Comment la pandémie du COVID-19 a radicalement changé le monde de la cybersécurité

En effet, dans la panique ou l'urgence, les individus deviennent moins vigilants : la prudence, un de nos mécanismes de protection les plus efficaces, est alors la première à passer par la fenêtre. Les réactions face à la pandémie actuelle ne dérogent pas à la règle.

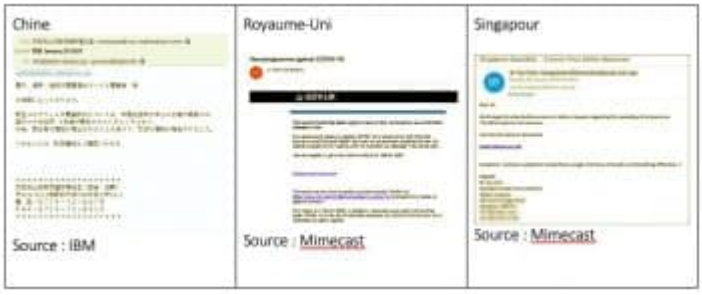
À l'heure où la plupart des membres de la population active sont désormais contraints de travailler de chez eux, ces agissements représentent un danger sans précédent. Les employés sont relativement protégés lorsqu'ils sont sur le lieu de travail et s'ils reçoivent un e-mail suspect, ils n'ont qu'à interroger leurs collègues pour en vérifier l'authenticité.

En revanche, quand on travaille à domicile, de façon isolée, cela devient plus compliqué.

Phishing et usurpation d'identité

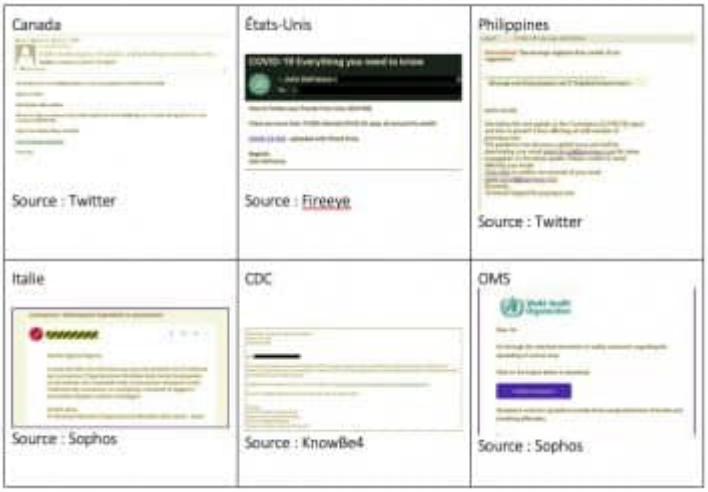
Les attaques les plus fréquemment observées durant ce genre d'événement relèvent du phishing (hameçonnage) ou ciblent l'identité des internautes[)] , et c'est particulièrement ce que nous voyons depuis le début de la crise du COVID-19. Cette avalanche d'attaques a poussé une multitude d'organismes gouvernementaux tels que l'OMS ou le FBI à publier des mises en garde. Il est donc opportun de se demander ce que recherchent les hackers et comment ils procèdent.

Tout d'abord, ils vont chercher à récupérer vos données personnelles (identifiants, nom, date de naissance, informations d'identification attribuées par le gouvernement etc.), ou vous pousser à installer des logiciels malveillants sur votre système. Et cela ne touche pas que les individus : les institutions, les entreprises, ou les organisations publiques constituent également des cibles très attrayantes.



En effet, toutes les nations sont ciblées, et les e-mails de phishing apparaissent dans presque toutes les langues. C'est pourquoi, à bien des égards, il s'agit d'une des plus vastes campagnes de cyber-attaques auxquelles nous n'ayons jamais assisté. La grande majorité de ces e-mails fournissent de fausses informations ou de fausses promesses d'aide liées à la pandémie du COVID-19.

Dans une campagne découverte par Proofpoint, les auteurs ont même promis des traitements (soit des éléments dont ils savent pertinemment qu'ils attireront immédiatement l'attention du grand public vu le climat d'inquiétude actuel). Mais les e-mails ne sont pas le seul vecteur des attaques par hameçonnage. Toutes les formes de médias sociaux et de communication sont concernées, en particulier les SMS, qui sont utilisés de façon identique pour cibler les utilisateurs.



La plupart de ces attaques manquent relativement de sophistication car elles sont criblées de fautes d'orthographe et dirigent sur des pages dont l'absence de fiabilité est évidente. Cependant, certaines sont remarquablement sophistiquées et mènent vers des pages conçues si intelligemment qu'elles téléchargent directement différents types de logiciels malveillants sur les ordinateurs.

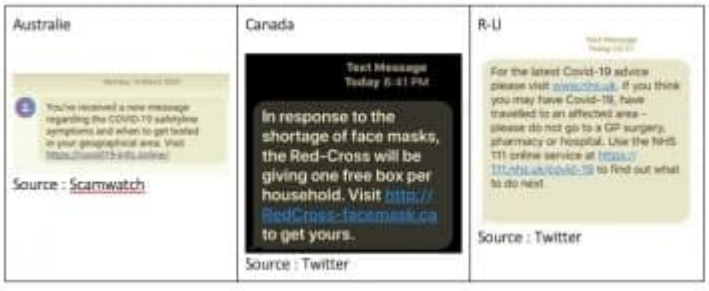
Logiciels malveillants et piratage, le combo gagnant

Pour le milieu du cybercrime, le contexte actuel ouvre la voie vers un véritable El Dorado. Jamais les

entreprises, les professionnels et les consommateurs n'auront été aussi désespérés et vulnérables. Les employés travaillant à distance ont besoin de VPN, ont des problèmes informatiques, doivent résister aux distractions et, surtout, sont isolés.
Dans une entreprise sécurisée, les maillons faibles sont pratiquement toujours les collaborateurs ou les prestataires. Ces derniers sont souvent décentralisés et disposent parallèlement des privilèges des employés internes, rajoutant un risque de sécurité supplémentaire.

Les cybercriminels ne sont pas les seuls à profiter de cette opportunité : les états-nations s'y mettent eux aussi. Malwarebytes a ainsi découvert une campagne attribuée à APT36, un acteur malveillant soupçonné d'être soutenu par l'état du Pakistan. Cet échantillon utilisait un e-mail de spear phishing (qui consiste à usurper l'identité de l'expéditeur), avec un lien vers un document prétendument issu du gouvernement indien, et contenant du code malveillant.
De son côté, le spécialiste de la cybersécurité Kaspersky aurait ainsi détecté des infections liées à la crise du COVID-19 chez 403 utilisateurs de ses produits. Au total, ses technologies ont détecté 2 673 fichiers infectés de ce type.

Preuve supplémentaire de l'expansion de ce phénomène : selon les données de Check Point plus de 4 000 noms de domaines liés au coronavirus auraient été créés à travers le monde depuis janvier 2020. Au total, 3% seraient malveillants et 5% de plus seraient suspects.
Les noms de domaines liés au coronavirus ont tendance à être plus fréquemment malveillants (50% de plus) que les autres domaines enregistrés au cours de la même période.



Comment se prémunir face aux attaques :

Phishing (Hameçonnage)

- Méfiez-vous des e-mails ou des fichiers envoyés par des inconnus. Évitez de cliquer sur des liens dans des e-mails non sollicités, et soyez particulièrement attentifs aux pièces jointes. Consultez les 10 règles de base de la sécurité sur l'Internet de l'ANSSI.
- En cas de doute, fermez l'e-mail, recherchez et rendez-vous par vous-même sur le site de

confiance afin d'accéder à la section nécessaire.

- Utilisez des sources fiables — tels que des sites gouvernementaux légitimes — pour obtenir des informations à jour et factuelles sur le COVID-19.
- Orientez-vous vers des sociétés reconnues et de confiance pour l'achat de produits de première nécessité.
- Ne révélez aucune information personnelle ou financière dans des e-mails, et ne répondez pas à ceux qui sollicitent de telles informations.
- Avant d'effectuer un don, vérifiez l'authenticité de l'organisme caritatif.
- Activez l'authentification à deux facteurs ou plus, ou des technologies de sécurité physique telles que Yubikey sur l'ensemble de vos sites compatibles.
- Utilisez un gestionnaire de mots de passe reconnu et de confiance, et générez des mots de passe uniques et complexes sur les sites ne prenant pas en charge plus d'un facteur. N'utilisez jamais le même mot de passe sur plusieurs sites.
- Soyez attentif aux questions de récupération de mots de passe – utilisez des informations qui ne peuvent pas être devinées ou recherchées, ou utilisez votre gestionnaire de mots de passe pour en recréer un de façon aléatoire.

Logiciels malveillants et piratage.

- Ne faites pas confiance à des inconnus vous demandant des informations sur votre entreprise.
- Installez un antivirus réputé pour votre plateforme, et veillez à ce qu'il soit constamment à jour.
- Gardez les logiciels et le système d'exploitation de votre ordinateur à jour.
- Attention aux logiciels gratuits ; parfois, cette gratuité cache quelque chose, notamment en ce qui concerne les applications disposant d'accès critiques telles que les VPN.
- Ne soyez pas le maillon faible de votre organisation : vérifiez que votre connexion au réseau de votre entreprise est sécurisée, et signalez toute activité suspecte, comme vous le feriez en travaillant au bureau.
- Si vous êtes responsable des systèmes d'information d'une organisation, assurez-vous de bien appliquer les principes du modèle Zero Trust. Vérifiez que les hackers ne peuvent pas pénétrer votre réseau sécurisé en profitant des failles créées par les employés travaillant à distance.
- Concevez votre architecture logicielle et réseau en mettant en place des principes de contrôle des identités renforcés. En utilisant l'authentification en continu et des mécanismes stricts de vérification d'identité, vous compliquez considérablement la tâche des hackers, car ces derniers auront beaucoup de mal à se faire passer pour des membres du personnel, même si leurs identifiants venaient à fuiter.