Pandémie : une situation exceptionnelle… aussi sur le front cyber

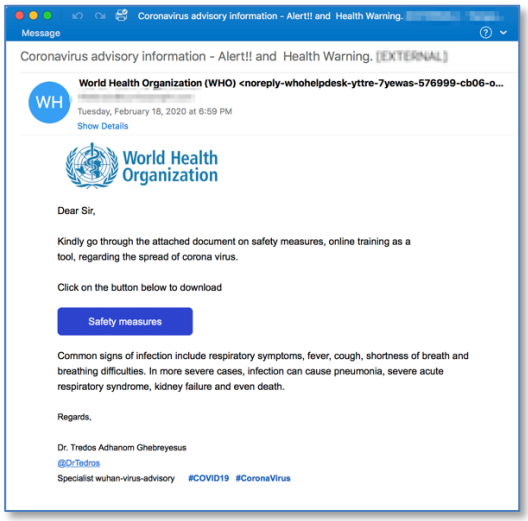
Loïc GUÉZO

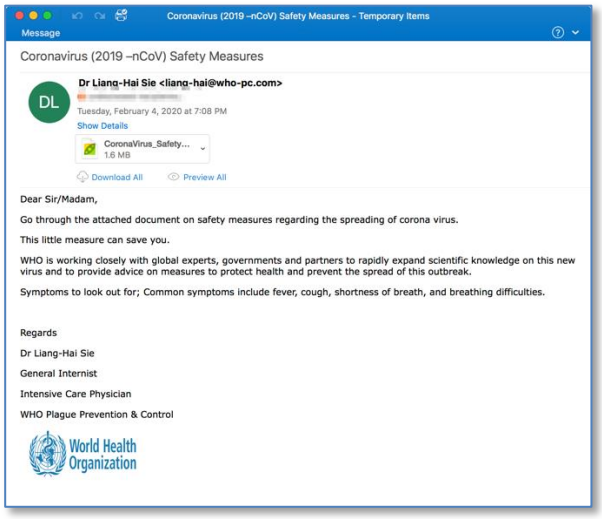
Senior Director, Cybersecurity Strategy SEMEA, Proofpoint
Réserviste Cybermenaces Police Nationale

Notre équipe de Recherche sur les menaces cyber (Cyber Threat Intelligence) constate désormais un volume cumulé de leurres électroniques sur le sujet du coronavirus qui en fait la plus grande collection de types d'attaques qu'ils aient vu depuis des années, voire même encore jamais vu sur un thème unique !

Les cybercriminels se nourrissent de perturbations et d'incertitudes et ne perdent pas de temps pour exploiter au maximum les opportunités qui s'offrent à eux. Les attaques de phishing liées aux coronavirus sont nombreuses, qu'il s'agisse de celles qui proposent un remède ou de celles qui collectent les informations nécessaires pour alimenter les "bases de données gouvernementales".

Certaines de ces attaques prétendent même provenir de l'Organisation Mondiale de la Santé (OMS), encourageant les destinataires à télécharger documents, applications ou à se connecter à leur site web.





Toutes invitent les victimes à cliquer sur des liens malveillants et à communiquer leurs identifiants ou d'autres informations personnelles.

Plus de 80 % des menaces utilisent d'une manière ou d'une autre des thèmes liés à la crise sanitaire actuelle. Cela inclut désormais des attaques qui ne mentionnent plus directement le coronavirus dans l'objet ou le corps d'un message, mais qui y font plutôt référence dans les pièces jointes, les liens ou les leurres.

Les messages que nous avons observés sont véritablement le reflet d'opérations d'ingénierie sociale à l'échelle mondiale où chacun d'entre eux est

soigneusement conçu pour convaincre les victimes potentielles d'effectuer une action (cliquer sur un lien malveillant, télécharger des pièces jointes malveillantes ou effectuer un paiement frauduleux...).

Ces exemples de courriels « coronavirus » visent essentiellement à tromper les personnes qui reçoivent ces messages en jouant sur l'humain via l'urgence, la peur voire la promesse d'un remède miracle.

À ce jour, nous avons vu plus de 500 000 messages, 300 000 URL malveillantes, 200 000 pièces jointes malveillantes ayant pour thème le coronavirus dans plus de 140 campagnes (et ce nombre continue d'augmenter[1]). Notre défi est que les attaquants persistent à envoyer des menaces liées au Covid-19 parce que leurs tactiques fonctionnent clairement.

Recours massif au télétravail, partout dans le monde…

Sur les conseils de la communauté médicale, le monde des affaires a appliqué des stratégies numériques pour participer à la limitation de la propagation du virus tout en maintenant la « continuité de service ».

Apple, Amazon, Facebook et Twitter ne sont que quelques-unes des organisations qui ont rapidement restreint les voyages ou imposé le travail à distance par mesure de précaution.

À Londres, le géant pétrolier Chevron a été la première entreprise à renvoyer ses 300 employés chez eux, et de nombreux autres lui ont emboîté le pas de par le monde.

Les cybercriminels ne sont que trop conscients que les entreprises s'appuient plus que jamais sur les outils de collaboration en ligne, ce qui augmente considérablement la taille de leur cible et surface d'attaque correspondante. Si la connectivité numérique est une bouée de sauvetage pour les entreprises dans des périodes comme celle-ci, elle pose également des problèmes qui lui sont propres.

La cybersécurité peut ne pas sembler être une priorité au regard des enjeux de santé mondiale ; mais en fait elle est plus importante que jamais.

Travailler à distance ? Comment être en sécurité !

Le confinement sanitaire a mené de nombreuses organisations à mettre en place le télétravail. Cet usage assure la continuité d'activité... mais il n'est pas sans risque !

La mise en œuvre de ces mesures de télétravail là où il est possible, demandé par le gouvernement français, nécessite pour beaucoup d'employeurs de mettre en œuvre ou de renforcer ces moyens de télétravail dans l'urgence.

Ces moyens d'accès à distance augmentent mécaniquement l'exposition des systèmes d'informations sur l'Internet, dans un contexte où les risques pour leur sécurité sont très élevés avec les découvertes récentes de vulnérabilités critiques touchant certaines de ces solutions d'accès VPN[2].

Enfin, un grand nombre de fraudes se développent qui peuvent notamment cibler et affecter les personnes en situation de télétravail. Il est nécessaire de sensibiliser ses équipes à ces risques qui peuvent les affecter à titre professionnel, mais également personnel.

Tout comme nous avons tous un rôle à jouer pour arrêter la propagation du virus (confinement, gestes barrière, distanciation sociale…[3]), chacun dans son organisation a un rôle à jouer pour en assurer la cybersécurité, en télétravail[4].

En complément des règles d'hygiène numérique déjà connues et mises en œuvre par les organisations (dont appliquer les correctifs de sécurité rapidement

[1] https://www.proofpoint.com/us/threat-insight/post/coronavirus-threat-landscape-update

[2] https://www.cert.ssi.gouv.fr/actualite/CERTFR-2020-ACT-001/

[3] https://solidarites-sante.gouv.fr/IMG/pdf/coronavirus_400x600_ech_1_option1_003_.pdf

[4] https://www.proofpoint.com/fr/learn-more/working-remotely-awareness-materials

et effectuer des sauvegardes hors ligne pour les données critiques) voici cinq conseils simples, à partager autour de vous et appliquer dès aujourd'hui[5] en situation de télétravail :

1 - Réfléchissez à deux fois avant de cliquer sur des liens

En télétravail, soyez conscient que vous ne bénéficiez plus toujours de la protection apportée par le réseau interne de l'entreprise notamment le filtrage des sites web ou de messagerie lors de vos usages personnels. Vous êtes donc plus vulnérable aux phishings. Les courriels de phishing conduisent à des sites web dangereux qui volent des données personnelles, des mots de passe et des informations sur les cartes de crédit. Saisissez plutôt l'adresse d'un site web connu directement dans votre navigateur !

2 - Confirmez toutes les demandes de transaction par téléphone

Évitez les escroqueries par courrier électronique en vérifiant oralement que toutes les demandes de paiement et de transfert de données sensibles sont réelles et autorisées.

3 - Utilisez des mots de passe forts

Ne réutilisez pas le même mot de passe deux fois. Envisagez d'utiliser un gestionnaire de mots de passe pour rendre votre navigation en ligne transparente, tout en restant sûre.

4 - Renforcez le WiFi

Changez le mot de passe par défaut de votre routeur wi-fi domestique et activez le chiffrement WPA/WPA2.

5 - Protégez votre connexion VPN

Les cybercriminels cherchent à se connecter au VPN d'entreprise pour accéder directement à tous les courriers électroniques, aux données et aux applications en nuage. Il appartient à l'organisation de vérifier que les utilisateurs distants sont limités aux seuls systèmes nécessaires et idéalement de mettre en place une solution d'authentification forte (MFA). Trop peu d'organisations ont encore pu déployer les nouvelles architectures d'accès dite « Zero Trust » : si votre accès VPN est détourné, alors c'est bien votre identité numérique professionnelle qui sera alors usurpée !

Enfin, concernant le télétravail ou le nomadisme numérique, il est toujours bon de (re)lire les recommandations de l'ANSSI[6] et de suivre l'actualité du CERT-FR [7].

[5] En cas de doute ou de pratiques complémentaires indiquées par votre organisation, il vous appartient de les respecter et de prendre attache avec votre service de support informatique si besoin.

[6] https://www.ssi.gouv.fr/guide/recommandations-sur-le-nomadisme-numerique/

[7] https://www.cert.ssi.gouv.fr/

Et en France, très concrètement ?

Sans oublier les derniers points d'actualité[8] avec du DDOS ou du rançongiciel, la Direction Centrale de la Police Judiciaire a déjà constaté de nombreuses escroqueries sous le prétexte de la crise sanitaire du coronavirus.

Par exemple, des groupes criminels organisés ont profité du début de la crise pour usurper l'identité de sociétés produisant ou distribuant des masques de protection et du gel hydro-alcoolique et cibler de nombreuses pharmacies, afin de les inciter à effectuer des commandes et des paiements sur des comptes bancaires français ou étrangers. Ce même type d'escroquerie est également en cours à l'encontre des hôpitaux, des EHPAD et des fournisseurs de matériel de protection médicale. Selon INTERPOL[9], plus de 2.000 bannières publicitaires en lien avec le COVID-19 ont été recensées sur Internet, proposant principalement des masques et des gels hydro-alcooliques contrefaits et/ou de mauvaise qualité et des activités de démarchage direct par téléphone sont même identifiées.

Plus largement, en cette période de confinement et de télétravail, les entreprises, n'ayant pas l'habitude d'appliquer le travail à distance, sont rendues plus vulnérables aux éventuelles fraudes car les processus habituels, mis en place au sein des sociétés pour lutter contre les fraudes financières, dont celle au changement de relevé d'identité bancaire, se retrouvent désorganisés.

Les fraudeurs peuvent espérer profiter de cette situation de crise sanitaire pour s'immiscer dans les chaînes de paiements des entreprises en ciblant les bons acteurs et percevoir des virements à leur insu…

Aujourd'hui, une stratégie de sécurité centrée sur l'infrastructure se révèle clairement insuffisante ; « protéger les personnes » garantit ici aux entreprises qui ont mis en place de tels programmes une vraie longueur d'avance : que les gens travaillent à domicile ou au bureau, une stratégie de sécurité centrée sur les personnes sera toujours payante...

Restons vigilants et confinés, nous ne sommes qu'au début de la vague…

[8] https://www.lemonde.fr/pixels/article/2019/11/26/apres-la-cyberattaque-au-chu-de-rouen-l-enquete-s-oriente-vers-la-piste-crapuleuse_6020609_4408996.html
https://lexpansion.lexpress.fr/high-tech/en-pleine-crise-du-coronavirus-les-hopitaux-de-paris-victimes-d-une-cyberattaque_2121692.html
http://www.leparisien.fr/high-tech/une-vaste-cyberattaque-cible-le-fabricant-de-verres-de-lunettes-essilor-25-03-2020-8287713.php

[9] https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2020/INTERPOL-warns-of-financial-fraud-linked-to-COVID-19