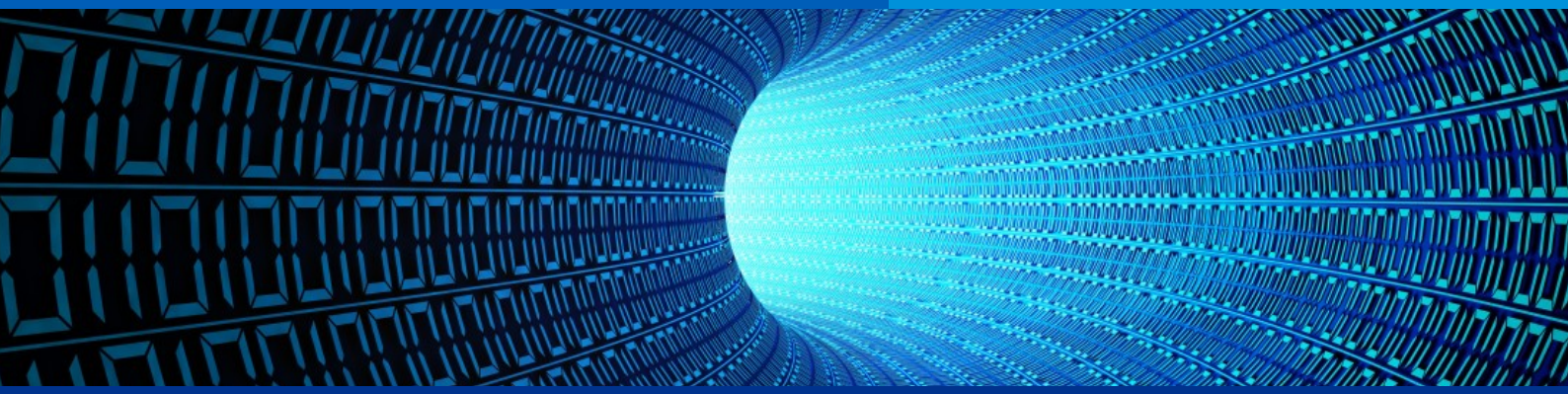
KPMG GLD & Associés Monaco

IT Advisory

Octobre 2020



Cybersécurité & COVID-19
Guide de Prévention

La Principauté de Monaco, comme la plupart des pays, fait face à une recrudescence de cyber attaques ciblées localement exploitant la sensibilité du public autour des thématiques de la pandémie de COVID-19 et de la crise sanitaire, économique et sociale.

Pour vous aider à vous prémunir des dangers liés à l'exploitation des failles de sécurité potentielles dus notamment à l'usage accru du travail à distance, KPMG vous propose un guide pour mettre à jour vos employés sur les mesures de prévention élémentaires à mettre en œuvre.

Sommaire

Les menaces

Depuis la mi-février, les sociétés membres de KPMG ont vu la mise en place rapide de l'infrastructure par les cybercriminels utilisée pour lancer des attaques de phishing sur le thème de COVID-19 et pour attirer des cibles vers de faux sites Web cherchant notamment à collecter des informations d'identification Office 365.

Voici quelques exemples de ces campagnes de cyber attaques:

- ✓ Une campagne d'e-mails de phishing «sans précédent » selon l'AMSN basé sur le malware Emotet, les courriels d'hameçonnage contenant généralement des pièces jointes Word ou PDF malveillantes, et plus rarement des URL pointant vers des sites compromis ou vers des documents Word contenant des macros.

- ✓ Des campagnes d'e-mails de phishing sur le thème de la COVID-19 contenant en pièces jointes des documents Microsoft Word prenant en charge les macros contenant des informations sur la santé qui déclenchent le téléchargement du malware Emotet ou Trickbot ;

- ✓ Plusieurs e-mails de phishing incitant les utilisateurs cibles à de fausses copies du site web du qui sollicitent les informations d'identification et les mots de passe des utilisateurs ;

- ✓ Une sélection de fausses alertes à la clientèle censées fournir aux clients des mises à jour sur les interruptions de service dues à la COVID-19 et entraînant le téléchargement de logiciels malveillants ;

- ✓ Des e-mails de phishing censés provenir du Ministère de la Santé ou de l'Organisation Mondiale de la Santé, qui imposent des mesures de précaution, incorporant à nouveau des logiciels malveillants ;

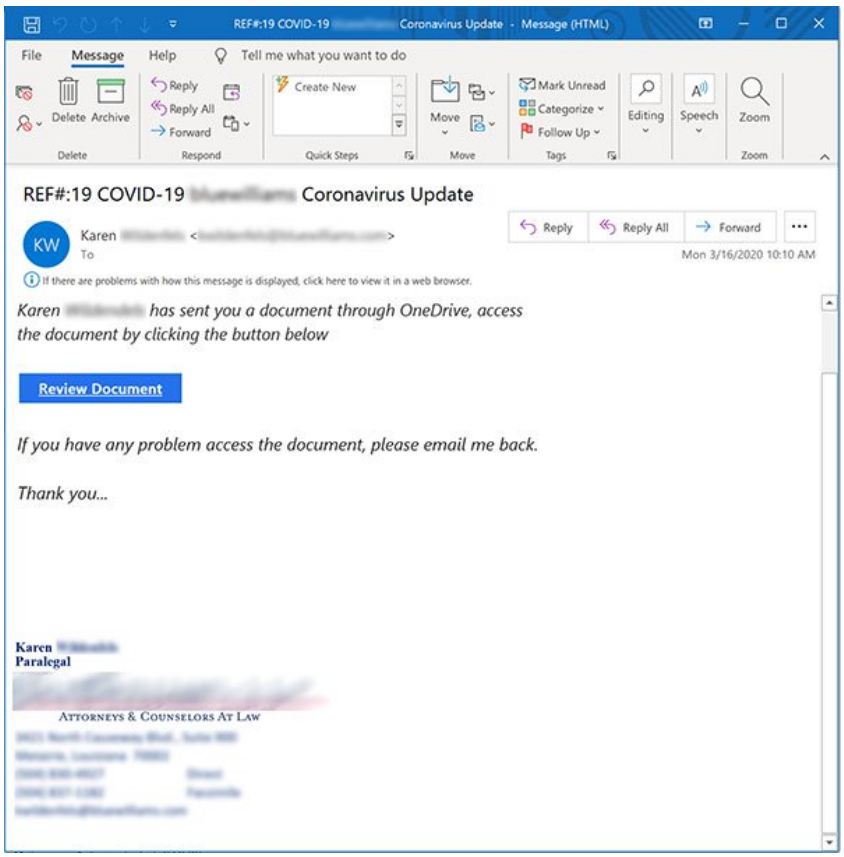
- ✓ Les mécanismes de d'aide ou remboursements liés à la COVID-19 attire le phishing pour encourager les destinataires à accéder à un faux site web qui recueille des informations financières et fiscales d'utilisateurs sans méfiance.

De nombreux groupes criminels organisés existants ont changé leurs tactiques pour utiliser les documents liés au COVID-19 sur les mises à jour sanitaires, les faux remèdes, les paquets fiscaux, les prestations d'urgence et les pénuries d'approvisionnement.

Les indices usuels pointant vers la nature suspecte d'un e-mail incluent notamment :

- ✓ Des fautes de grammaire, de ponctuation et d'orthographe ;
- ✓ Une mise en page et une qualité générale du courrier électronique qui détonent par rapport aux courriels habituels du correspondant ;
- ✓ Le courriel ne vous est pas adressé directement à votre nom mais utilise des termes génériques tels que «Cher collègue», «Cher ami» ou «Cher client» ;
- ✓ Implique une menace voilée ou génère un sentiment exagéré d'urgence ;
- ✓ Sollicite directement des informations personnelles ou financières.

En général, si cela semble trop beau pour être vrai, top générique pour être professionnel, ou trop alarmiste pour être réaliste, c'est généralement le cas.



Exemple de courriels d'hameçonnage (phishing) lié à la COVID-19

Les réponses

Vous devez prendre certaines mesures clés de prévention pour réduire les risques pour votre organisation et vos employés, en particulier dans le cadre du télétravail :

- ✓ Sensibiliser votre équipe en les avertissant du risque accru d'attaques de phishing sur le thème du COVID-19 – par exemple en partageant ce document ;
- ✓ Partagez des sources de conseils faisant autorité sur les moyens de travailler en sécurité et fournissez des mises à jour régulières sur l'approche que votre organisation adopte face à la pandémie COVID-19 ;
- ✓ Assurez-vous de mettre en œuvre des politiques de mots de passe forts - de préférence assortis d'une authentification à deux facteurs, pour tous les comptes d'accès à distance; en particulier pour l'accès Office 365 ;
- ✓ Fournir aux travailleurs à distance des conseils simples sur la façon d'utiliser les solutions de travail à distance, y compris comment s'assurer qu'ils restent en sécurité et des conseils sur l'identification du phishing
- ✓ Assurez-vous que tous les ordinateurs portables fournis disposent d'un logiciel antivirus et de pare-feu à jour ;
- ✓ Mettez en place une ligne d'assistance téléphonique ou un canal de discussion en ligne accessible facilement pour obtenir des conseils ou signaler tout problème de sécurité, y compris un éventuel phishing ;
- ✓ Crypter les données conservées sur les ordinateurs portables utilisés pour le travail à distance pour réduire les conséquences d'un vol ;
- ✓ Evitez si possible de transférer des données vitales sur des clés USB – même encryptées - pour éviter le risque de logiciels malveillants, en offrant au personnel un autre moyen de transférer des données, tel qu'un outil de collaboration à distance.
- ✓ En cas de doute sur un fichier suspect, vous pouvez le tester en ligne : https://www.virustotal.com/gui/home/upload

Conseils divers de cybersécurité

Prévention contre les FOVI (faux ordres de virement)

Assurez-vous que vos processus financiers nécessitent que les équipes financières confirment toute demande de paiement important pendant la pandémie COVID-19.

Cette confirmation peut aider à se prémunir contre le risque accru de compromission des e-mails professionnels et de fraudes au PDG.

Idéalement, utilisez un autre canal tel que téléphoner ou envoyer des SMS pour confirmer une demande par e-mail.

Protection du parc informatique

Attendez-vous à un risque accru de ransomware (*rançongiciels*) et doxware pendant la pandémie COVID-19, car les groupes cybercriminels exploitent le phishing sur le thème du COVID-19.

Assurez-vous d'appliquer les mises à jour correctifs de sécurité critiques et de mettre à jour les pares-feux et les logiciels antivirus dans l'ensemble de votre parc informatique, y compris tous les ordinateurs portables utilisés pour le travail à distance.

Assurez-vous de sauvegarder tous les systèmes critiques et de valider l'intégrité des sauvegardes, idéalement en organisant régulièrement le stockage hors ligne des sauvegardes.

Procédures spécifiques de gestion de crise

Enfin, travaillez avec votre équipe de gestion des incidents et des crises pour vous assurer que votre organisation dispose d'un environnement de secours pour les conférences audio et vidéo.

Cette plate-forme alternative sera nécessaire si vous avez un incident de ransomware qui perturbe vos systèmes informatiques, et fournira également une redondance supplémentaire si votre plateforme principale présente des problèmes de capacité ou de disponibilité.

La COVID-19 entraînera des changements importants dans la façon dont vous et votre organisation travaillez, protégez vos ressources et la sécurité de votre entreprise !

Homologation PASSI à Monaco

Les entreprises qualifiées PASSI à Monaco sont en capacité d'auditer la sécurité des systèmes informatique en suivant un processus strict de certification et le référentiel PASSI, ainsi que défini par l'Arrêté Ministériel 2017-625 du 16 août 2017.

L'homologation PASSI permet notamment de certifier les points suivants :

- ✓ Garantie de compétences des auditeurs en charge de l'audit
- ✓ Garantie de déontologie, de protection et de confidentialité des données, rapports et documents échangés
- ✓ Garantie d'une méthodologie appropriée aux audits de sécurité
- ✓ Recours possible auprès de l'Agence Monégasque de Sécurité Numérique (AMSN) si la prestation réalisée s'avère non conforme au référentiel PASSI.

Nos services homologation PASSI à Monaco

KPMG GLD & Associés Monaco fait désormais partie du cercle très restreint des entreprises ayant obtenu le diplôme de qualification de Prestataire d'Audit de la Sécurité des Systèmes d'Information (PASSI) auprès des autorités monégasques.

- ✓ + de 100 collaborateurs basés à Monaco au sein du cabinet ;
- ✓ + de 120 missions d'audit / conseil SI à Monaco ;
- ✓ Pour la 3ème année consécutive, KPMG leader mondial en Cyber Sécurité ;
- ✓ Qualifié PASSI sur toutes les activités d'audit de sécurité avec un « Lab » dédié ;
- ✓ 1er « Big Four » avec une équipe « Audit et Conseil en SI » à temps plein à Monaco ;
- ✓ Données collectées et stockées exclusivement à Monaco ;
- ✓ Réseau mondial de plus de 2.500 experts en cybersécurité dans 50 pays ;
- ✓ Spécialisé dans l'accompagnement des OIV et les audits d'homologation PASSI ;

Pour plus d'informations, contactez notre service IT Advisory.

Liens utiles / Plus d'informations

KPMG - Cyber sécurité à Monaco : risques et prévention pendant la COVID-19 :
https://assets.kpmg/content/dam/kpmg/mc/pdf/KPMG-Monaco-IT-Advisory-Cybersecurite-COVID-19.OCT-2020.pdf

KPMG Monaco : Homologation PASSI à Monaco
https://home.kpmg/mc/fr/home/services/advisory/it-advisory-homologation-passi.html

KPMG Monaco : Cyber Sécurité : évaluations et accompagnement
https://home.kpmg/mc/fr/home/insights/2020/01/kpmg-monaco-technologie-securite.html

Agence Monégasque de Sécurité Numérique :
https://amsn.gouv.mc

Alertes CERT-MC (AMSN) :
https://amsn.gouv.mc/Alertes-CERT-MC/

L'Homologation de sécurité en neuf étapes :
https://amsn.gouv.mc/var/amsn/storage/original/application/1eef84da244679829afb98664c63a2f5.pdf

Recommandations de sécurité informatique pour le télétravail en situation de crise :
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/recommandations-securite-informatique-teletravail

KPMG - Key cyber security considerations for 2020 *(en anglais)* :
https://assets.kpmg/content/dam/kpmg/xx/pdf/2020/03/all-hands-on-deck-key-cyber-security-considerations-for-2020.pdf

Contactez-nous

Bettina Ragazzoni
Associé
bragazzoni@kpmg.mc

André Garino
Associé
agarino@kpmg.mc

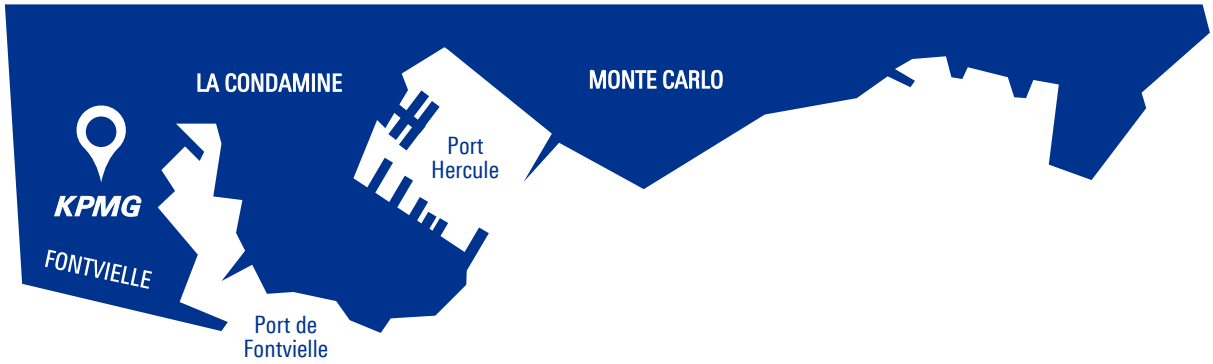
Bernard Squecco
Associé
bsquecco@kpmg.mc

Tony Guillemot
Associé
tguillemot@kpmg.mc

Stéphane Garino
Associé
sgarino@kpmg.mc

Gérard de Gregori
Associé
gdegregori@kpmg.mc

2, rue de la Lüjerneta - “Athos Palace” - 98000, Monaco



+377 97 777 700

www.KPMG.mc

mc-contact@kpmg.mc

@kpmg-monaco

@KPMGMonaco

@KPMG_Monaco