facteur cybernétique comme ce qui pourrait être la plus grave menace au bien-être mondial depuis la seconde guerre mondiale.

Tout comme le virus lui-même, il existe un risque réel et inquiétant pour la cybersécurité.

Ses conséquences ne sont toutefois pas inévitables ni son impact irrémédiable. Considérez votre stratégie de cyber-réponse sous cet angle et conservez un esprit ouvert.

Le monde est actuellement subjugué par la peur, l'incertitude et le doute - des émotions auxquelles l'industrie de la sécurité a été tristement vulnérable et honteusement coupable d'exploiter.

Pas de panique

Le monde est en ce moment en panique face à plusieurs menaces réelles et imminentes. N'aggravons pas les choses en créant une panique inutile autour des cybermenaces également. Afin de rester rationnels durant la crise, nos lignes directrices sont les suivantes :

1. Comprendre que nous vivons un état de **menace accrue, mais que notre vulnérabilité n'a que légèrement augmenté**. Nous ne pouvons pas contrôler la menace, mais nous pouvons contrôler la vulnérabilité, alors concentrons-nous sur ce point.
2. **Saisir ce qui a et ce qui n'a pas changé.** Le modèle de menace de votre entreprise peut être très différent aujourd'hui de ce qu'il était hier, mais il peut aussi ne pas l'être. S'il n'a pas changé, alors votre stratégie et vos opérations n'ont pas à changer non plus.
3. Former des partenariats mais évitez les foules. **Vos fournisseurs, votre prestataire de services et même vos concurrents sont tous, plus que jamais, dans le même bateau**. Ils n'ont peut-être pas toutes les réponses non plus, mais il est temps de tendre la main et de trouver des partenaires qui ont des points de vue équilibrés et rationnels et d'éviter les communautés qui font de la publicité et nourrissent l'hystérie.
4. **Contextualiser**. L'informatique et Internet ont survécu pendant vingt ans en dépit de diverses défaillances de sécurité. Il ne fait aucun doute que la situation actuelle est préoccupante, et que le risque d'une crise fondamentale de la cybersécurité au cours de notre vie est réel et ne peut être ignoré. Cependant, à l'heure actuelle, la crise est d'ordre médical et humain. Ne vous laissez pas distraire par le battage médiatique sur la cybersécurité.
5. **Travailler intelligemment, pas durement.** Vous ne pourrez pas faire grand-chose pendant cette période de capacité réduite, alors consacrez du temps et de l'énergie à étudier vos principales préoccupations et à vous concentrer sur celles-ci.

Prenez le temps de vous améliorer

Le scénario n'est pas noir ou blanc. Si des éléments de votre infrastructure ou de vos processus n'étaient pas prêts lorsque cette crise a éclaté, il est temps maintenant de les revoir et de les améliorer. Les ressources informatiques domestiques et les solutions d'accès à distance peuvent être progressivement perfectionnées. Tout comme pour notre réponse à la pandémie : chaque victoire compte

Espérez le meilleur, prévoyez le pire

Il est possible que les choses empirent. Dès que le temps le permet, faites un effort pour envisager la réponse de votre entreprise en cas de compromis ou de violation. L'hameçonnage, le credential stuffing, la compromission des systèmes d'accès à distance, les DDoS, les ransomwares et autres attaques d'extorsion sont actuellement des sujets de préoccupation spécifiques. Il n'existe pas de formule unique ou simple pour y répondre, mais il est essentiel de mettre en place les personnes, les systèmes et les processus nécessaires pour réagir rapidement et en toute sécurité à un incident.

Faites preuve de bon sens avec vos collaborateurs

Comme nous l'avons déjà mentionné dans ce document, un domaine de menace exagérée est lié au niveau de vulnérabilité accru des personnes à l'ingénierie sociale, et à l'exploitation accrue du contexte par les agresseurs pour mener des attaques d'ingénierie sociale.

Rappelez à vos employés et à vos équipes informatiques de rester vigilants, fournissez-leur des informations précises et de guidez-les en douceur à l'aide d'exemples.

Toutefois, dans le cadre d'une équipe qui doit faire face à une crise sanitaire mondiale, la menace de ne pas recevoir des communications essentielles peut être plus importante que celle de recevoir des communications malveillantes. Il faut donc en tenir compte lors de la communication avec le personnel sur les nouvelles cybermenaces et leur importance relative.

Contrôlez vos fournisseurs

Pour de nombreuses entreprises, il existe une corrélation directe entre le niveau de sécurité des fournisseurs et le leur, comme l'ont illustré des incidents récents tels que la campagne contre les logiciels malveillants « notPetya ». En cette période où le niveau de risque est élevé, les entreprises doivent se préoccuper de la sécurité de leurs fournisseurs et partenaires autant que de la leur. Comme dans notre réponse à l'épidémie de COVID-19, nous sommes directement dépendants les uns des autres pour maîtriser les menaces de cybersécurité.

Les équipes chargées de la sécurité et des risques doivent envisager d'ouvrir et de maintenir des canaux de communication avec les fournisseurs, prestataires, consultants et partenaires susceptibles d'avoir accès à des systèmes et des données sensibles. Discutez de leurs réactions face aux niveaux de menace élevés à ce stade et assurez-vous qu'elles restent appropriées et conformes aux vôtres.

Restez en contact avec vos partenaires

Les fournisseurs de services comme Orange Cyberdefense font tout ce qui est en leur pouvoir pour rester prêts et disponibles afin de soutenir leurs clients. Comme nous l'avons déjà mentionné, les fournisseurs de services informatiques sont généralement bien préparés pour offrir une assistance à distance et devraient, dans l'ensemble, disposer de ressources même en cas d'aggravation de la crise. Les fournisseurs de services ont évidemment un intérêt économique à conserver et mettre à disposition leurs capacités, mais beaucoup d'entre eux réagissent aussi de manière altruiste à cette crise, en aidant là où ils le peuvent, quand ils le peuvent.

Il existe également diverses initiatives de soutien gouvernementales (comme le NCSC au Royaume-Uni) et communautaires (comme le CV-19, dont nous avons parlé précédemment) qui peuvent proposer des conseils, des orientations et même un soutien direct si nécessaire.[17]

Tendre la main, maintenir la communication et rester en contact. Notre équipe et d'autres personnes disposent d'informations, de renseignements et d'autres ressources qui peuvent grandement vous aider si le pire devait arriver, ou pour réduire la probabilité qu'il arrive...

Priorisez

Comme nous l'avons déjà dit, nous voulons concentrer nos ressources limitées sur les éléments de la menace qui nous préoccupent le plus en ce moment. Il est cependant très difficile de déterminer quelles sont les « menaces importantes ». C'est en effet un défi à propos duquel avons beaucoup parlé et écrit ces derniers temps. Nous estimons que le paysage des cybermenaces (même sans crise mondiale aggravée) est trop complexe et trop fluide pour être réduit à de simples listes ou aides-mémoire. Face au risque de tomber dans ce piège, nous suggérons de réfléchir pendant cette crise aux priorités à partir de deux réalités : les choses qui ont changé et celles qui n'ont pas changé.

Ce qui a changé

Comme cela devrait être maintenant manifeste à la lecture du document, nous estimons que seul un petit aspect du paysage de la cybermenace a considérablement changé à la suite de la pandémie. Voici ce qui, pour nous, est différent :

1. Vos salariés sont plus vulnérables qu'à l'accoutumée à l'ingénierie sociale et aux escroqueries.
2. Vous disposez de moins de contrôle et de visibilité sur les systèmes informatiques que vous protégez que ce à quoi vous êtes habitué.
3. Vos utilisateurs peuvent se connecter à partir de systèmes et d'environnements qui sont fondamentalement peu sécurisés ou peut-être simplement mal configurés.
4. Vous vous êtes empressé de mettre en place des systèmes d'accès à distance sans avoir le temps de les planifier et de les déployer aussi bien que vous le souhaiteriez.
5. Vous, votre équipe et vos fournisseurs êtes susceptibles de fonctionner avec des capacités réduites.

Ce qui n'a pas changé

Bien que nous vivions une période sans précédent dans l'histoire humaine récente, il y a vraiment très peu de choses qui sont fondamentalement nouvelles dans le paysage actuel des menaces. Ainsi, nos priorités d'un point de vue cybernétique n'ont pas besoin de s'écarter trop de ce qu'elles étaient avant la crise :

1. Le phishing, le spear-phishing, le Business Email Compromise (BEC) et d'autres formes d'attaques d'ingénierie sociale ne sont pas nouvelles, ni le fait que nos utilisateurs soient fondamentalement prédisposés à tomber dans le piège tendu par ce type d'attaques. Notre réponse à ces vecteurs d'attaque n'a pas changé, malgré le niveau de menace élevé.
2. Les attaques contre les interfaces basées sur le cloud, les systèmes d'accès à distance et les passerelles VPN se multiplient depuis un certain temps déjà. En effet, pour cette raison, la récente campagne du groupe de hackers chinois APT41 exploitant ces techniques ne peut être définitivement mise en corrélation avec la crise, bien que le timing coïncide. Les faiblesses de sécurité exploitées par APT41, bien que potentiellement plus graves, sont bien comprises et relativement simples à corriger.
3. Le travail à distance et la facilitation d'un accès à distance sécurisé pour les travailleurs nomades est un défi très bien compris et notre boîte à outils contient plusieurs technologies et approches, adaptées à presque tous les budgets et niveaux de sophistication technique.
4. La main-d'œuvre moderne est nomade depuis deux décennies maintenant, et les fournisseurs et les équipes informatiques peuvent proposer plusieurs méthodes pour surveiller, maintenir et gérer les endpoints à distance. Des exigences encore plus complexes, comme l'isolement et le triage à distance, sont facilement satisfaites, même sans disposer d'un budget exorbitant.

La liste de priorités que nous proposons

Sur la base des points que nous avons présentés ci-dessus, nous proposons la série de priorités générales suivante que les entreprises devraient considérer à la lumière du paysage actuel des menaces.

Si vos propres priorités en matière de sécurité ne sont pas déjà claires pour vous, nous vous proposons de vous concentrer sur les éléments suivants, par ordre d'importance :

1. Mettre en place des procédures et des systèmes de réponse aux incidents.
2. Mettre en place une ligne d'assistance téléphonique pour le soutien à la sécurité.
3. Réviser la sauvegarde et la récupération après sinistre (DR).
4. Fournir à vos utilisateurs les informations dont ils ont besoin pour prendre de bonnes décisions.
5. Fournir un accès à distance sécurisé.
6. Organiser la visibilité sur des endpoints éloignés.
7. Considérer les applications mobiles malveillantes.
8. Envisagez de raccorder et de renforcer les endpoints distants, y compris les endpoints mobiles.
9. Revoir votre police d'assurance.

Mettre en place des procédures et des systèmes de réponse aux incidents

Compte tenu de tout ce dont nous avons discuté, nous devons supposer que des attaques se produiront pendant cette période et que des compromissions réussies sont plus à prévoir qu'à l'accoutumée. Dans cette hypothèse, planifier et se préparer est essentiel.
Prenez le temps d'animer une session de planification avec les principaux acteurs des technologies de l'information et de la sécurité afin d'examiner vos capacités de réaction en cas de suspicion de compromission ou de violation. Voici quelques points à prendre en compte :

- Comment détecter une brèche ? Quels indicateurs pourraient être mis à votre disposition en plus des indicateurs classiques, par exemple les rapports des utilisateurs ou des prestataires de services externes ?
- Qui doit être informé et impliqué en cas de crise ?
- Comment une équipe d'intervention pourrait-elle communiquer et collaborer, même dans le pire des scénarios où des systèmes sécurisés seraient touchés ?
- Comment communiqueriez-vous avec d'autres parties prenantes comme les utilisateurs, les régulateurs, les clients, les membres du conseil d'administration et les actionnaires ?
- Êtes-vous en mesure d'isoler un terminal ou un serveur, que ce soit à distance ou sur place ?
- Avez-vous accès à une équipe de réponse aux incidents compétente, que ce soit en interne ou par l'intermédiaire d'un partenaire ?
- Disposez-vous d'un plan de sauvegarde et de récupération efficace ? Quand a-t-il été testé pour la dernière fois ? Peut-il être testé maintenant ?
- Êtes-vous dotés d'une politique sur les ransomwares et l'extorsion ? Si vous estimez être prêts à payer une rançon, avez-vous les fonds et les systèmes nécessaires pour le faire ? Vous devez également réfléchir à votre stratégie de négociation et désigner à l'avance une équipe de négociation.
- Comprenez-vous vos exigences réglementaires, par exemple en ce qui concerne l'OIC britannique, et êtes-vous prêt à les respecter en cas de violation ?

Mettre en place une ligne d'assistance téléphonique pour le soutien à la sécurité

Vos utilisateurs sont très anxieux en ce moment et les cybermenaces ne font que nourrir leur degré d'anxiété.

La mise à disposition aux utilisateurs et même aux clients d'un numéro ou d'une adresse qu'ils pourraient utiliser pour parler à quelqu'un de façon rationnelle des attaques techniques et cognitives qu'ils pourraient suspecter, ou de leurs propres systèmes et comportements, pourrait s'avérer être un outil puissant au service de la réduction de leur niveau d'anxiété ou même dans le but d'améliorer votre posture de sécurité.
Si vous disposez déjà d'une ligne d'assistance téléphonique, préparez-vous (au moins au début) à une augmentation rapide du volume des appels, des courriels et des autres méthodes de communication existantes.

Réviser la sauvegarde et de la récupération après sinistre (DR)

Deux menaces qui étaient réelles avant même la crise se sont sans doute aggravées en raison de la pandémie. Il s'agit des rançons et du déni de service.

Prenez le temps de réviser l'état de vos sauvegardes et l'état de disponibilité de vos données et des processus de récupération après sinistre (Disaster Recovery)

Dans ce cadre, vous devez penser aux travailleurs à domicile et aux données avec lesquelles ils peuvent travailler localement. Si vous ne disposez pas déjà d'un système de sauvegarde adapté pour les utilisateurs distants, les solutions de cloud public facilement disponibles comme Google Drive, Dropbox et Microsoft OneDrive peuvent constituer une alternative viable dans ces circonstances.

Fournissez à vos utilisateurs les informations dont ils ont besoin pour prendre de bonnes décisions

Dans le contexte actuel, les utilisateurs formeront plus que jamais votre première ligne de défense. Plus ils seront formés et équipés pour reconnaître et contrer les cybermenaces, plus votre sécurité sera renforcée.

Nos études sur la psychologie de l'ingénierie sociale suggèrent que votre objectif devrait être d'équiper et de sensibiliser les utilisateurs, plutôt que de les effrayer ou de les punir. Des exemples fréquents d'attaques et des rappels sur la façon de réagir seront plus utiles aujourd'hui que des politiques et des contrôles. La vigilance à l'égard des applications mobiles malveillantes et des sites de suivi du COVID-19 devrait également être soulignée ici. Le fait de fournir aux utilisateurs des sites fournis et prêts à l'emploi pour obtenir des informations et mener des discussions utiles concernant la crise actuelle réduira également leur désir d'en chercher ailleurs.

Fournir un accès à distance sécurisé

Proposer un accès à distance sûr et fiable à internet et aux systèmes de l'entreprise est manifestement le plus grand défi que doivent relever nos clients à l'heure actuelle. La meilleure solution à ce défi variera considérablement d'un client à l'autre, mais les principes suivants devraient servir de guide à la conception de toute architecture d'accès à distance :

1. Comprendre clairement votre modèle de menace. Nous affirmerons pour l'instant que le principal défi consiste à fournir une authentification et un contrôle d'accès appropriés aux données et aux systèmes de l'entreprise. Le cryptage entre le point de terminaison de l'utilisateur et internet, via son internet mobile ou son internet personnel, est sans doute moins préoccupant à l'heure actuelle.
2. Assurez-vous que vous sécurisez le DNS. Plusieurs attaques contemporaines consistent à rediriger les requêtes DNS afin de présenter des sites de phishing, de watering hole ou de mener des attaques de type « Person in the Middle ». Soyez attentif à la manière dont vous contrôlez les serveurs DNS que vos employés utilisent, que ce soit en utilisant des configurations VPN ou en leur faisant simplement installer des résolveurs DNS en dur sur leurs terminaux.

3. Mettre en œuvre une authentification à plusieurs facteurs (MFA). Nous estimons qu'à l'heure actuelle, pour la plupart des entreprises, l'authentification va devenir une priorité plus importante que la confidentialité. Contrôlez tous vos systèmes d'accès à distance (y compris les interfaces web, les VPN et les passerelles d'accès à distance) et réfléchissez à la manière dont une authentification forte pourrait être mise en œuvre. À ce stade, la forme du second facteur est moins importante que le fait de disposer d'un second facteur, de sorte que les systèmes basés sur les SMS et le courrier électronique sont également une option à envisager. Toutefois, si l'on a le choix, une solution complète de « push-to-mobile » - comme celle proposée par Okta, Duo, Google et Microsoft - sera la meilleure option en termes d'utilisation, de sécurité et peut-être même de facilité de déploiement.
4. Clarifier et communiquer les politiques relatives aux mots de passe intelligents. Nous soulignons à nouveau qu'actuellement, les attaques contre les technologies d'accès à distance en utilisant des mots de passe compromis constituent l'une des principales menaces. Si vous n'êtes pas en mesure de mettre en œuvre une solide authentification multi-facteurs (MFA), alors réfléchissez à ce que vous pouvez faire pour garantir que les utilisateurs choisissent des mots de passe solides. Plus précisément, les utilisateurs devraient être encouragés à
   - changer leur mot de passe (mais pas une nouvelle fois tant que la crise n'est pas terminée),
   - choisir un mot de passe qu'ils n'ont jamais utilisé ailleurs, et
   - choisir une phrase de passe longue mais facile à retenir, plutôt que courte et complexe.
5. Gérez vos dispositifs de sécurité. Comme indiqué précédemment, les campagnes actuelles comme APT41 ciblent activement des systèmes d'entreprise spécifiques comme les serveurs Citrix Application Delivery Controller (NetScaler ADC) et Citrix Gateway (NetScaler Gateway), le Zoho ManageEngine Desktop Central et les routeurs Cisco RV320 et RV325. Les serveurs VPN Pulse non patchés constituent une autre cible de choix. Ces attaques sont remarquables car elles exploitent des vulnérabilités connues et corrigées et utilisent même des outils de piratage gratuits ou commerciaux. En d'autres termes, elles sont réelles, mais ne sont pas difficiles à réparer. Assurez-vous que vous savez où se trouvent toutes vos technologies d'accès à distance via Internet, et que chacune d'entre elles est correctement patchée et configurée.

Organiser la visibilité sur un terminal distant

Avec des utilisateurs qui travaillent désormais à distance à grande échelle, les entreprises qui ne disposent pas de solides capacités de détection et de protection ou de réaction des endpoints peuvent se retrouver à piloter dans le brouillard dans l'œil d'une crise.

Bien qu'il ne faille pas se ruer sur la visibilité des endpoints, les entreprises qui ne disposent pas de telles capacités devraient envisager cette option dès maintenant.

Les deux voies logiques à suivre pour la plupart des configurations d'endpoints sont les suivantes :

1. Microsoft Sysmon : Microsoft System Monitor (Sysmon) est un service système et un pilote de périphérique Windows qui, une fois installé sur un système, reste résident lors des redémarrages du système pour surveiller et enregistrer l'activité du système dans le journal des événements Windows. Il fournit des informations détaillées sur les créations de processus, les connexions réseau et les modifications du temps de création des fichiers. En collectant les événements qu'il génère à l'aide des agents Windows Event Collection ou SIEM et en les analysant ensuite, vous pouvez identifier les activités malveillantes ou anormales et comprendre comment les intrus et les logiciels malveillants opèrent sur votre réseau. Sysmon est relativement sûr et facile à déployer, il prend en charge la plupart des versions contemporaines de Windows et il existe de nombreux projets commerciaux et open source qui offrent un support de configuration, de gestion, de collecte et de reporting. Voir la documentation MS pour démarrer.[18]
2. Solution EDPR commerciale : Plusieurs fournisseurs proposent des produits de détection, de protection et de réponse aux endpoints reconnus, notamment Cybereason, Cylance, Crowdstrike et d'autres encore. Nombre de ces solutions sont très fiables, ont fait leurs preuves et sont faciles à déployer et à gérer. Certaines offrent également différentes fonctions « d'isolation » qui permettent de mettre partiellement hors ligne un endpoint tout en effectuant un tri des incidents et des analyses cyber-légales.

En dehors de ces solutions simples, d'autres options existent pour parvenir aux mêmes objectifs. Les agents VPN peuvent, par exemple, être utilisés pour mettre en place une isolation virtuelle du réseau, tandis que les produits open source comme le Remote Response (GRR) de Google offrent des options de triage à distance et d'expertise cyber-légale qui fonctionnent.

Prendre en compte les applications mobiles malveillantes

Comme le souligne un document publié par le US National Institute of Standards and Technology, référencé plus bas : « Les appareils mobiles sont conçus pour faciliter la recherche, l'acquisition, l'installation et l'utilisation d'applications tierces à partir de magasins d'applications pour appareils mobiles. Cela pose des risques de sécurité évidents, en particulier pour les plateformes d'appareils mobiles et les magasins d'applications qui n'imposent pas de restrictions de sécurité ou d'autres limitations à la publication d'applications tierces. Les organisations doivent planifier la sécurité de leurs appareils mobiles en partant du principe qu'on ne peut faire confiance aux applications mobiles tierces inconnues téléchargeables par les utilisateurs.

Comme nous l'avons déjà mentionné, nous avons observé une multiplication par cinq du nombre d'applications mobiles malveillantes détectées entre les mois de février et mars cette année. Nous pouvons nous attendre à ce que cette tendance se poursuive à mesure que la crise s'étend.

Les options liées aux applications malveillantes dont disposent les entreprises sont notamment les suivantes :

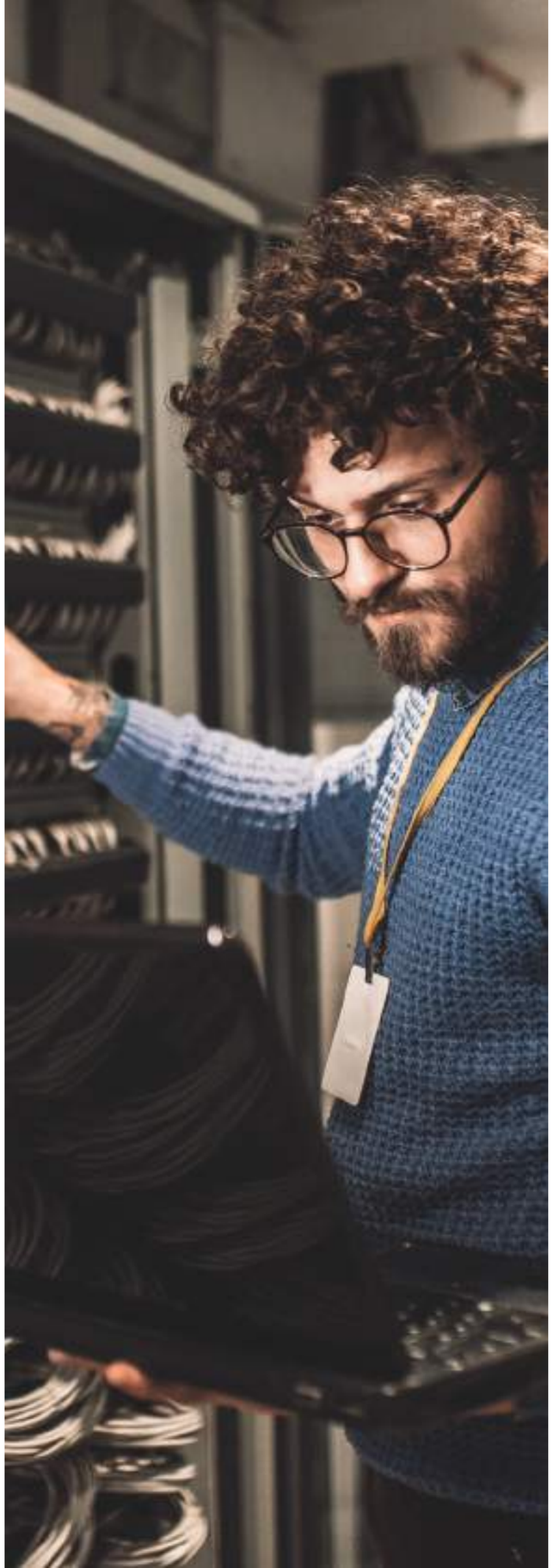
- Interdir toute installation d'applications tierces.
- Mettre en place une liste blanche pour autoriser l'installation des seules applications approuvées.
- Vérifier que les applications ne reçoivent que les autorisations nécessaires sur l'appareil mobile.
- Mettre en place un sandbox/conteneur sécurisé qui isole les données et les applications de l'entreprise de toutes les autres données et applications disponibles sur l'appareil mobile.

Pour la plupart des entreprises, la seule solution technique pratique consiste à fournir à leurs utilisateurs une solution antivirus mobile ou à équiper les appareils mobiles de l'entreprise d'un logiciel de gestion des données de référence (GDR ou MDM pour master data management en anglais).

« La GDR fait généralement référence au déploiement d'une combinaison d'applications et de configurations, de politiques et de certificats d'entreprise, et d'une infrastructure backend sur les appareils mobiles, dans le but de simplifier et d'améliorer la gestion informatique des appareils des utilisateurs finaux ».[19]

Pour les entreprises qui n'ont pas encore mis en place une forme de GDR, les options à envisager pendant la crise comprennent l'expédition d'appareils mobiles dédiés aux utilisateurs pour une utilisation sur les systèmes de travail, la proposition aux utilisateurs de solutions antivirus mobiles à télécharger sur leurs propres téléphones portables, ou simplement la sensibilisation des utilisateurs aux risques particuliers qui affectent les appareils mobiles en ligne.

Le document complet du NIST et les conseils associés sont disponibles en ligne. [20]



Envisager de raccorder et de renforcer les terminaux distants, y compris les terminaux mobiles

Le 25 mars, nous avons publié un avis de sécurité concernant deux failles critiques de type « zero-day » dans les systèmes Windows. Ces vulnérabilités sont présentes dans toutes les versions de Windows prises en charge et pourraient conduire à l'exécution de code à distance si elles sont exploitées avec succès. Microsoft a prévenu que des attaques limitées et ciblées avaient été détectées. [21]

Avant cela, le 11 mars, nous avons mis en garde nos clients contre une vulnérabilité d'exécution de code à distance dans le protocole Microsoft Server Message Block 3.1.1 (SMBv3) qui donnerait à un attaquant la possibilité d'exécuter du code sur le serveur SBM ou le client SBM cible.[22]

Ce type de vulnérabilités sur les serveurs et ordinateurs Windows ne cessent d'apparaître et sont activement exploitées. Le même défi existe pour les appareils mobiles, tant personnels que privés. Bien que nous ne pensions pas qu'ils représentent le vecteur d'attaque le plus probable à l'heure actuelle, les endpoints distants ne peuvent pas être ignorés et le fait de ne pas y remédier pourrait exposer votre entreprise à des risques inutiles.

Une fois que les autres priorités dont nous avons parlé dans cette section auront été abordées, il faudra s'efforcer d'analyser comment les endpoints des utilisateurs distants pourraient être patchés. Une option viable (en lieu et place d'une solution centrale de patching) pourrait consister à simplement informer les utilisateurs des correctifs essentiels via les communications de l'entreprise et à leur demander d'appliquer le correctif directement.

Les mouvements latéraux à partir d'enpoints compromis étant sans doute moins probables avec des travailleurs à distance, la pression exercée sur nous pour tout réparer est un peu moins forte. Les patchs spécifiques qui rendent les terminaux des utilisateurs moins exploitables constituent en ce moment la principale préoccupation, et chaque machine qui est patchée réduit la surface d'attaque et donc le risque. C'est loin d'être une réponse parfaite au problème, mais comme nous l'avons suggéré précédemment : à ce stade, chaque victoire compte.

Revoir votre police d'assurance

La cyberassurance est un sujet complexe dans son principe et il est presque certain qu'il vaut mieux laisser parler les experts sur ce sujet.
Toutefois, étant donné que le modèle de la cybermenace a presque certainement déjà muté à l'heure actuelle, nous recommandons aux entreprises de faire un effort pour revoir et reconsidérer la pertinence de leurs polices d'assurance cybernétique.

La cyber-assurance doit être considérée comme la dernière ligne de défense dans toute stratégie de sécurité, et ne peut certainement pas être considérée comme un substitut aux autres actions décrites dans ce document. Toutefois, à l'heure actuelle, une assurance décente peut faire la différence dans le cadre de la survie d'une entreprise.

Bien qu'il soit préférable de laisser ce domaine aux experts, nos observations sur le secteur de la cyberassurance nous incitent à encourager les clients à tenir compte de deux facteurs quelque peu inhabituels :

1. Étant donné que les attaques et les compromissions actuels sont souvent perpétrés par des attaquants dits « parrainés par l'État », assurez-vous que votre assurance ne contient pas de clauses déraisonnables d'« acte de guerre » qui auraient un impact sur les remboursements s'il était prouvé que l'acteur malveillant était affilié à un gouvernement.
2. Les paiements de rançon constituent un élément clé des cyber-assurances modernes. Il est donc important d'examiner attentivement cette clause, à la fois pour vous assurer que vous êtes correctement couvert en cas de besoin, mais aussi pour vous assurer que votre politique morale et éthique en matière de paiement de rançon est alignée sur celle de l'assureur. Vous ne voulez certainement pas que l'assureur fasse pression sur vous pour que vous payiez une rançon comme moyen le moins cher de sortir d'un compromis, alors que dans les faits, votre entreprise a une aversion morale

Une leçon à tirer

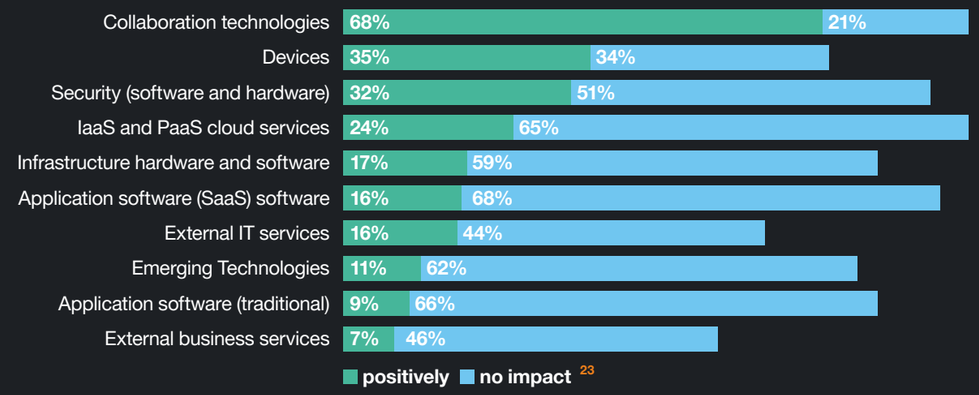
Enfin, nous pensons que l'impact de cette pandémie et notre réponse collective sont riches d'enseignements pour les praticiens de la sécurité ; le virus montre à quel point nos sociétés et nos économies sont étroitement liées et à quel point une catastrophe dans une région se répercute de manière spectaculaire dans une autre. En réagissant à la crise, nous apprenons à apprécier l'impact de notre comportement sur l'ensemble de la société, et pas seulement sur nous en tant qu'individus, familles et entreprises. C'est une leçon essentielle pour la communauté de la sécurité également.

Lorsque nous réfléchissons à quand, où et combien investir dans la sécurité, nous devons penser au-delà du risque unidimensionnel que nous traitons pour notre entreprise et considérer l'impact des effets secondaires et tertiaires sur l'économie au sens large lorsque des violations et des compromissions se manifestent. Nous devons reconnaître que ce qui est mauvais pour la société en général, l'est aussi pour nous en tant qu'entreprises.

Ce que l'avenir nous réserve

Vous trouverez ici nos prévisions quant aux manières dont les exigences en matière de cybersécurité changeront lorsque le pire de la pandémie sera derrière nous :

1. Nous nous attendons à ce que des pressions soient exercées pour revoir et améliorer ou créer des plans d'essais de BCP (best current practice) et de DR et d'intégrer la « réponse aux maladies contagieuses » dans la planification de l'entreprise. Nous nous attendons à une augmentation de la demande de conseil et de soutien en raison de l'intérêt pour ce type de politiques et d'exercices.
2. Nous nous attendons à une prise de conscience de la possibilité que la taille des bureaux puisse être réduite et du fait que le phénomène de « hot desking » (bureau nomade) n'est pas aussi négatif qu'on le pensait.
3. Nous prévoyons une augmentation de la demande de solutions de vidéoconférence « plus complètes » et d'applications facilitant le travail à distance, voire à une percée des applications de réalité virtuelle.
4. Nous nous attendons à ce que la demande de modèles « zero trust » et de technologies similaires sans VPN augmente.
5. À l'inverse, nous prévoyons que la demande de services de bureau à distance (VDI) et de front end Citrix augmente également, ou du moins la demande pour une solution de bureau à distance par navigateur web dans le cloud.
6. Nous prévoyons une accélération de la demande de technologies protégeant le nouveau périmètre (zero-trust, data centric, IdO, etc.)
7. Les services en ligne (banque, paiements, commerce électronique, formation, divertissement) vont continuer à se multiplier et nous prévoyons donc une augmentation de la consommation et du développement de plateformes technologiques de sécurité des applications pour sécuriser les logiciels en ligne. Cela comprend :
   - un équilibrage des charges
   - une protection DoS
   - des outils de sécurité des applications (SAST/DAST)
   - un WAF (Web Application Firewall)
   - une sécurité de l'API
8. Nous prévoyons de l'innovation et anticipons l'émergence de produits et de plateformes additionnels en matière de réponse aux incidents et des BCP, tels que des simulateurs, et l'évaluation et la mesure des BCP existantes.
9. Nous anticipons une perception accrue du risque lié aux appareils (ordinateurs portables) qui ne sont pas connectés au réseau mère pour des périodes plus longues (patching, AV, configuration sécurisée, etc.) et, par conséquent, une demande d'outils permettant de mettre en quarantaine les appareils non conformes lors de leur retour sur le réseau.
10. Nous nous attendons à un risque accru du fait que le personnel ait un accès plus détendu à Internet, par exemple O365 etc. qui ne nécessite pas d'accès au réseau mère, que les fonctions de rendu comme le filtrage des URL, les pare-feu et les IDS/IPS soient abandonnés pendant un certain temps. De nouvelles fonctionnalités et une nouvelle architecture de pare-feu Next Generation seront nécessaires.
11. Nous nous attendons à ce que les attitudes morales, juridiques et répressives concernant le piratage informatique des établissements de santé se durcissent considérablement, peut-être même avec des accusations aussi graves que l'homicide involontaire ou volontaire portées contre des pirates informatiques dont les activités ont perturbé les services médicaux pendant cette période. Cela pourrait avoir des conséquences considérables sur la capacité des forces de l'ordre à lutter contre la cybercriminalité, même après la fin de la crise.
12. Les budgets consacrés aux technologies de l'information et à la sécurité vont certainement être modifiés du fait de la crise. On ne sait pas encore si ce sera pour le « mieux » ou pour le « pire », mais nous prévoyons que l'on se concentrera davantage sur/et que l'on exigera un retour sur investissement clair et mesurable des dépenses en matière de cybersécurité



[23]

Quand tout sera terminé

Nous vivons dans l'espoir et nous croyons que cette période terrible prendra rapidement fin et que la vie reviendra à la « normale », quelle que soit la « normale ». Pour beaucoup, cela impliquera, espérons-le, un retour à une vie professionnelle normale, au bureau.

Nous ne savons pas à quel moment cela arrivera et nous devrions nous préparer à ce que la réalité actuelle s'étende encore sur des semaines, voire des mois. Mais les travailleurs finiront par retourner au bureau et il nous incombe, avant que cela n'arrive, de réfléchir à la manière de gérer cette journée d'un point de vue sécuritaire.

Nous devrions nous attendre à trouver au moins certains des éléments suivants, lorsque les travailleurs retourneront au bureau

1. Il se peut qu'il y ait des cobwebs sur vos systèmes. Après des semaines de stagnation et de négligence, vous devez vous attendre à trouver des éléments de votre système rouillés ou en mauvais état. En outre, les données mises en cache, telles que les journaux des terminaux, les sauvegardes ou les mises à jour rétroactives, peuvent être repoussées d'un seul coup lorsque les utilisateurs se connectent à nouveau, ce qui entraîne une pression supplémentaire sur votre infrastructure. Prévoyez d'organiser la reprise du travail de bureau de manière à ce que ces problèmes puissent être identifiés et résolus sans causer trop de perturbations.
2. De nombreuses données seront stockées localement et ne seront pas encore enregistrées dans des référentiels d'entreprise sécurisés. Faites de la sécurité et de la fiabilité des emplacements une priorité pour que les utilisateurs puissent y déposer leurs données afin de réduire le plus rapidement possible votre dépendance à l'égard des endpoints.
3. À moins que vous n'ayez pu relever certains des défis fondamentaux de la protection, de la détection et de la gestion des vulnérabilités des endpoints pendant cette période, vous devez vous attendre à ce que certains terminaux mobiles d'entreprise reviennent au bureau dans un état de compromission. Ce n'est pas un problème entièrement nouveau, mais c'est un défi auquel nous sommes rarement confrontés à une telle échelle. Il n'existe pas de solution simple et unique pour faire face à ce risque, mais il faut réfléchir à la manière dont les endpoints compromis sont traités au fur et à mesure qu'ils reviennent sur le réseau de l'entreprise.
4. Comme nous l'avons précédemment suggéré, un programme de retour échelonné permettrait aux opérateurs informatiques et de sécurité de relever le défi petit à petit. Diverses technologies de sécurité des endpoints (comme le contrôle d'accès au réseau - NAC) permettront d'isoler les endpoints et de vérifier leur conformité avant qu'ils ne soient entièrement connectés au réseau. Si c'est envisageable, l'opportunité de restaurer les endpoints à partir d'un build standard sécurisé et actualisé mérite d'être prise en considération.

L'une des nombreuses caractéristiques spécifiques au COVID-19 réside dans son impact mondial. Habituellement, les entreprises anticipent des pannes localisées ou régionales, et non pas globales, qui ne touchent pas seulement eux-mêmes et leurs employés, mais qui s'étendent aussi à leurs chaînes d'approvisionnement à travers la planète. Sachant que la réponse de chaque entreprise sera également unique, voici quelques éléments clés à prendre en compte.

Évaluation de la situation

- Effectuez une évaluation de la situation dans toute l'organisation, en déterminant quels points de l'entreprise ont été les plus touchés. A titre d'exemple, les ordinateurs portables ont-ils été autorisés à sortir des programmes de patchs acceptables ? Les nouveaux équipements ont-ils été distribué pour faire face à la situation, sans protection adéquate ?
- Donner la priorité aux missions de l'entreprise et retrouvez prudemment votre activité habituelle.
- Documentez autant que possible et demandez aux autres équipes de faire de même.
- Procédez à une évaluation des risques.

Notification et communication

- Évaluez la technologie et les fonctions de sécurité et exécutez les changements de retour au BAU sur les systèmes concernés.
- Identifiez toute modification implicite ou explicite survenu » dans la politique et déterminez s'il faut revenir à l'original ou validez les changements. Évaluez votre chaîne d'approvisionnement, y compris les tierces parties, et informez-les de tout changement dans les mesures de sécurité. Le cas échéant, notifiez les autorités gouvernementales.
- Travaillez avec l'équipe de gestion de crise ou, s'il n'y en a pas, avec vos services relations publiques, marketing et juridiques pour informer les clients de tout changement lié à la sécurité (comme les procédures de notification de fraude et de sécurité, la prime aux bugs, etc.).

Contrôle des changements

- Lancez la procédure de contrôle des changements pour chacun des systèmes concernés (utilisateur final, systèmes d'entreprise, connectivité, téléphonie, etc.)
- Organisez une session sur les lesson learns et mettez à jour le plan et les scénarios des BCP en conséquence.

Mesures techniques de sécurité

- Sécurité des appareils de l'utilisateur final - examiner les correctifs et la configuration sécurisée avant de se connecter au réseau (zone de quarantaine, évaluation des compromissions et déploiement de l'IPS hôte)
- Effectuer un examen des règles du pare-feu et un examen des accès pour vérifier les modifications et supprimer les règles/autorisations d'accès inutiles. Evaluation de la Sécurité physique pour revoir les contrôles d'accès physiques

Partie III:

Analyse: ce que nous avons observé jusqu'à présent

Dans cette section, nous présentons un résumé des activités et des développements significatifs que nos différentes équipes de renseignement ont observé depuis le début de la crise.

Au 25 mars, au moins 20 % de la population mondiale était placée en quarantaine en raison du coronavirus.[24] Pour les entreprises qui ne sont pas encore préparées à un paradigme de travail à distance à grande échelle, cela a généré une ruée désespérée vers la mise en place des systèmes et processus nécessaires pour s'adapter à une nouvelle réalité brutale.

En tant que fournisseur bien établi de services de sécurité gérés et d'assistance, Orange Cyberdefense a pu observer directement cette escalade de la demande. Au sein de nos opérations au Royaume-Uni, par exemple, l'équipe des Services professionnels traite en temps normal un engagement Pulse Secure VPN par mois en moyenne. Au 23 mars 2020, elle avait répondu à six demandes déjà.

Le centre des opérations de sécurité britannique a connu une escalade similaire de la demande. Au cours des trois premières semaines de mars seulement, nous avons observé une augmentation de 50 % des demandes de service liées aux produits VPN par rapport à février. Il y a eu des augmentations similaires entre janvier et février.

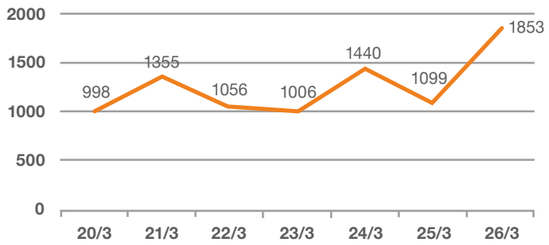
Quiconque a la chance aujourd'hui d'avoir encore un emploi (qui n'implique pas d'être sur place et directement exposé au virus) pourra témoigner du changement radical de la réalité de l'organisation mondiale du travail. Le travail à domicile s'impose au monde entier, et il pourrait s'imposer pour toujours.

L'appât idéal

Alors que la pandémie COVID-19 se propage au monde entier, les campagnes de phishing et de logiciels malveillants se sont également multipliées, cherchant à instrumentaliser les craintes et la soif d'information des individus.

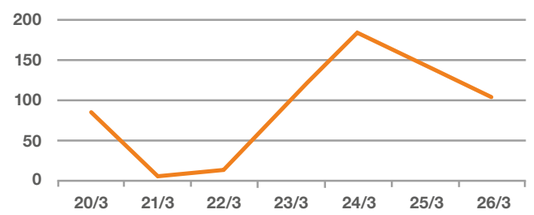
Il a été détecté que ces campagnes utilisaient des cartes en ligne légitimes suivant la propagation du virus afin de tenter de distribuer des malwares qui dérobent des informations, ainsi que des sujets et des pièces jointes ciblés comme leurres dans des courriels de phishing.

Domaines enregistrés liés au COVID-19



Selon les statistiques publiées par notre équipe du CERT le 26 mars, environ 8 900 nouveaux domaines DNS liés aux termes « coronavirus », « covid-19 » et « ncov » ont été enregistrés au cours de la semaine dernière, soit plus du double par rapport à la semaine précédente.

Nombre de courriels potentiellement frauduleux transmis par les clients du CERT



En 24 heures, rien que pour la journée du 24 mars, notre équipe du CERT en France a enregistré 23 courriers de phishing uniques basés sur le COVID-19. Notre équipe CERT a également rapporté, qu'au cours de la même semaine, les clients ont signalé plus de 600 courriels potentiellement frauduleux, dont 10 % se sont révélés malveillants. Le nombre de courriels confirmés comme étant malveillants a été 4 fois plus élevé que la semaine précédente.

Plusieurs exemples illustrent ce type de « prétexte » du RAT-COVID-19. Nous avons observé certains botnets et voleurs tels que Hancitor, NetWire, Formbook, Loda, JRat, Danabot et d'autres encore adopter le même type de comportement.

Coronavirus data map watering hole

La « Live coronavirus Data Map » du John Hopkins Center for Systems Science and Engineering (CSSE) a été utilisée comme leurre pour répandre des logiciels malveillants.[25]

Le tableau de bord interactif est utilisé par des sites web malveillants (et éventuellement des courriels de spam) pour diffuser des logiciels malveillants dérobant les mots de passe. Selon Krebsonsecurity.com[26], un membre de « plusieurs forums de cybercriminalité russophones a commencé à vendre un kit d'infection du coronavirus numérique qui utilise la carte interactive de Hopkins dans le cadre d'un plan de déploiement de logiciels malveillants basés sur Java. Le kit coûte 200 dollars si l'acheteur a déjà un certificat de signature de code Java, et 700 si l'acheteur souhaite plus simplement utiliser le certificat du vendeur ».

Notre laboratoire épidémiologique a estimé que le watering hole avait été utilisé pour distribuer une souche de malware Danabot. DanaBot est un cheval de Troie bancaire modulaire développé à Delphi et conçu pour voler les références bancaires et les informations sensibles en collectant les données des formulaires, en faisant des captures d'écran ou en enregistrant les frappes sur les ordinateurs compromis. Une récente variante de DanaBot détectée par Check Point ajoute un module « non ransomware » à sa liste précédente de capacités qui lui permet de voler les identifiants des navigateurs et des clients FTP, de collecter les identifiants des portefeuilles cryptés. Lancer un proxy sur une machine infectée, prendre des captures d'écran et enregistrer des vidéos, fournit un contrôle à distance via RDP ou VNC et bien plus encore.[27]

Les logiciels malveillants s'adaptent

L'écosystème de la cybercriminalité a toujours été remarquablement agile et capable de s'adapter aux changements du paysage. Les pirates informatiques et les escrocs sont très attentifs à la dynamique de la pandémie et ont réagi rapidement pour en tirer parti de diverses façons, certaines intelligentes et d'autres presque naïvement opportunistes. Ces réponses vont des applications de suivi COVID-19 intelligentes mais factices et des watering holes attack, au rebranding presque enfantin des produits existants sur des thèmes liés au COVID-19 .

Applications malveillantes

Selon l'unité OSINT, une division de notre Laboratoire d'épidémiologie, des informations provenant de sources externes certifiées indiquent que, dès le début de la crise, des liens web ont été envoyés à certains téléphones Android, promettant des applications pour traquer les coronavirus.[28] Il s'agissait en réalité d'un leurre. Une fois l'application téléchargée, les individus, soupçonnés d'opérer depuis la Libye, peuvent voir à travers la caméra du smartphone, avoir accès aux messages textuels ou écouter via le microphone. Le logiciel malveillant identifié serait une version personnalisée de SpyMax, un logiciel espion commercial qui peut être très facilement obtenu gratuitement en ligne.

Les chercheurs de Bitdefender ont également récemment analysé la télémétrie liée aux applications légitimes et aux logiciels malveillants basés sur le thème du coronavirus et ont observés d'énormes pics dans les analyses d'applications contenant « covid » ou « corona » dans le nom du package ou le chemin de fichier. [29]

On Le 26 mars, notre propre équipe du CERT a signalé que les campagnes de propagation de logiciels malveillants étaient de plus en plus nombreuses. Entre février et mars 2020, le nombre total de campagnes de diffusion de logiciels malveillants liées au COVID-19 a été multiplié par 5. À la date de rédaction du présent document, notre équipe du CERT suit 39 familles de logiciels malveillants distribués par des courriels liés au COVID-19. Ces tentatives sont susceptibles de persister et de s'intensifier au fur et à mesure que la pandémie progresse, ce qui reflète le mode opératoire habituel des acteurs de la menace qui consiste à instrumentaliser les événements de dimension mondiale pour tenter d'en tirer profit.

L'informatique domestique attaquée

Comme il fallait s'y attendre, les pirates ont commencé à cibler les systèmes informatiques domestiques, et plus particulièrement les routeurs domestiques vulnérables. Dans un article du 26 mars, ZDNet rapporte que « depuis près d'une semaine, un groupe de pirates s'est introduit dans les routeurs domestiques et en ont modifié les paramètres DNS afin de diriger les utilisateurs d'appareils peu méfiants vers des sites liés au coronavirus qui propagent des logiciels malveillants ».[30]

Ce type d'attaque, dont Orange Cyberdefense a déjà fait état, consiste à compromettre un routeur domestique puis à rediriger les requêtes DNS des utilisateurs domestiques vers des sites web malveillants sur le thème du COVID-19 utilisés pour le phishing ou pour télécharger des applications malveillantes. Selon Bitdefender, les pirates utilisent des attaques par force brute pour deviner le mot de passe administrateur des routeurs ciblés.

Une fois qu'ils ont deviné un mot de passe et se sont introduits, les pirates modifient les paramètres par défaut du serveur DNS du routeur, en pointant l'appareil vers leurs propres serveurs. Cela signifie que chaque requête DNS faite par les utilisateurs connectés à un routeur piraté passe par les serveurs DNS des pirates, donnant aux attaquants le contrôle total des sites auxquels un utilisateur accède ».[31]


NEWS

Home UK World Business Politics Tech Science Health Family & Education

Technology

Coronavirus: How hackers are preying on fears of Covid-19

By Joe Tidy
Cyber-security reporter

12 March 2020

Coronavirus pandemic

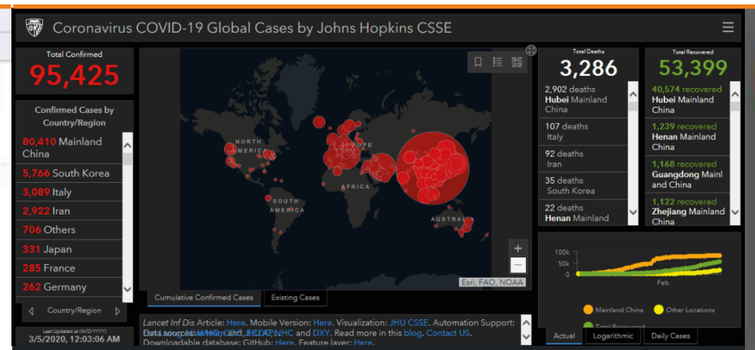

Subject: [W.H.O] COVID-19 VACCINE NOW AVAILABLE

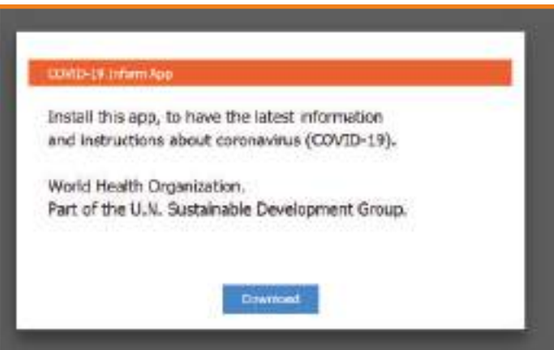
Message COVID-19 VACCINE.Xtz.iso

From: WORLD HEALTH ORGANIZATION (WHO) [mailto:healthcaresupport@who.int]
Sent: Thursday, March 26, 2020 3:05 PM
Subject: [W.H.O] COVID-19 VACCINE NOW AVAILABLE

World Health Organization

part(1):
AVALABLE COVID-19 VACCINE .doc 35 KB





Maze Team official press release. March 18 2020

Due to situation with incoming global economy crisis and virus pandemic, our Team decided to help commercial organizations as much as possible. We are starting exclusive discounts season for everyone who have faced our product. Discounts are offered for both decrypting files and deleting of the leaked data. To get the discounts our partners should contact us using the chat or our news resource.

In case of agreement all the info will be deleted and decryptors will be provided.

The offer applies to both new partners and the «archived» ones. We are always open for cooperation and communication.

We also stop all activity versus all kinds of medical organizations until the stabilization of the situation with virus

Cesser le feu ?

Sur une note plus positive, plusieurs des principaux groupes de diffusion de ransomwares ont annoncé ne jamais cibler les établissements médicaux et de recherche ou qu'ils ne les cibleraient plus tant que la pandémie sera en cours. Certains proposent même le décryptage ou la récupération des données à un tarif réduit si une telle organisation est accidentellement ciblée.

Le « communiqué de presse » ci-dessus a été publié par MAZE le 18 mars 2020. Le monde a ensuite appris le 24 mars que HMR Ltd - Hammersmith Medicines Research - avait été piraté par MAZE. Nos chercheurs en cybercriminalité ont cependant déterminé que la faille de HMR remonte en réalité au 14 mars, ce qui suggère que MAZE a effectivement tenu sa parole jusqu'à présent.

Le 26 mars, notre équipe du CERT a signalé que, contrairement à ce qui avait été annoncé par plusieurs groupes cybercriminels, certains d'entre eux, comme le groupe à l'origine du ransomware Ryuk, continuaient de cibler les établissements de santé. Les attaques de type DDOS contre ces établissements se multiplient, comme on l'a observé le 22 mars avec l'attaque visant l'Assistance Publique - Hôpitaux de Paris (AP-HP).

Enfin, il convient de noter que l'opérateur de rançon Doppelpaymer a déclaré que, bien qu'il ne ciblerait pas les hôpitaux dans le contexte de pandémie COVID-19, il n'aura pas de pitié pour les entreprises pharmaceutiques qui ne sont intéressées que par le profit. Tout cessez-le-feu dont nous pourrions bénéficier ne sera certainement pas universel.

Si les promesses de cessez-le-feu faites par les principaux groupes de menace constituent un répit bienvenu, on ne peut pas s'attendre à ce que leur impact soit substantiel. Les menaces « traditionnelles » comme les logiciels de rançon persistent.

Fake news !

Dans le domaine public, nous observons un niveau important de désinformation sur l'origine du virus, sa propagation, la mortalité et les remèdes possibles. Il y a de fortes raisons de penser qu'en Chine et aux États-Unis, des opérateurs soutenus par l'État mènent des campagnes de désinformation afin d'articuler le discours autour du virus et des efforts de lutte.

Nous avons également observé un certain niveau de mésinformation/désinformation concernant les offres technologiques qui sont devenues importantes au moment de la rédaction du présent rapport. Notamment, le logiciel de vidéoconférence Zoom et les réseaux sociaux ont fait l'objet de critiques importantes concernant des questions de sécurité ou de vie privée qui semblent non fondées ou du moins exagérées.[32]

La criminalité profite de la crise

Selon un article disponible sur Vice, « les pirates informatiques ont pris le contrôle d'une vague de comptes Twitter pour faire de la publicité agressive pour un site web qui prétendait vendre des masques et du papier toilette pendant la pandémie de coronavirus ».[33] De nombreux autres cas similaires sont observés, où des criminels (cyber ou autres) exploitent les préoccupations liées à la crise pour mener diverses escroqueries et arnaques

L'escalade géopolitique

La crise du COVID-19 est d'une ampleur sans précédent et il est juste de dire que le monde entier est en guerre. Si ces crises ont l'effet remarquable de rassembler les gens, elles peuvent aussi, malheureusement, exacerber et aggraver les conflits pour les ressources ainsi que les tensions idéologiques.

Depuis le début de la crise, nous observons des attaques malveillantes qui visent vraisemblablement des installations médicales. Reuters a, par exemple, rapporté le 16 mars que « le département américain de la santé et des services sociaux a subi une cyber-attaque sur son système informatique, dans le cadre de ce que les personnes familières à l'incident ont appelé une campagne de perturbation et de désinformation visant à saper la réponse à la pandémie de coronavirus et qui pourrait avoir été le fait d'un acteur étranger ».[34]

D'autres attaques ont manifestement tenté de cibler ce type d'installations, en particulier dans le monde occidental, afin d'essayer de perturber ou de saper la recherche sur le COVID-19 et l'élaboration d'un traitement.

Dans un autre exemple, les systèmes informatiques de l'hôpital universitaire de Brno, en République tchèque, ont été arrêtés le 13 mars en raison d'une cyber-attaque. Cet hôpital est le deuxième plus grand du pays et abrite l'un des 18 laboratoires tchèques mobilisés pour tester le virus. Selon Bleeping Computer, « les systèmes qui servent les laboratoires comme l'hématologie, la microbiologie, la biochimie, le diagnostic des tumeurs ou la radiologie semblent être sur un réseau différent que les systèmes infectés puisqu'ils continuent de fonctionner ». L'attaque a néanmoins été jugée suffisamment grave pour que les systèmes informatiques soient éteints et que les patients gravement malades soient transférés dans un autre établissement.

Les soins de santé en ligne de mire

Le laboratoire d'épidémiologie des logiciels malveillants d'Orange Cyberdefense surveille les attaques visant spécifiquement les prestataires de soins de santé. L'équipe met en garde contre le fait qu'à court terme, l'interruption de la continuité des activités commerciales peut entraîner des risques pour la santé des patients. [35]

Les entreprises pharmaceutiques sont une cible de choix pour les pirates informatiques, que ce soit en raison de la propriété intellectuelle ou des données sensibles qu'elles détiennent. Plusieurs entreprises pharmaceutiques ont été touchées par des cyber-attaques au cours des dernières années. Certaines sont des victimes collatérales, d'autres sont infectées à des fins d'espionnage ou de rançon. Quels que soient le motif et la méthode, les conséquences peuvent être désastreuses.

Parmi les groupes de hackers qui ciblent l'industrie pharmaceutique, les acteurs soutenus par des Etats apparaissent particulièrement actifs et dangereux. Plusieurs semblent avoir des liens avec des gouvernements et APT 41 - un opérateur présumé soutenu par l'État chinois - apparaît particulièrement dangereux à l'heure actuelle.

L'intérêt récent des pirates informatiques pour l'industrie biopharmaceutique est également à souligner. Il est rapporté que les entreprises biopharmaceutiques sont parmi les cibles préférées des groupes de pirates informatiques, que ces derniers soient ou non financés par un État, à qui ils dérobent des secrets commerciaux.

L'Iran semble également viser le secteur de la santé. Le 30 mars, le Bureau fédéral américain d'investigation (FBI) a publié une notification de l'industrie privée mettant en garde contre une campagne de logiciels malveillants baptisée Kwampirs, vaguement liée à des pirates informatiques soutenus par l'État iranien, qui vise spécifiquement le secteur de la santé et a la capacité de se déplacer latéralement dans la chaîne d'approvisionnement. Selon le rapport, « le Kwampirs RAT est un ver modulaire RAT qui permet d'accéder aux machines et aux réseaux victimes, avec l'objectif premier d'obtenir un accès large, mais ciblé, aux entreprises victimes pour autoriser des activités d'exploitation de réseaux informatiques (CNE).

Grâce à la victimologie et à la criminalistique, le FBI a découvert que les secteurs fortement ciblés sont les soins de santé, la chaîne d'approvisionnement en logiciels, l'énergie et l'ingénierie aux États-Unis, en Europe, en Asie et au Moyen-Orient ».[36]

L'exemple du FBI ci-dessus illustre également le risque que représente la compromission de la chaîne d'approvisionnement, que nous traitons ailleurs dans ce document.

Internet sous tension

Alors que les détaillants et les prestataires de services se précipitent pour proposer leurs produits et services en ligne, certains se heurtent à des niveaux de trafic et de demande sans précédent. Tout comme le « zoom », les « files d'attente virtuelles » sont devenues partie intégrante de notre langage contemporain presque du jour au lendemain.

Bien que nous n'ayons pas observé de nombreux cas d'échec à grande échelle, nous considérons qu'il est prudent de prévoir que la demande de commerce et autres services en ligne va s'accroître pendant et après la crise.[37]

Préoccupations concernant la vidéoconférence

Nous avons observé un certain nombre d'inquiétudes liées aux politiques et pratiques de confidentialité des plateformes de vidéoconférence comme Zoom qui, aidé par la crise du coronavirus, semble être devenu le leader incontesté du secteur.

Certaines de ces préoccupations sont légitimes. En particulier, vis-à-vis de l'attaque appelée « zoombombing », grâce à laquelle les trolls passent d'un identifiant Zoom à un autre jusqu'à ce qu'ils en trouvent un qui soit actif et se joignent à l'appel sans y être invités.[38]

Ce ne serait pas la première fois que des problèmes de sécurité importants sont signalés avec Zoom (ou tout autre logiciel de vidéo ou de webconférence).

La fondation de défense des droits numérique, Electronic Freedom Foundation (EFF), résume ses réflexions sur sa page d'accueil.[39]

Zoom, pour sa part, « prend bien sûr très au sérieux la vie privée de ses utilisateurs » et a en effet répondu à un rapport de la carte mère en modifiant certains comportements de l'application.[40]

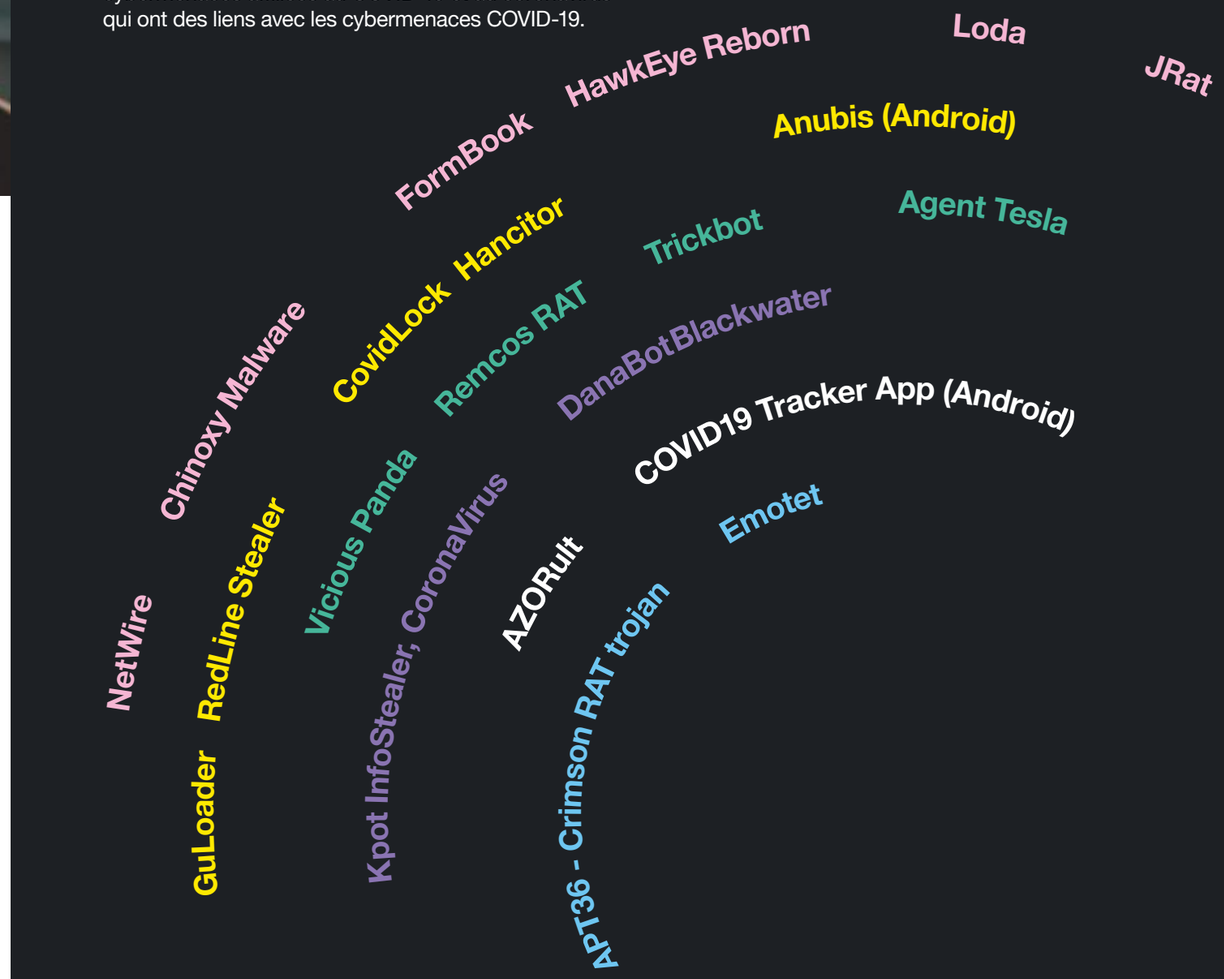
Comme il fallait s'y attendre, le nouvel intérêt considérable pour Zoom est également observé et exploité par des attaquants qui profitent de l'afflux de nouveaux utilisateurs inexpérimentés sur la plate-forme. Le 31 mars, par exemple, notre laboratoire d'épidémiologie a fait état de pirates utilisant des installateurs malveillants du logiciel Zoom pour propager le malware Neshta et d'autres applications potentiellement indésirables. L'équipe a également répertorié 197 nouveaux domaines DNS liés à Zoom dans un avis publié ce jour-là, bien qu'ils ne soient pas nécessairement tous malveillants.

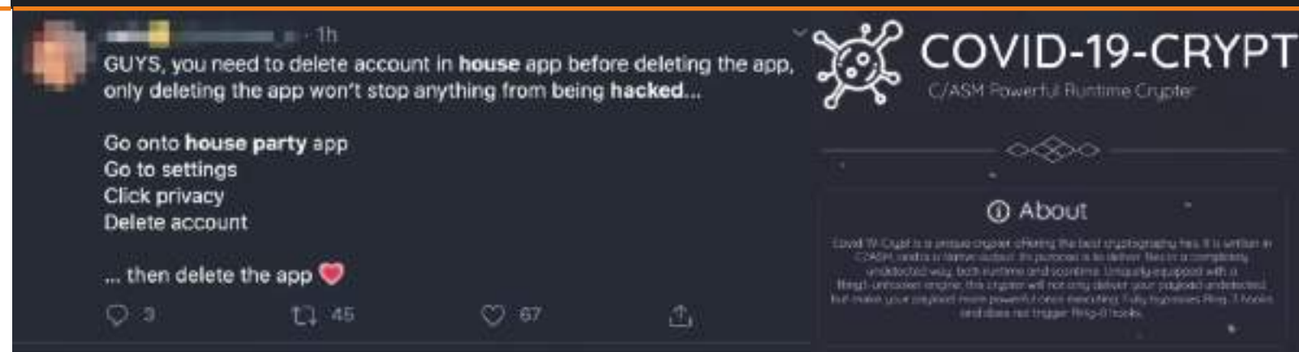
Orange Cyberdefense

Laboratoire épidémiologique

Cybermenaces liées au COVID-19/coronavirus (source OSINT)

Ce graphique résume les observations actuelles de nos équipes d'épidémiologie des logiciels malveillants des cybermenaces affiliées au COVID-19 et au coronavirus qui ont des liens avec les cybermenaces COVID-19.





Contributeurs et ressources

Contributeurs

Nous reconnaissons et apprécions les précieuses contributions des experts suivants, issus de l'ensemble du groupe Orange Cyberdefense. Ce sont leurs idées collectives qui ont rendu ce rapport possible :

Marc Germain-Laurent Blanchard	Orange Cyberdefense unité OSINT (France)
Alina Ribeiro	Manager de l'unité Cybercrime du CERT (France)
Laurent Celerier	Vice-président exécutif Technologie & Marketing (France-Mondial)
Diana Selck-Paulsson	Threat research Analyst (Suède)
Samsher Sagoo	Director of Professional Services and PMO (RU)
Mark Smith	Pre-Sales Manager (RU)
Richard Jones	Global CISO (Suède)
Nadav Shatz	Director of Advisory and Architecture (RU)
Mark Sprules	CISO (RU)
Feras Batainah	Senior Advisory Services Consultant (RU)
Wicus Ross	Group Security Research Center (Afrique du Sud)
Carl Morris	Group Security Research Center (RU)
Charl van der Walt	Head of Security Research (Afrique du Sud-Mondial)
Etienne Greeff	Global CTO (RU-Mondial)
Chris Miles	SVP Global Portfolio Management (RU-Mondial)
Tatiana Chamis-Brown	VP Global Marketing (RU)
Franz Haertl	Head of Global Content Marketing (ALL)
Lisanne Meerkerk	Head of Global Marketing Campaigns (NL)
Madina Maglione	Head of Global Field Marketing (RU)

Ressources

[1] https://www.forbes.com/sites/daveywinder/2020/03/23/meet-the-volunteer-covid-19-cyber-fighters-helping-healthcare-fight-the-hackers/
[2] https://www.europol.europa.eu/newsroom/news/how-criminals-profit-covid-19-pandemic
[3] https://isc.sans.edu/diaryimages/Kwampirs_PIN_20200330-001.pdf
[4] https://isc.sans.edu/diaryimages/Kwampirs_PIN_20200330-001.pdf
[5] https://isc.sans.edu/diaryimages/Kwampirs_PIN_20200330-001.pdf
[6] https://isc.sans.edu/diaryimages/Kwampirs_PIN_20200330-001.pdf
[7] https://isc.sans.edu/diaryimages/Kwampirs_PIN_20200330-001.pdf
[8] https://www.bleepingcomputer.com/news/security/chinese-hackers-use-cisco-citrix-zoho-exploits-in-targeted-attacks/
[9] https://geoffwhite.tech/2019/11/08/more-trouble-with-free-wifi/
[10] https://orangecyberdefense.com/uk/white-papers/databreaches-in-healthcare-the-attractiveness-of-leaked-healthcare-data-for-cybercriminals/
[11] https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-creditcard-idUSKCN-0HJ21I20140924
[12] https://www.hipaajournal.com/healthcare-data-breach-statistics/
[13] https://www.bbc.co.uk/news/health-39899646
[14] https://www.verdict.co.uk/ coronavirus-hackers-wrath/
[15] https://www.forbes.com/sites/daveywinder/2020/03/23/meet-the-volunteer-covid-19-cyber-fighters-helping-healthcare-fight-the-hackers/
[16] https://www.cyberthreatcoalition.org/
[17] https://isc.sans.edu/diaryimages/Kwampirs_PIN_20200330-001.pdf
[18] https://isc.sans.edu/diaryimages/Kwampirs_PIN_20200330-001.pdf
[19] https://en.wikipedia.org/wiki/Mobile_device_management
[20] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf
[21] https://threat-advisories.secdata.com/threats/viewSignal/SIG-4618
[22] https://threat-advisories.secdata.com/threats/viewSignal/SIG-4467
[23] Source: IDC European Survey - Impact of COVID-19 on European ICT Market and Ecosystem, March 2020
[24] https://www.businessinsider.co.za/countries-on-lockdown- coronavirus-italy-2020-3
[25] Security Affairs, https://securityaffairs.co/wordpress/99446/cyber-crime/coronavirus-map-delivers-malware.html
[26] Security Affairs, https://securityaffairs.co/wordpress/99446/cyber-crime/coronavirus-map-delivers-malware.html
[27] https://www.bleepingcomputer.com/news/security/danabot-banking-trojan-upgraded-with-non-ransomware-module/
[28] https://www.forbes.com/sites/thomasbrewster/2020/03/18/coronavirus-scam-alert-covid-19-map-malware-can-spy-on-you-through-your-android-microphone-and-camera/#396f2a8c75fd
[29] https://labs.bitdefender.com/2020/03/android-apps-and-malware-capitalize-on-coronavirus/
[30] https://www.zdnet.com/article/d-link-and-linksys-routers-hacked-to-point-users-to-coronavirus-themed-malware/
[31] https://www.zdnet.com/article/d-link-and-linksys-routers-hacked-to-point-users-to-coronavirus-themed-malware/
[32] https://www.grahamcluley.com/houseparty-hack-claims-reward/
[33] https://www.vice.com/en_us/article/y3m4b7/hackers-twitter-accounts-advertising-face-masks-coronavirus
[34] https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response
[35] https://cyberdefense.orange.com/en/2020/03/20/the-threat-of-cyberattacks-on-healthcare-establishments-during-the-covid-19-pandemic/
[36] https://cyberdefense.orange.com/en/2020/03/20/the-threat-of-cyberattacks-on-healthcare-establishments-during-the-covid-19-pandemic/
[37] https://www.thesun.co.uk/money/11276203/boots-shoppers-queue-hour-website/
[38] https://www.thesun.co.uk/money/11276203/boots-shoppers-queue-hour-website/
[39] https://www.eff.org/deeplinks/2020/03/what-you-should-know-about-online-tools-during-covid-19-crisis
[40] https://www.vice.com/en_us/article/z3b745/zoom-removes-code-that-sends-data-to-facebook

Ressources additionnelles (citations et captures d'écran sur Twitter):

https://twitter.com/TProphet/status/1245170055043825669?s=20
https://twitter.com/WHNSC/status/1239398218292748292?s=20
https://www.grahamcluley.com/houseparty-hack-claims-reward/ (House Party)
https://twitter.com/joehancock/status/1243097550841757696
https://twitter.com/drdavidjday/status/1243132223840227328?s=20
https://twitter.com/ruskin147/status/1243265319176732672?s=20
https://twitter.com/drdavidjday/status/1243814550530596865?s=20

Pourquoi Orange Cyberdefense ?

Orange Cyberdefense est l'unité commerciale experte en cybersécurité du groupe Orange. En tant que fournisseur européen de sécurité, nous nous efforçons de construire une société numérique plus sûre.

Nous sommes un fournisseur de sécurité axé sur la recherche et le renseignement, offrant un accès inégalé aux menaces actuelles et émergentes.

Nous sommes fiers de pouvoir proposer une protection globale doublée d'une expertise locale et de soutenir nos clients tout au long du cycle de vie des menaces.

Orange Cyberdefense a plus de 25 ans d'expérience dans le domaine de la sécurité de l'information et rassemble plus de 250 chercheurs et analystes, 16 SOC, 10 CyberSOC et 4 CERT répartis dans le monde entier ainsi qu'une assistance commerciale et de services dans 160 pays.

Contactez nous sur orangecyberdefense.com