michel creuzot
vous simplifie l'entreprise

FICHE ALERTE Cyber et COVID-19
Risque élevé d'attaques informatiques

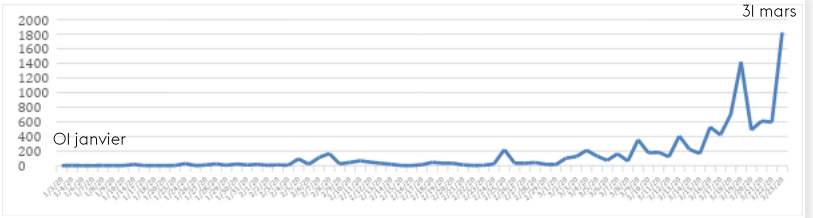
>> Pourquoi en ce moment ?

> Parce que les conditions de travail que nous vivons (télétravail, réduction d'effectif, ...) sont inhabituelles et peuvent être déstabilisantes ;
> Parce que l'ambiance anxiogène liée à la gestion de crise peut induire des comportements à risque ;
> Parce que des attaquants profitent de l'actualité pour générer des escroqueries ou des actes malveillants.

+ 667%

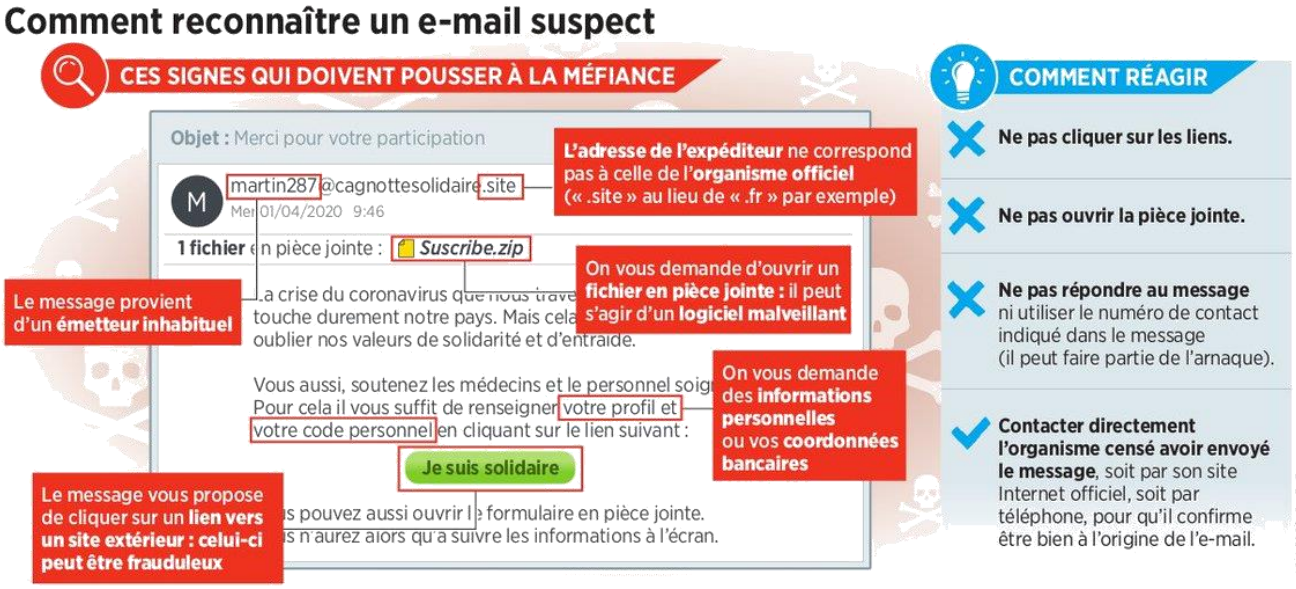
C'est l'augmentation du nombre d'attaques par phishing liées au Covid-19 depuis fin février 2020 !

Source : Undernews.fr



>> Comment agissent les pirates informatiques ?

> Mise en ligne de fausses attestations de déplacement sans limite de date, dans le but de collecter des données personnelles ou de vous demander de l'argent ;
> Déploiement de logiciels malveillants (type rançongiciels (« ransomware »)) via de fausses applications pour smartphone, censées suivre l'évolution du virus ;
> En se faisant passer pour la collectivité, l'assistance informatique ou la DRH, ou en demandant d'appeler un faux numéro, en prétextant un problème informatique ou une directive RH, dans le but de bloquer votre ordinateur, votre smartphone, ou de vous soutirer de l'argent ;
> En utilisant la technique habituelle de l'hameçonnage (« phishing ») pour prendre une fausse identité officielle (site du ministère de la santé par exemple), afin de vous faire cliquer sur un lien frauduleux dans un mail ou SMS.



Source : Le Parisien

>> Que faire pour redoubler de vigilance face à ces appels / messages ?

- **Vérifiez l'identité de leur expéditeur**, en cas de doute, supprimez le mail et appelez vos contacts habituels ;
- **Ne cliquez surtout pas sur les liens qui vous paraissent suspects** (en particulier si vous ne reconnaissez pas l'adresse Internet (URL) qu'ils indiquent) ;
- **Ne vous connectez que sur des sites officiels** (ceux qui se terminent par « seinemaritime.fr » ou « gouv.fr » par exemple), et ne cliquez pas sur les liens présents dans les mails, utilisez plutôt le moteur de recherche de votre navigateur Internet pour trouver les sites (exemple : https://qwant.fr) ;
- **Ne propagez pas de tels messages**, et n'alertez pas la cellule d'assistance informatique (sauf en cas de récidive ou si vous êtes confrontés à un blocage), mais supprimez-les immédiatement ;
- **N'installez pas d'applications gratuites**, elles sont potentiellement porteuses de code malveillant ;
- **Ne communiquez jamais votre mot de passe** à quiconque, et **verrouillez votre ordinateur quand vous sortez** ;
- **Ne communiquez jamais de données personnelles** à quiconque ou sur aucun site sans en avoir vérifié la source ;
- En télétravail, **protégez le matériel contre le vol**, et ne mélangez pas vie privée et vie professionnelle ;
- **Ne connectez pas de périphériques de stockage externe** (clé USB par exemple) à votre ordinateur.

>> Quelques exemples de phishing spécial Covid-19

- Survivre au coronavirus
  - Utilisation d'une image en lieu et place du texte pour contourner les filtres de détection
  - Emails marketing graphiquement assez travaillés
- Arnaque à la vente de masques ;
- Dons en faveur de la recherche ;
- Proposition de médicaments miracles.

Source : Silicon.fr

>> ET SURTOUT !

Si vous pensez être victime d'une attaque, déconnectez-vous immédiatement du réseau, contactez votre assistance informatique mais n'éteignez pas votre ordinateur.

>> Pour plus d'informations :

- https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/recommandations-securite-informatique-teletravail
- https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/coronavirus-covid-19-vigilance-cybersecurite
- Quelques comptes à suivre sur Twitter : (pensez à cliquer sur le bouton Suivre pour être alerté des publications)
  - @CERT_FR : Centre gouvernemental de veille aux attaques informatique
  - @cybervictimes : Compte officiel du dispositif d'assistance aux victimes de cybermalveillance
  - @clusif : Club de la sécurité de l'information français
  - @GendarmeriePjgn : Pôle judiciaire de la Gendarmerie nationale
  - @CNIL : Commission Nationale de l'Informatique et des Libertés
  - @ANSSI_FR : Agence Nationale de la Sécurité des Systèmes d'Information

⚠ CONCLUSION

La période de crise est une opportunité supplémentaire pour les pirates informatiques. **RESTONS VIGILANTS !** Ces attaques sont réelles ! La ville de Marseille, la région PACA ainsi que d'autres collectivités et les hôpitaux de Paris ont fait l'objet d'une attaque récente.

Contactez-nous !
Privilégiez les communications par mail