Risques liés à la sécurité numérique pendant la crise du coronavirus (COVID-19)

Version du 3 avril 2020

Messages clés

- Les risques liés à la sécurité numérique augmentent à mesure que des acteurs malveillants profitent de l'épidémie de coronavirus (COVID-19). On assiste à une hausse des escroqueries et des campagnes d'hameçonnage liées au coronavirus. Il existe également des cas de rançongiciels et d'attaques par déni de service distribué (DDoS) ciblant les hôpitaux.
- Les particuliers et les entreprises devraient procéder avec prudence lorsqu'ils reçoivent des messages concernant le coronavirus, et appliquer les mesures appropriées relatives à l'« hygiène » de sécurité numérique (par exemple, les correctifs, l'utilisation de mots de passe sécurisés et différents, les sauvegardes régulières, etc.).
- Les gouvernements devraient sensibiliser le public, surveiller le contexte de menaces et publier des lignes directrices facilement accessibles sur l'hygiène de sécurité numérique, en particulier pour les groupes vulnérables comme les personnes âgées et les petites et moyennes entreprises (PME). Les pouvoirs publics devraient également coopérer avec toutes les parties prenantes concernées, afin de, notamment, fournir une assistance aux opérateurs des activités critiques comme les hôpitaux, le cas échéant.

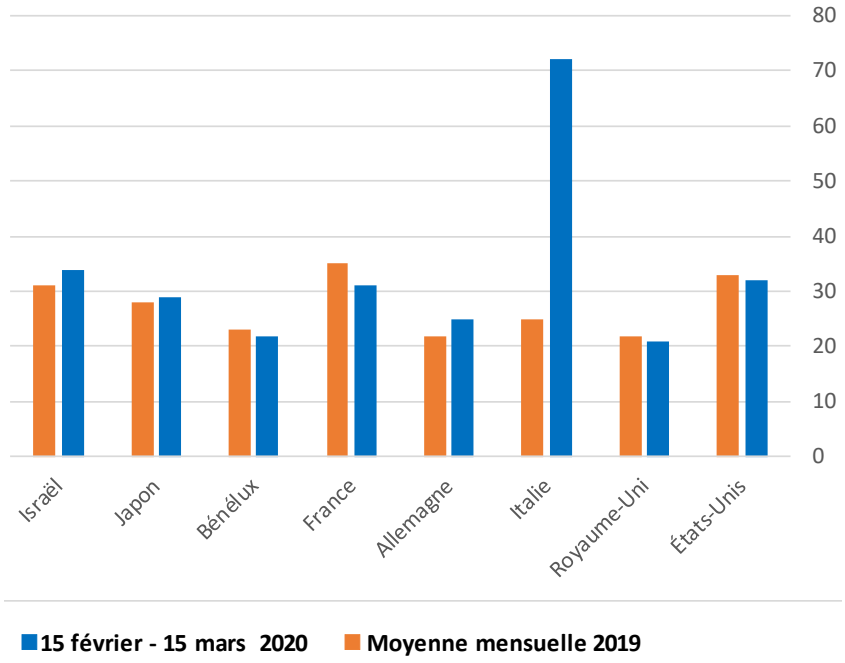
Les risques liés à la sécurité numérique augmentent au fur et à mesure de la crise du coronavirus (COVID-19)

Les acteurs malveillants tirent profit de l'épidémie pour rendre leurs attaques plus efficaces. Depuis février 2020, on observe une recrudescence des campagnes d'hameçonnage[1] utilisant des contenus relatifs au COVID-19, notamment :

- des courriers électroniques reprenant le thème du coronavirus dans le sujet ou le nom du fichier joint
- des courriers électroniques ou des SMS au nom des pouvoirs publics en Australie et au Royaume-Uni
- des courriers électroniques au nom de dirigeants ou d'institutions, comme l'Organisation Mondiale de la Santé
- des courriers électroniques, des liens ou des applications web imitant des initiatives légitimes.

Une entreprise de sécurité a constaté que les entreprises italiennes ont connu une augmentation des attaques d'hameçonnage en mars 2020. En Italie, une campagne d'hameçonnage sur le thème du COVID-19 a touché plus de 10 % des organisations du pays avec un courriel incitant les destinataires à ouvrir une pièce jointe malveillante.

Graphique 1. Pic d'attaques par hameçonnage en Italie



Source : Cynet.

Le tableau de bord interactif de l'université Johns Hopkins, qui localise les infections par coronavirus, a été imité par des cybercriminels en vue de répandre des logiciels malveillants qui dérobent les mots de passe. Le kit de logiciels malveillants est en vente sur les forums de l'internet clandestin (« dark web ») pour 200 USD.

[1] L'hameçonnage est une pratique frauduleuse qui consiste à envoyer des courriers électroniques censés provenir d'organisations fiables afin d'inciter des personnes à dévoiler des données personnelles, à donner des identifiants, à ouvrir des pièces jointes malveillantes, etc.

Au début du mois de mars 2020, une campagne de courriers électroniques ciblant les secteurs de la santé et des industries manufacturières aux États-Unis a contourné un projet légitime d'informatique distribuée pour la recherche sur les maladies. Dans le courrier électronique, il était demandé aux destinataires d'installer une pièce jointe qui permettait d'aider à obtenir un remède contre le coronavirus. La pièce jointe contenait un logiciel malveillant qui dérobait les informations d'identification et les portefeuilles de crypto-monnaie froids (portefeuilles de crypto-monnaie stockés hors ligne).

Les cybercriminels tirent également parti de la popularité des outils utilisés pour le télétravail, comme Zoom pour la visioconférence. Des experts ont détecté des campagnes d'hameçonnage avec des pièces jointes malveillantes contenant zoom dans le nom de fichier, et plus de 1 700 nouveaux noms de domaine Zoom ont été enregistrés depuis le début de la pandémie, vraisemblablement pour être utilisés à des fins malveillantes. On peut mentionner comme autre exemple les nouveaux domaines se faisant passer pour le site légitime de Google Classroom.

Des cas de rançongiciel[2] et des attaques par déni de service (DDoS)[3] ciblant des activités essentielles comme les hôpitaux ont eu lieu, notamment en France, en Espagne et en République tchèque.

- Les 12 et 13 mars, l'hôpital universitaire de Brno, deuxième plus grand hôpital de la République tchèque, a subi une attaque qui a provoqué l'arrêt immédiat des ordinateurs en plein milieu de l'épidémie de coronavirus. L'hôpital, qui abrite l'un des plus grands centres de dépistage du COVID-19 du pays, a été contraint d'annuler des opérations et de transférer les patients souffrant d'une affection aiguë vers d'autres hôpitaux.
- Le dimanche 22 mars, le centre hospitalier universitaire d'Ile de France (Assistance Publique – Hôpitaux de Paris [AP-HP]) a été victime d'une attaque DDoS d'une durée d'une heure qui a paralysé deux adresses connectées à internet. L'attaque n'a pas eu d'incidence sur les infrastructures de santé.
- Le 23 mars 2020, une attaque par rançongiciel a été lancée contre des établissements de soins en Espagne.
- Le 15 mars 2020, le département de la santé et des services sociaux des États-Unis (HHS) a subi une attaque DDoS.
- Le 14 mars 2020, le système d'information des services municipaux de la ville de Marseille (France) a fait l'objet d'une attaque par rançongiciel, à la veille des élections municipales. Toutes les applications destinées au public, ainsi que plusieurs systèmes internes, ont été mis hors ligne.

Les cybercriminels misent sur le fait que les individus et les organisations seront plus prompts à tomber dans le piège des escroqueries ou à payer des rançons en période de stress ou de crise, en particulier ceux qui n'appliquent pas les bonnes pratiques relatives à la sécurité numérique ou qui font face à des bouleversements organisationnels. **Toutefois, comme leurs techniques d'attaque et leurs codes malveillants ne sont pas nouveaux, appliquer une « hygiène » de base en matière de sécurité numérique est un moyen efficace permettant de diminuer ces attaques.**

[2] Le rançongiciel est un type de logiciel malveillant qui, le plus souvent, permet de crypter les données des utilisateurs et de menacer de bloquer l'accès aux données en l'absence de versement d'une rançon.

[3] Une attaque DDoS permet d'inonder le service d'une cible (par exemple un site web) de demandes provenant d'un grand nombre d'adresses IP, entraînant l'indisponibilité du service pour les utilisateurs légitimes, qui peut durer de quelques minutes à des journées entières.

Les pays prennent déjà des mesures pour contrer l'augmentation des risques liés à la sécurité numérique

Dans les pays de l'OCDE, les organismes publics chargés de la sécurité numérique répondent à la crise en sensibilisant le public, en surveillant le contexte de menaces, en fournissant une assistance le cas échéant et en coopérant avec les parties prenantes concernées, y compris au niveau international.

- L'agence de cybersécurité et de sécurité des infrastructures des États-Unis (Cyber and Infrastructure Security Agency [CISA]) a créé sur son site web une nouvelle rubrique entièrement consacrée aux risques de sécurité liés à la crise du COVID-19 (www.cisa.gov/coronavirus). Elle comprend des alertes et des recommandations sur les campagnes d'escroquerie et d'hameçonnage liées au COVID-19, des conseils pour le télétravail et une note sur la gestion des risques liés au nouveau coronavirus.
- La Commission européenne, l'ENISA, CERT-EU et Europol ont publié le 20 mars une déclaration dans laquelle ils soulignent leurs efforts de coopération en vue de traquer les activités malveillantes liées au COVID-19, d'alerter leurs communautés respectives et d'aider à protéger les citoyens confinés.
- Le Centre canadien de cybersécurité a publié une alerte dans laquelle il estime que la pandémie de COVID-19 expose les organismes de santé canadiens impliqués dans la réponse nationale à la pandémie à un niveau de risque plus élevé en matière de sécurité numérique. Le Centre recommande à ces organismes de rester vigilants et de prendre le temps nécessaire pour s'assurer qu'ils mettent en œuvre les meilleures pratiques en matière de cyberdéfense. Il mène également des actions de sensibilisation ciblant toutes les organisations au Canada.
- À la lumière des preuves recueillies lors du règlement de l'incident de l'hôpital de Brno, l'Agence nationale tchèque pour la sécurité informatique et cybernétique (NÚKIB) a ordonné à certains organismes du secteur de la santé de prendre des mesures pour renforcer la sécurité des principaux systèmes de TIC. La NÚKIB a proposé à ces organismes des services de consultation et de soutien.

En outre, de nombreuses entreprises, ainsi que des groupes industriels et professionnels, communiquent auprès du public sur les risques de sécurité numérique liés à la crise du COVID-19. Ils ont mise en place des guichets uniques et des centres de documentation, et fournissent des conseils sur des sujets spécifiques comme le télétravail sécurisé.

Principales recommandations

Il est recommandé au grand public de mettre en œuvre des mesures de sécurité personnelle pour se protéger et protéger les autres, et notamment de :

- Traiter avec prudence toute communication liée à la crise du coronavirus, même indirectement (par exemple les outils de télétravail), y compris les courriers électroniques, les messages sur les médias sociaux, les liens, les pièces jointes et les SMS.
- Garantir que les ordinateurs, les smartphones et autres appareils sont à jour et intègrent les derniers correctifs de sécurité.
- Sauvegarder régulièrement le contenu, en particulier les données importantes.

Il est recommandé aux gouvernements et aux autres parties prenantes de :

- Sensibiliser le public sur les risques accrus en matière de sécurité numérique liés au COVID-19, en particulier au regard des campagnes d'hameçonnage, des rançongiciels et des attaques DDoS. Fournir des conseils pratiques et des outils (affiches, graphiques, études de cas) susceptibles d'être facilement repris par d'autres parties prenantes.

- Publier des informations et des lignes directrices pour les organismes du secteur public, les entreprises et les particuliers, concernant notamment les nouvelles menaces et les bonnes pratiques relatives à l'hygiène de sécurité numérique et au télétravail.
- Soutenir les groupes vulnérables, en particulier les personnes âgées et les PME, car ils sont susceptibles de passer plus de temps en ligne et risquent de moins bien connaître les menaces.
- Surveiller le contexte de menaces (par exemple, l'hameçonnage, les rançongiciels) et alerter les communautés ciblées.
- Encourager les opérateurs qui mènent des activités critiques, en particulier dans le secteur de la santé, à relever le niveau de sécurité numérique et leur fournir un appui spécifique, le cas échéant, conformément à la *Recommandation du Conseil sur la sécurité numérique des activités critiques* adoptée par l'OCDE en 2019 (OCDE, 2019).
- Faciliter la coopération et l'échange d'informations sur les risques liés à la sécurité numérique entre les principales parties prenantes, tant au niveau national qu'international, et au niveau sectoriel (par exemple, la santé).

Pour aller plus loin

OCDE (2019), *Recommandation du Conseil sur la sécurité numérique des activités critiques*, OCDE, Paris, https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0456.

OCDE (2015), *Recommandation du Conseil sur la gestion du risque de sécurité numérique pour la prospérité économique et sociale*, OCDE, Paris, https://www.oecd.org/fr/sti/ieconomie/DSRM_French_final_Web.pdf.

L'OCDE réunit des données, des informations, des analyses et des recommandations relatives aux défis sanitaires, économiques, financiers et sociétaux soulevés par les conséquences de la crise du COVID-19. Pour des informations complètes sur le coronavirus, rendez-vous sur notre page dédiée.

www.oecd.org/sti – sti.contact@oecd.org – @OECDinnovation – http://oe.cd/stinews