Télétravail, numérique et cyberattaque - sensibilisation sur le Coronavirus

Ajouté le 27/03/2020

https://www.proofpoint.com/us/learn-more/attack-spotlight-COVID-19-awareness-training-asset (dont une vidéo et un poster, complétant un plan projet, en anglais …).

Alerte rédigée par la DCPJ qui a constaté que les cybermalveillants profitent de la baisse d'attention des directions financières pour obtenir des **virements indus par changement de relevé de coordonnées bancaires**, préjudiciant notamment la sphère médicale (CHU, EHPAD, pharmacies et fournisseurs de matériel principalement) dans le cadre de commandes de masques de protection et de gel hydro-alcoolique :

****

Sensibilisation relative aux escroqueries dans le cadre de la crise sanitaire du COVID 19

Paiement de fausses factures par usurpation d'identité du fournisseur

La Direction Centrale de la Police Judiciaire a constaté de nombreuses escroqueries visant notamment des pharmacies sous le prétexte de la crise sanitaire du CORONAVIRUS. En effet, 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.

De plus, selon INTERPOL, 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.

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 vulnérables aux éventuels fraudes. En effet, les process 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 profiter de cette situation de crise sanitaire pour s'immiscer dans les chaînes de paiements des entreprises et percevoir des virements à leur insu.

La Direction Centrale de la Police Judiciaire incite les sociétés et hôpitaux **à vérifier tout paiement et notamment ceux en lien avec un changement de coordonnées bancaires du fournisseur**.

Dans le cas de l'exécution d'une escroquerie suite à un virement non causé, ou faussement causé, veuillez prendre attache immédiatement avec votre banque pour effectuer un rappel des fonds et contacter la direction de la police judiciaire territoriale pour les prévenir de la fraude.

****

Le lien Gitub sur les site légitime COVID-19 :
https://github.com/krassi/covid19-related
NB. Les listes vont évoluer pour qualifier le niveau de confiance

---

Sensibilisation aux bonnes pratiques/risques liés au télétravail, des illustrations mises sous licence Creative Commons par Advens :
https://www.advens.fr/fr/ressources/publications/kit-sensibilisation-teletravail-securite

Bulletin d'informations Cyber issu de notre SOC avec des préconisations pour faire face à l'augmentation de la menace, liée au contexte sanitaire et au recours accru au télétravail

➔ https://www.advens.fr/ressources/publications/covid-19-bulletin-dinformations-cyber

---

En réponse à l'appel lancé par Cédric O, secrétaire d'Etat chargé du numérique, le 9 mars, les entreprises technologiques se sont mobilisées pour proposer gratuitement (ou au moins avec une offre promotionnelle importante) leurs solutions innovantes. Cette solidarité doit aider les Français à traverser cette épreuve commune.

Tout est là : https://www.economie.gouv.fr/coronavirus-offre-services-numeriques

---

1- La précipitation du passage au télétravail complet a conduit à l'ouverture de beaucoup de flux pour accéder aux applications à distance, dont des flux RDP avec les failles connues et facilement exploitables sur ce protocole.
    a. *Notre conseil est d'utiliser vos scanner de vulnérabilités pour connaitre les vulnérabilités liées à ce protocole si vous l'avez autorisé et d'essayer de le corriger ou de faire passer le trafic par un reverse proxy.*
2- Certain utilisateur n'étant pas dotés d'ordinateur portables fournis par leur entreprise, ils ont été autorisés à utiliser leur matériel personnel sans que celui puisse répondre à des critères de conformité liés à la sécurité du poste.
    a. *Notre conseil : essayez tant que possible de protéger ces terminaux avec des solutions utilisées par l'entreprise afin de limiter les accès frauduleux aux SI par ce vecteur, il me semble que l'éditeur d'EDR SentinelOne met à disposition des licences « gratuites » utilisables jusqu'au 15 mai 2020. Un formulaire est disponible sur leur site à cet effet.*

- le référencement du Syntec Numérique des « *acteurs du numérique présents sur le territoire français et qui apportent des solutions concrètes et opérationnelles pour mieux gérer la situation de crise entraînée par le Covid-1* », classées par catégories (pour le grand public et les familles, pour les entreprises et les salariés, pour les malades, et professionnels de santé) : Lien : https://covidsyntecnumerique.fr/

- l'action des membres de l'association Hexatrust qui fournissent des solutions gratuitement pour aider à traverser la crise d'un point de vue SSI : https://www.hexatrust.com/coronavirus/

Coronavirus : la solidarité s'exprime aussi chez les fournisseurs de solutions IT (remis à jour régulièrement)

Les outils sont évidements à voir s'ils sont pertinents dans son contexte :

https://www.itforbusiness.fr/coronavirus-la-solidarite-sexprime-aussi-chez-les-fournisseurs-de-solutions-it-34991?utm_source=phplist197&utm_medium=email&utm_content=HTML&utm_campaign=Les+technologies+qui+animent+les+meilleurs+Dashboards+de+suivi+du+Coronavirus+sur+le+Web+-

+Ce+que+les+nouvelles+consoles+PS5+et+XBox+Series+X+peuvent+apprendre+aux+DSI%E2%80%A6+-+78%25+des+entreprises+ont+d%C3%A9j%C3%A0+pass%C3%A9+Kubernetes+en+production

Coronavirus (COVID-19)

APPEL AU RENFORCEMENT DES MESURES DE VIGILANCE CYBERSÉCURITÉ

Face à l'exploitation de la crise sanitaire par les cybercriminels, voici quelques recommandations pour adopter les bonnes pratiques et se prémunir des risques, à titre personnel et professionnel :

1. **Méfiez-vous des messages** (mail, SMS, chat...) ou appels téléphoniques d'origine inconnue ou inattendus
2. **Ne téléchargez vos applications** que depuis les sites ou magasins officiels des éditeurs
3. **Vérifier la fiabilité** et la réputation des sites que vous visitez
4. **Soyez vigilants** aux fausses informations
5. **Attention** aux appels aux dons frauduleux

Pour les professionnels :

- soyez attentifs aux fausses commandes ou aux modifications de virements bancaires frauduleux
- ne baissez pas la garde, au contraire, montez-là !

Tous ces conseils en détail sur **www.cybermalveillance.gouv.fr**

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/recommandations-securite-informatique-teletravail

Crise Covid19 : Risques et challenges pour le travail distant

https://www.cesin.fr/uploads/files/CESIN%20et%20COVID-19%20v2.pdf

---

Cellules de crises et SI (Clusif)

https://clusif.fr/publications/cellules-de-crises/

Comment réussir le déploiement d'un SOC (Clusif)

https://clusif.fr/publications/reussir-deploiement-dun-soc/

Management des Risques et des Assurances de l'Entreprise
80 BOULEVARD HAUSSMANN 75008 PARIS - TEL : +33 (0)1 42 89 33 16 - FAX : +33 (0)1 42 89 33 14 - amrae@amrae.fr - www.amrae.fr