Orange
Cyberdefense

COVID-19

Quand un risque biologique devient numérique

Analyser la crise dans la crise

Nicolas Arpagian – VP Stratégie & Affaires publiques

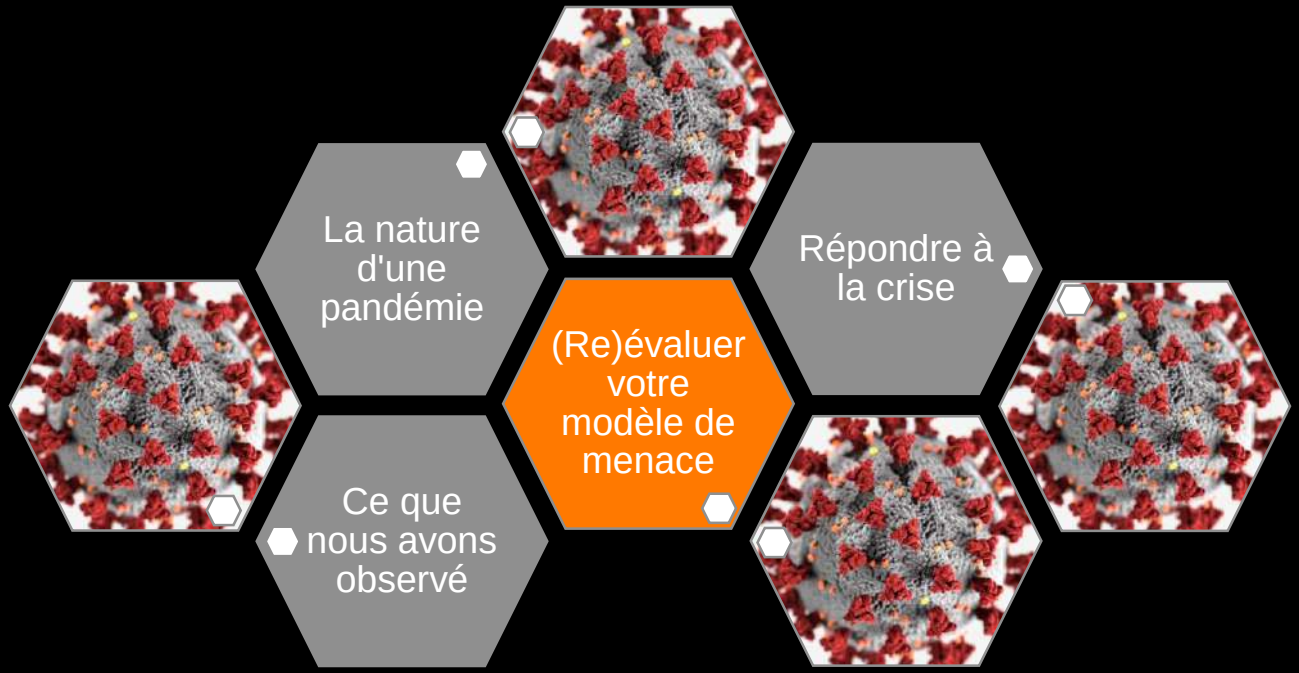
@cyberguerre

OrangeCyberdefense.com

Avec nos remerciements

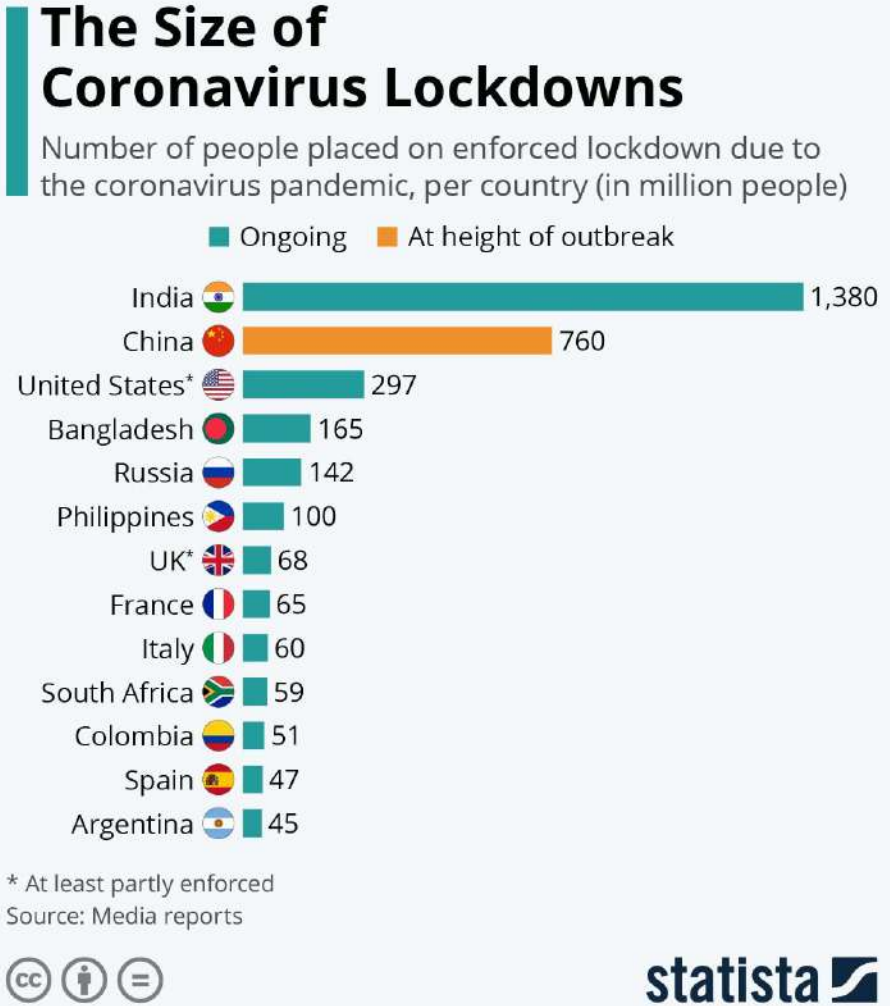
- Centre de recherche sur la sécurité (SRC)
- Computer Emergency Response Team (CERT)
- Laboratoire d'épidémiologie (logiciels malveillants)
- Unité OSINT
- CyberSOC
- Conseil & Architecture
- Bureau mondial du CISO
- Bureau mondial du CTO

Structure

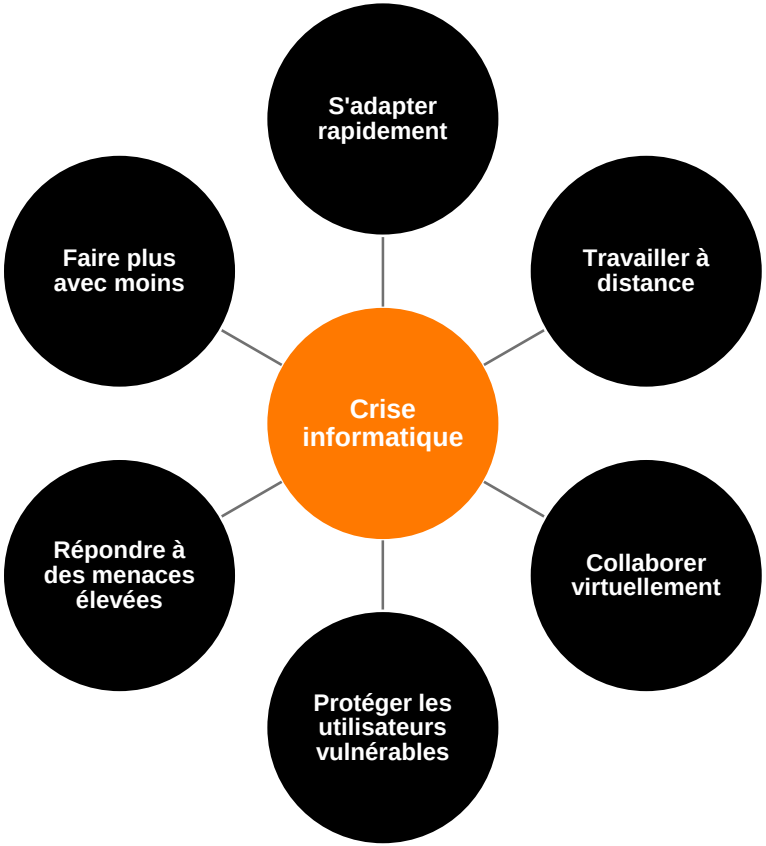

La nature d'une pandémie
Répondre à la crise
(Re)évaluer votre modèle de menace
Ce que nous avons observé

1. La nature d'une pandémie

“Un tiers”.


The Size of Coronavirus Lockdowns
Number of people placed on enforced lockdown due to the coronavirus pandemic, per country (in million people)
Ongoing
At height of outbreak
India 1,380
China 760
United States* 297
Bangladesh 165
Russia 142
Philippines 100
UK* 68
France 65
Italy 60
South Africa 59
Colombia 51
Spain 47
Argentina 45
* At least partly enforced
Source: Media reports
statista

Une situation d'urgence qui oblige les entreprises à...



2. Ce que nous avons observé

Vue d'ensemble d'une crise

Les utilisateurs sont plus suspects

Les attaquants ont pivoté

L'informatique à domicile n'est pas sûre

L'accès à distance est une cible

Les systèmes de santé et les données liées sont des cibles

L’appât idéal

World Health Organization
UNITED NATIONS FOUNDATION
SWISS PHILANTHROPY Foundation

HELP FIGHT CORONAVIRUS

COVID-19 Solidarity Response Fund for WHO

We are all affected by the growing COVID-19 pandemic. It's an unprecedented health challenge and we know people and organizations everywhere want to help. The World Health Organization is leading and coordinating the global effort, supporting countries to prevent, detect, and respond to the pandemic.

The greatest need right now is to help ensure all countries are prepared, especially those with the weakest health systems. **Donations support WHO's work to track and understand the spread of the virus; to ensure patients get the care they need and frontline workers get essential supplies and information; and to accelerate efforts to develop vaccines, tests, and treatments.**

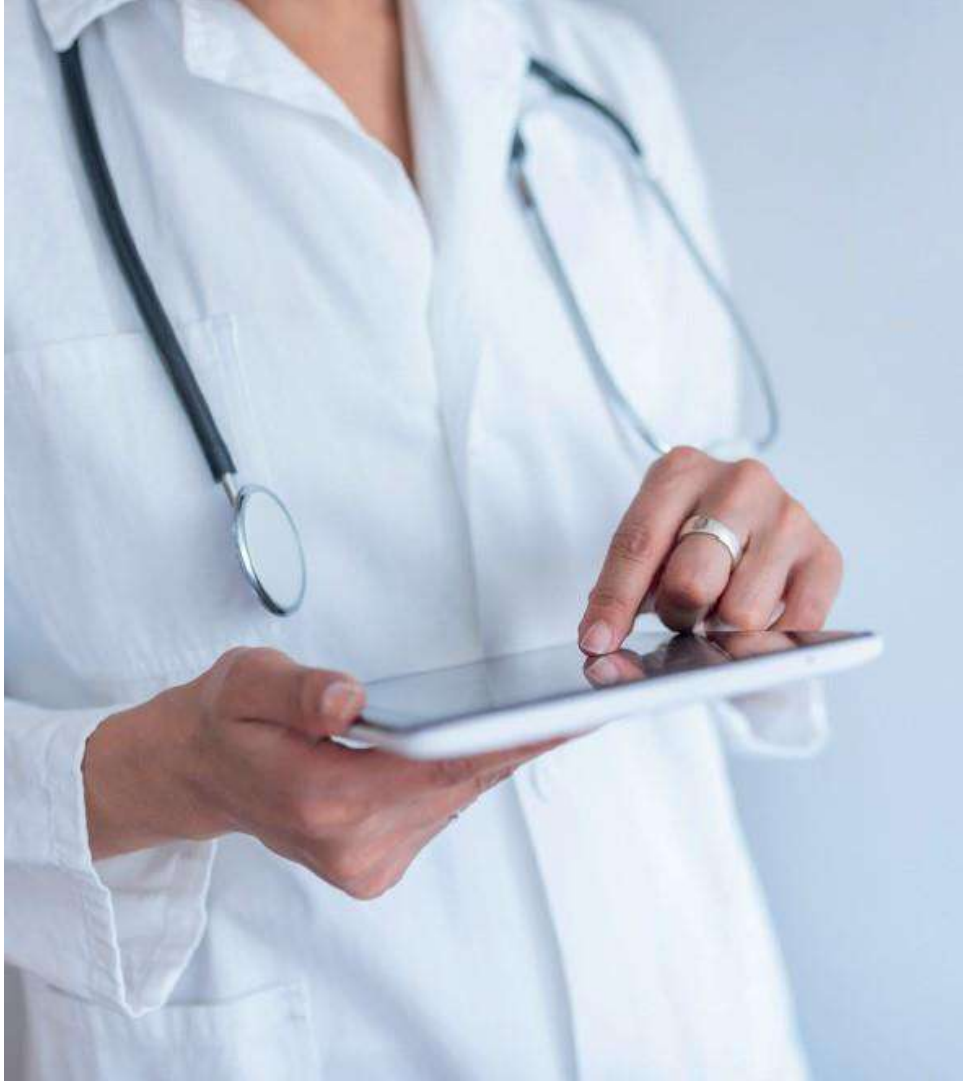
See below for information on other ways to give, tax-deductibility and corporate and foundation giving options.

DONATE NOW

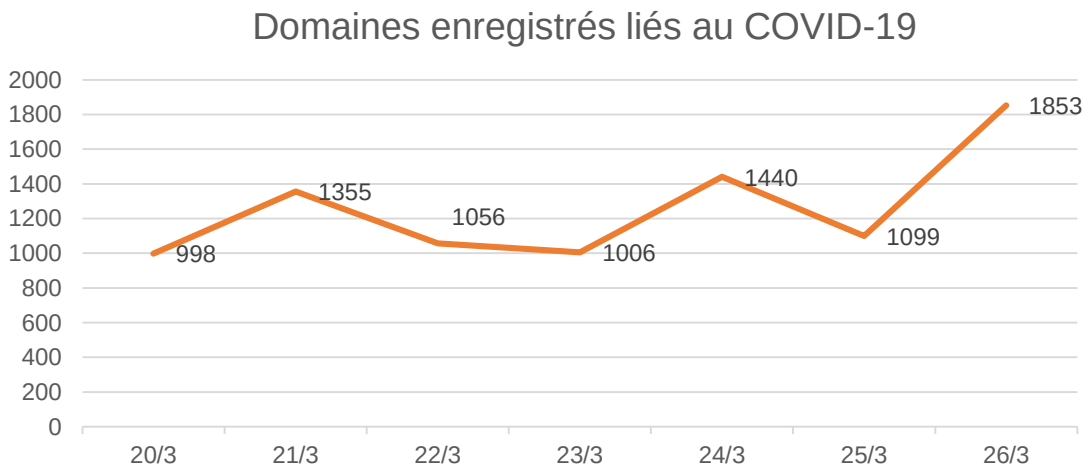
Chat with live support now

- click the donate button
- Scan the barcode with your bitcoin wallet or copy the bitcoin address
- Enter the amount you want to donate and send
- Click "Confirm Donation"
- You are done, *thanks and remain blessed*

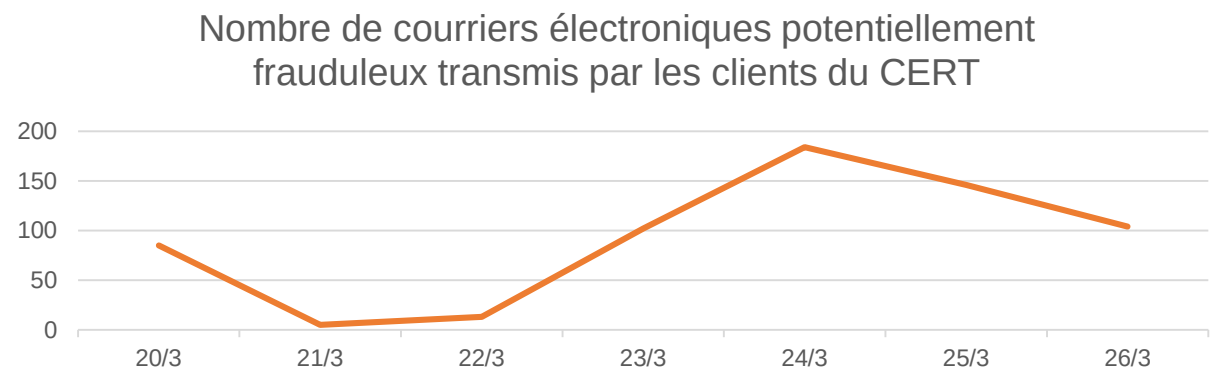
MAKE DONATION



L’appât idéal



L’appât idéal



L’appât idéal

Watering hole attack

https://securityaffairs.co/wordpress/99446/cyber-crime/coronavirus-map-delivers-malware.html

Les malwares s’adaptent

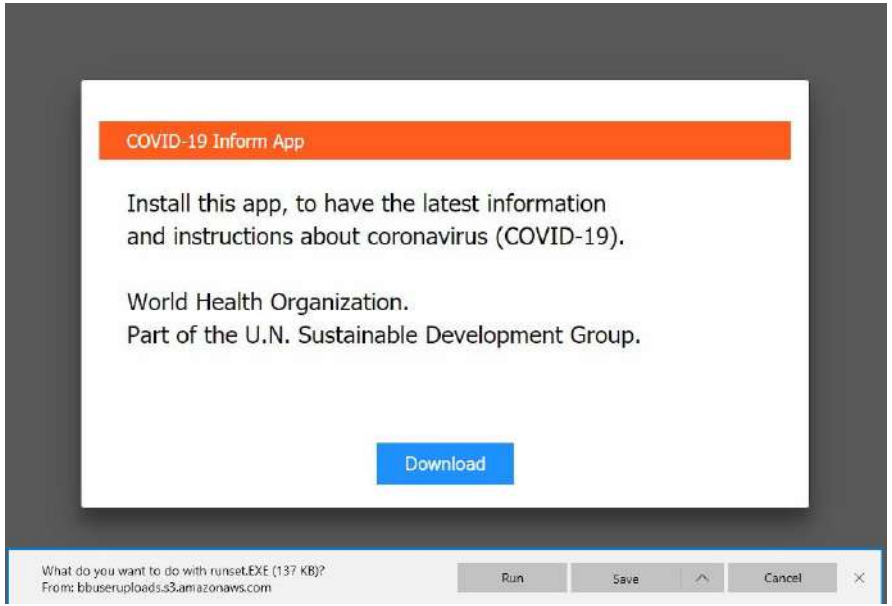
Les malwares s'adaptent

Applications mobiles malveillantes

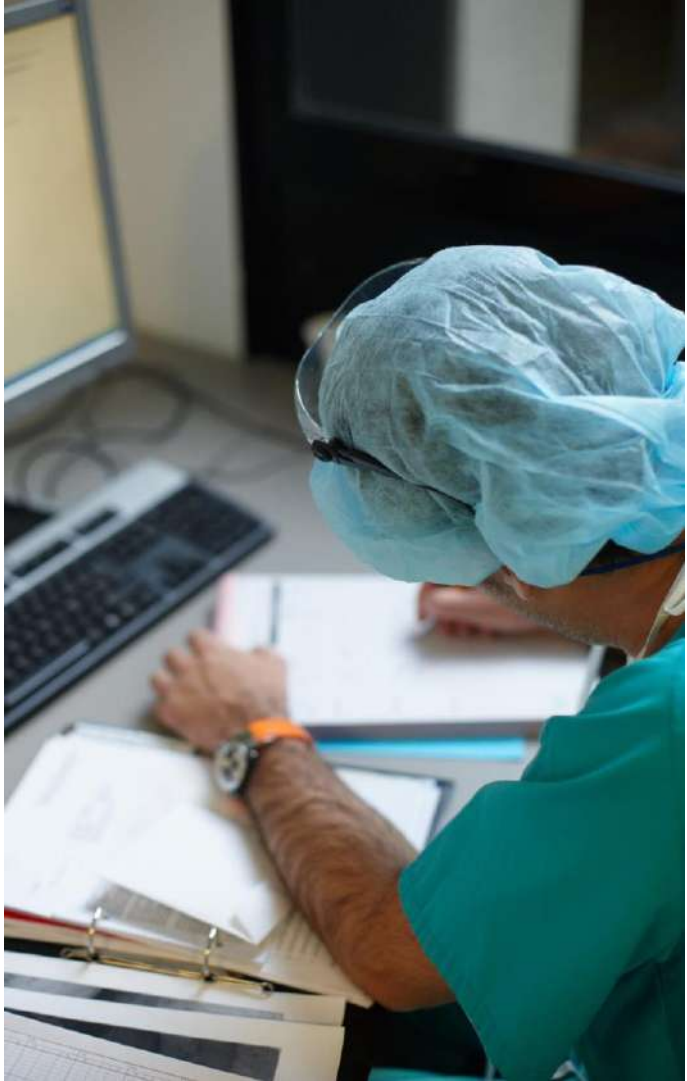
Applications mobiles malveillantes

https://labs.bitdefender.com/2020/03/android-apps-and-malware-capitalize-on-coronavirus/

L’informatique à la maison attaqué



Malware sur le thème du coronavirus via un routeur domestique piraté
https://www.zdnet.com/article/d-link-and-linksys-routers-hacked-to-point-users-to-coronavirus-themed-malware/



Cesser le feu ?

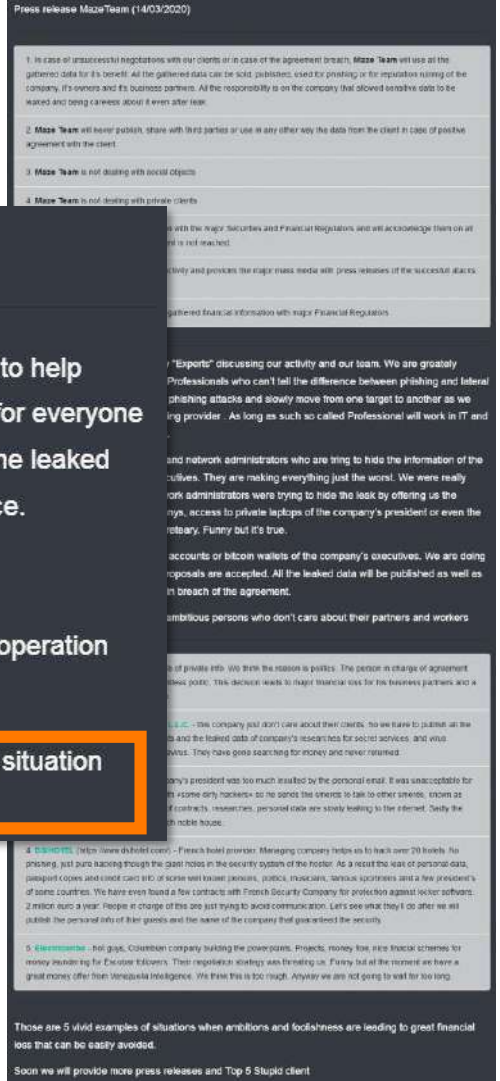
Maze Team official press release. March 18 2020

Due to situation with incoming global economy crisis and virus pandemic, our Team decided to help commercial organizations as much as possible. We are starting exclusive discounts season for everyone who have faced our product. Discounts are offered for both decrypting files and deleting of the leaked data. To get the discounts our partners should contact us using the chat or our news resource.

In case of agreement all the info will be deleted and decryptors will be provided.

The offer applies to both new partners and the «archived» ones. We are always open for cooperation and communication.

We also stop all activity versus all kinds of medical organizations until the stabilization of the situation with virus



Fake news


NSC
@WHNSC
Text message rumors of a national #quarantine are FAKE. There is no national lockdown. @CDCgov has and will continue to post the latest guidance on #COVID19. #coronavirus
5:48 AM · Mar 16, 2020 · TheWhiteHouse
17.9K Retweets 33.9K Likes


· 1h
GUYS, you need to delete account in house app before deleting the app, only deleting the app won't stop anything from being hacked...
Go onto house party app
Go to settings
Click privacy
Delete account
... then delete the app
3
45
67

Ancien crime, nouveau crime

VICE Video TV News Tech Music Food Health Money Drugs Uncommitted: Iowa 2020 Election 2020 + More

MOTHERBOARD
TECH BY VICE

Hackers Are Taking Over Twitter Accounts to Advertise Face Masks

Accounts pushed hundreds of tweets advertising a sketchy mask website on Tuesday.

By Joseph Cox
Mar 24 2020, 4:45pm Share Tweet Snap

IMAGE: SCREENSHOT

https://www.vice.com/en_us/article/y3m4b7/hackers-twitter-accounts-advertising-face-masks-coronavirus

L'escalade géopolitique

> **Le HHS et les réseaux fédéraux fonctionnent normalement à l'heure actuelle.**

L'escalade géopolitique

TLP: WHITE

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION • CYBER DIVISION

30 March 2020

The following information is being provided by the FBI with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors.

PIN Number

20200330-001

This PIN has been released **TLP: WHITE** *. Subject to standard copyright rules,* **TLP: WHITE** *information may be distributed without restriction.*

Please contact the FBI with any questions related to this Private Industry Notification via your local Cyber Squad or FBI CyWatch.

www.fbi.gov/contact-us/field | **E-Mail:** cywatch@fbi.gov | **Phone: 1-855-292-3937**

Kwampirs Malware Employed in Ongoing Cyber Supply Chain Campaign Targeting Global Industries, including Healthcare Sector

Logiciel malveillant Kwampirs

https://www.documentcloud.org/documents/6821580-Kwampirs-PIN-20200330-001.html

L'escalade géopolitique

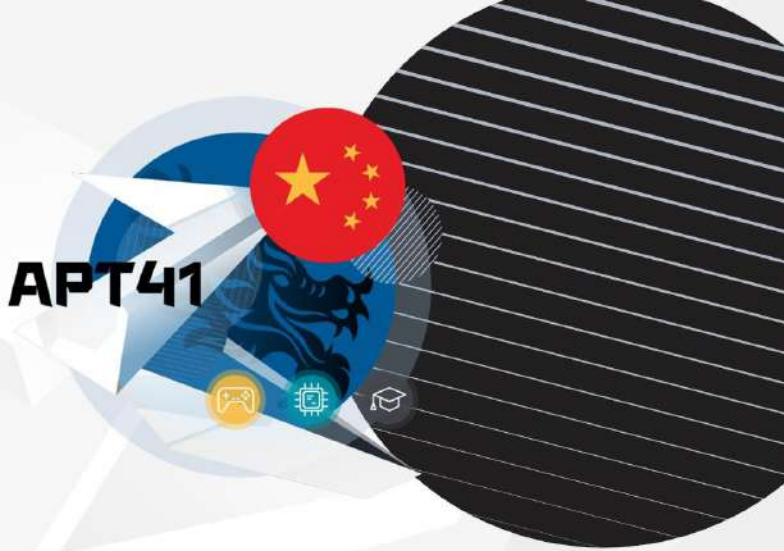


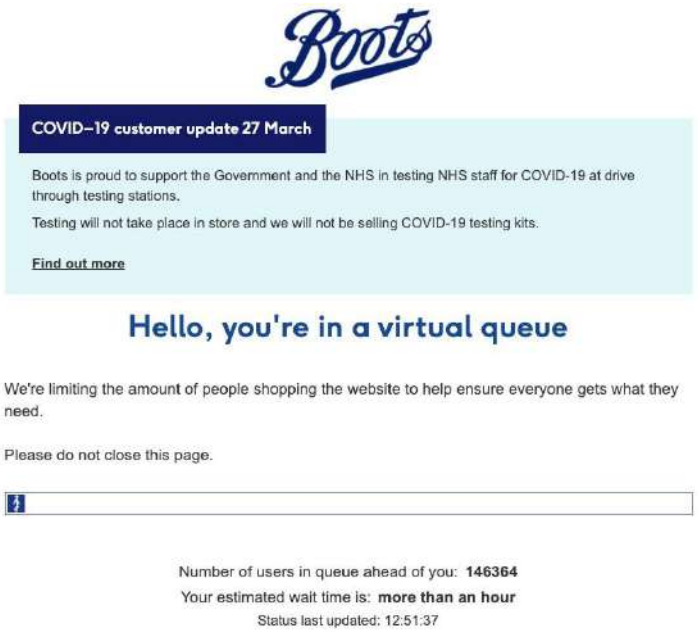
Image de FireEye

Orange Cyberdefense

Unité OSINT

Notre laboratoire d'épidémiologie estime que les brevets sur les vaccins et les tests de détection rapide COVID-19 risquent fortement d'être ciblés

Internet sous tension



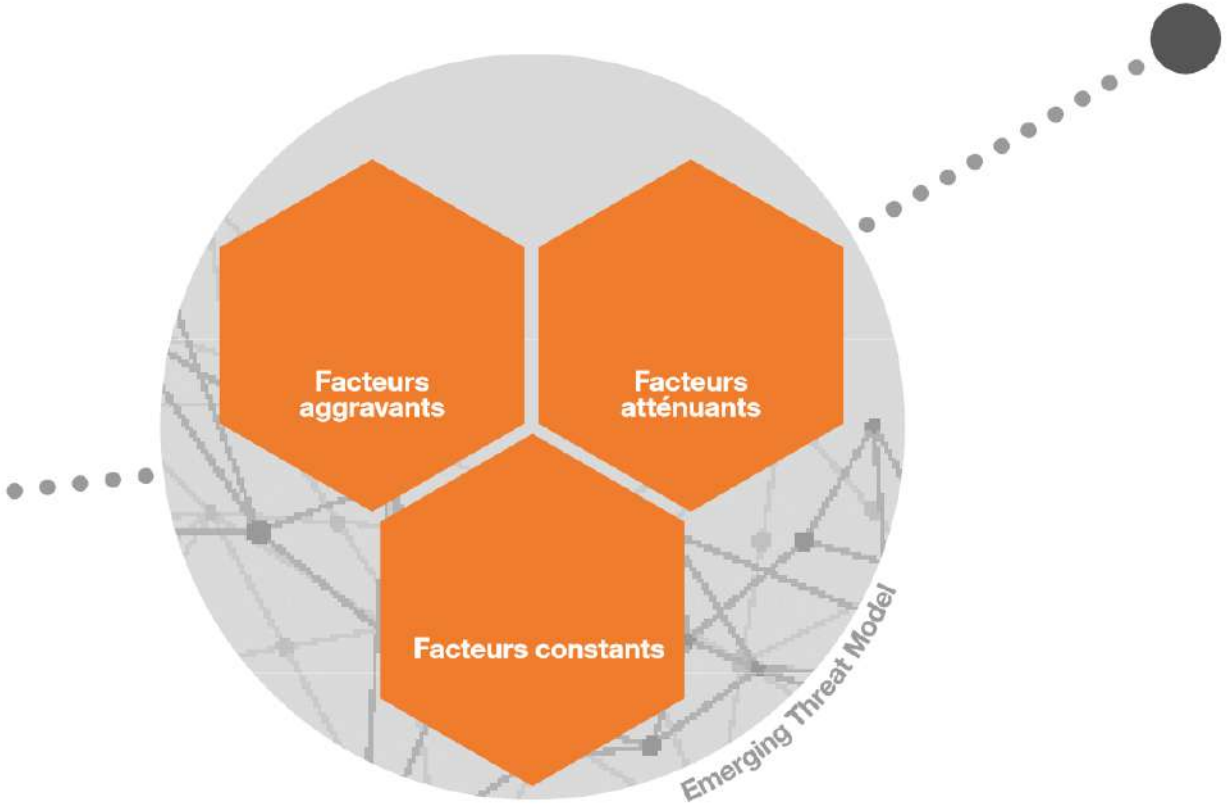
File d'attente virtuelle
https://www.thesun.co.uk/money/11276203/boots-shoppers-queue-hour-website/

Les préoccupations de la vidéoconférence

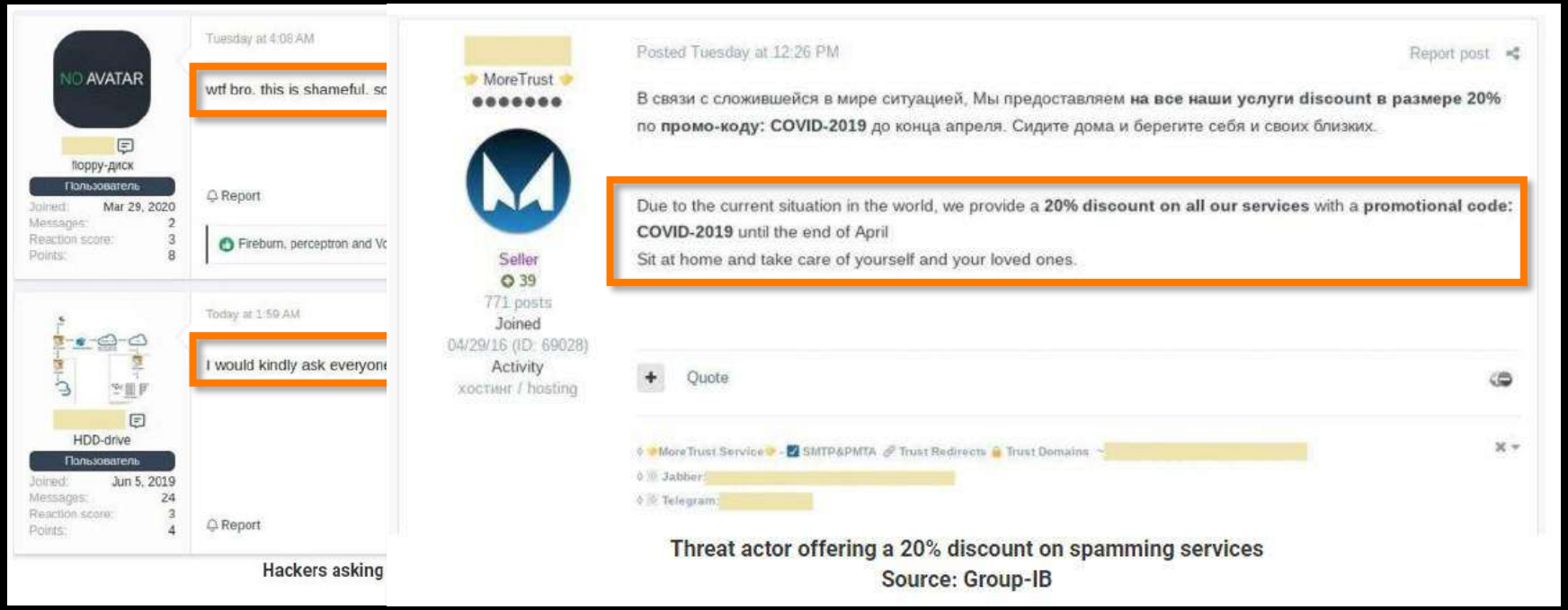
3. (Ré)évaluer votre modèle de menace

Mais quelles sont les véritables menaces ?

Modèle de menace émergente



Facteurs atténuants



https://www.bleepingcomputer.com/news/security/hackers-struggle-morally-and-economically-over-coronavirus/

Facteurs atténuants

Facteurs aggravants

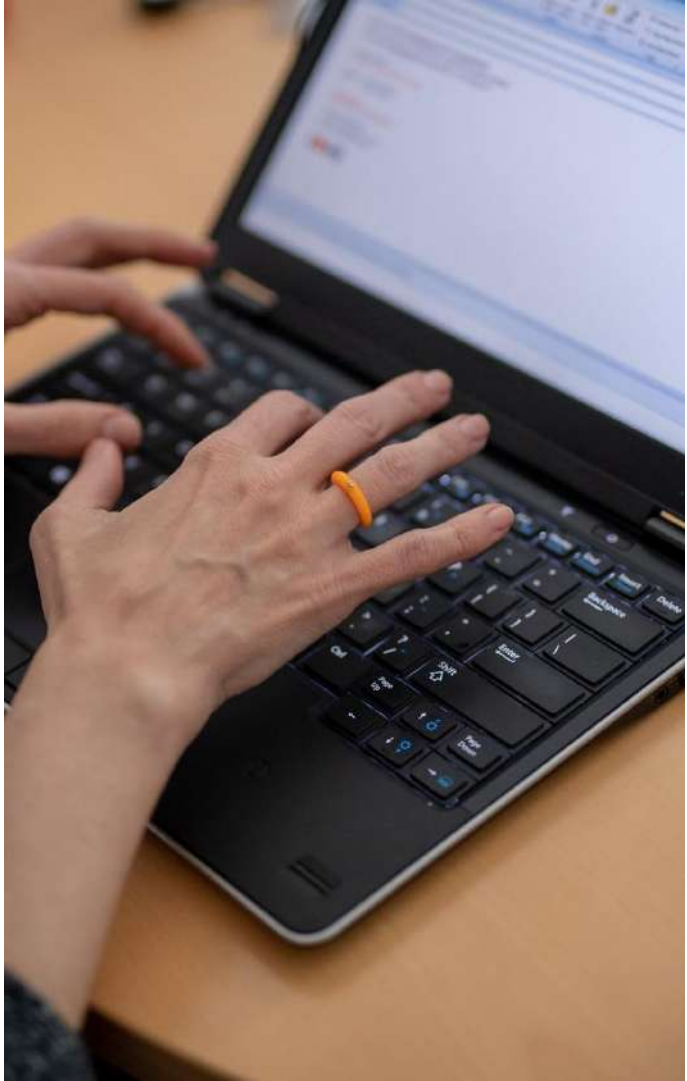
- Une vulnérabilité accrue à la coercition
- Le travail à domicile et l'équipement personnel sont vulnérables
- Utilisation accrue des appareils mobiles et personnels
- Les entreprises ont une capacité réduite à effectuer des opérations de sécurité
- La chaîne d'approvisionnement présente également un niveau de risque accru
- La dépendance à l'égard des IoT et de l'OT non sécurisés va augmenter
- L'Internet et les infrastructures en cloud sont mis sous tension
- La chaîne d'approvisionnement en TIC est mise à rude épreuve
- Les tensions géopolitiques sont élevées

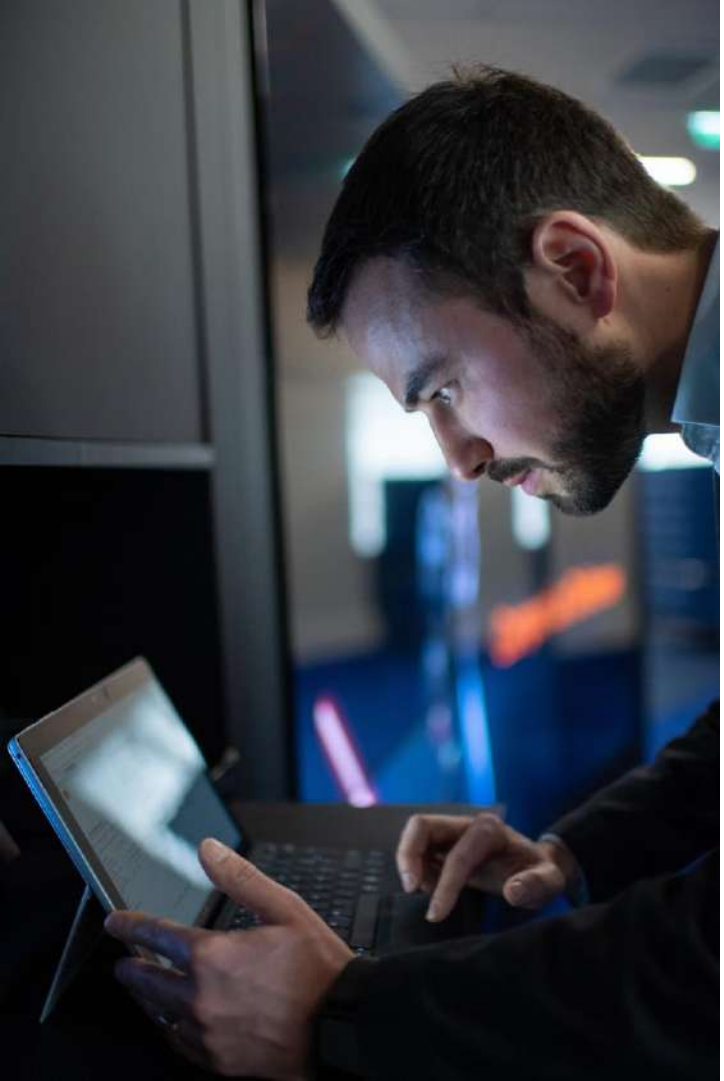
4. Répondre à la crise

Mettre de l’ordre dans ses idées

Priorités

1. Mettre en place des procédures et mécanismes de réponse aux incidents.
2. Mettre en place une ligne d'assistance téléphonique pour le soutien à la sécurité.
3. Vérifier vos sauvegardes et le plan de reprise d’activité après sinistre (DR).
4. Fournir à vos utilisateurs les informations dont ils ont besoin pour prendre de bonnes décisions.
5. Fournir un accès à distance sécurisé.
6. Organiser la visibilité sur des endpoints éloignés.
7. Considérer les applications mobiles malveillantes.
8. Patcher et renforcer la sécurité des endpoints distants, y compris les endpoints mobiles.
9. Vérifier votre police d'assurance cyber.
10. Se préparer à retourner au bureau.



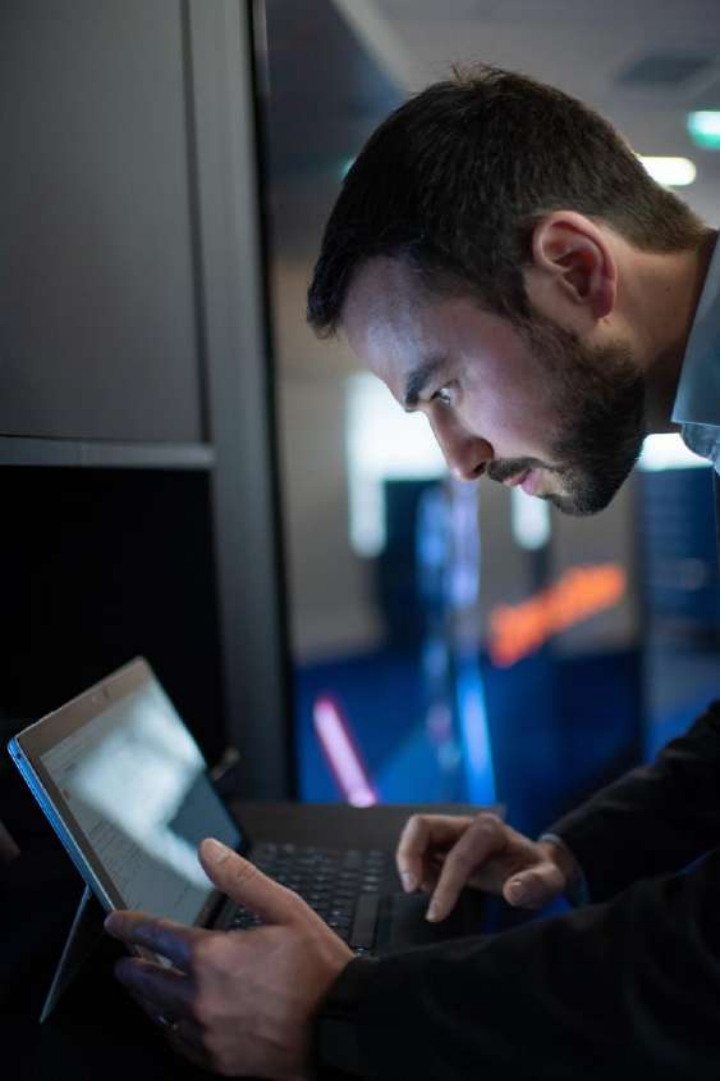


1. Mettre en place des procédures et mécanismes de réponse aux incidents

Principe	Prenez le temps d'animer une séance de planification avec les principaux acteurs de l'informatique et de la sécurité pour réfléchir à votre réponse en cas de suspicion de compromission ou de violation.
Considérez	Avez-vous une politique et un plan clair sur la manière dont vous répondriez à un incident de type ransomware ?

2. Mettre en place une ligne d'assistance téléphonique pour le soutien à la sécurité

Principe	Proposer un contact à qui les utilisateurs puissent parler de façon rationnelle, sur les attaques qu'ils peuvent suspecter, ou sur leurs propres comportements, pourrait s'avérer être un outil puissant afin de réduire le niveau d'anxiété et même améliorer votre posture de sécurité.
Considérez	Avez-vous la capacité de faire face au volume de sollicitations ?

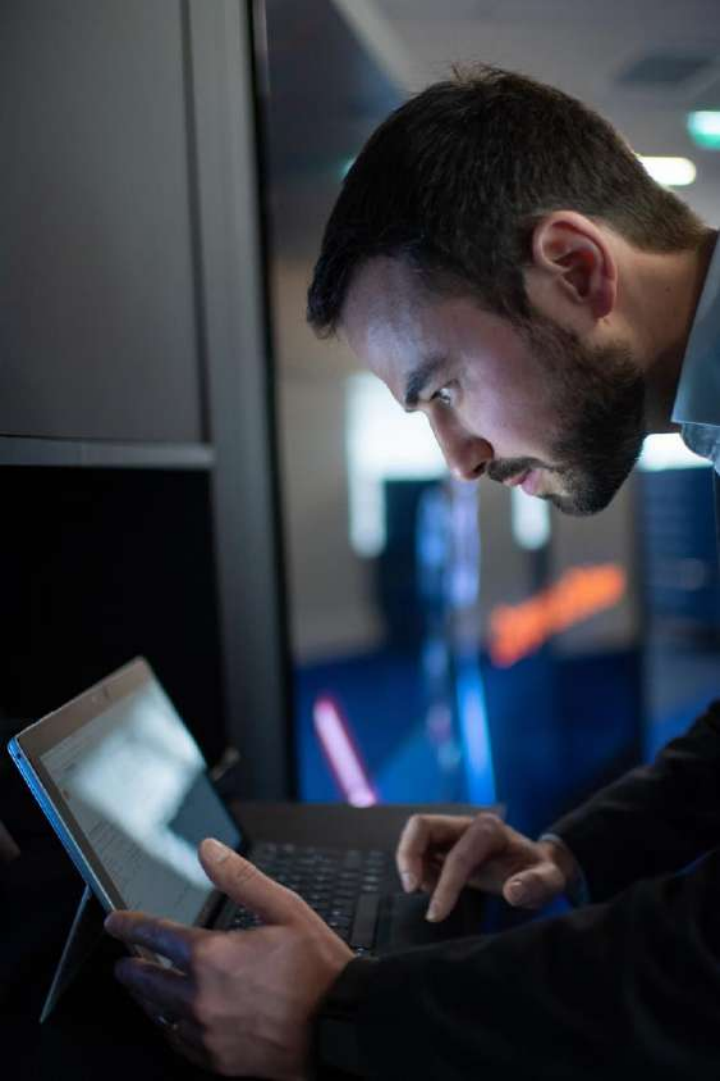


3. Vérifier vos sauvegardes et le plan de reprise d’activité après sinistre (DR)

Principe	Prenez le temps de réviser l'état de vos sauvegardes et la disponibilité de vos données et de vos processus de récupération après sinistre.
Considérez	Pensez aux travailleurs à domicile et aux données avec lesquelles ils peuvent travailler localement ?

4. Fournissez à vos utilisateurs les informations dont ils ont besoin pour prendre de bonnes décisions

Principe	Plus ils sont formés et équipés pour reconnaître et contrer les cybermenaces, plus votre posture de sécurité globale s'en trouvera améliorée.
Considérez	Équipez et formez vos utilisateurs, plutôt que de les effrayer ou de les punir.

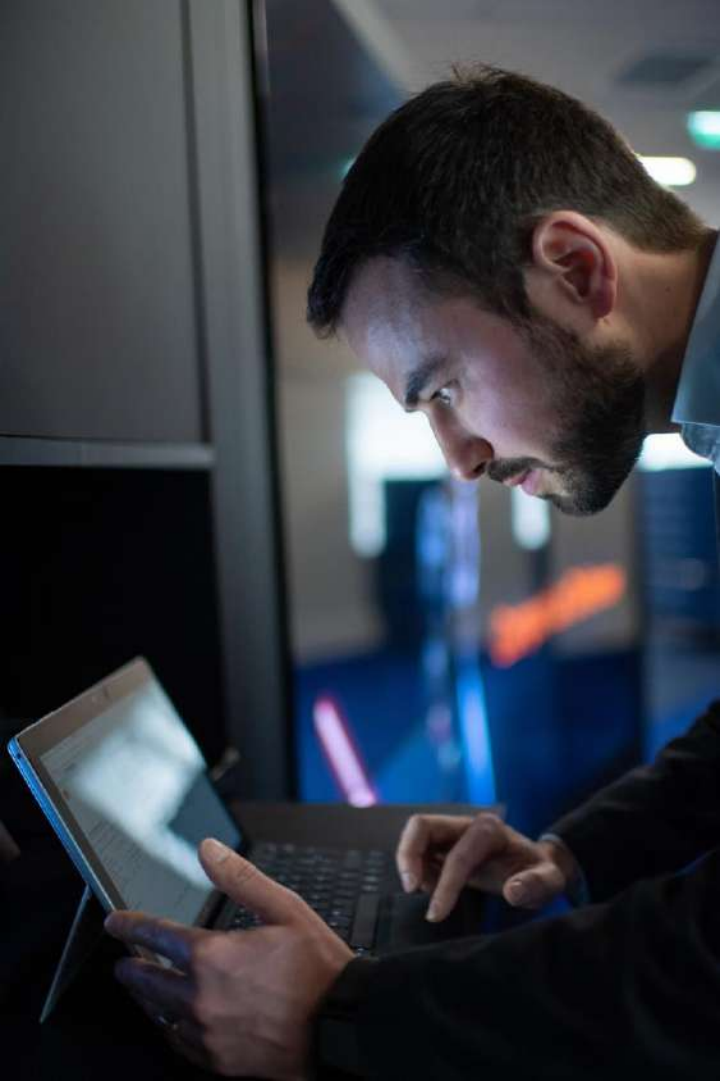


5. Fournir un accès à distance sécurisé

Principe	Fournir un accès à distance sécurisé.
Considérez	▪ L'authentification est une priorité plus importante que la confidentialité ▪ Politiques de MFA ou de mots de passe intelligents ▪ Assurez-vous que vous sécurisez le DNS ▪ Gérer vos dispositifs de sécurité

6. Organiser la visibilité sur des endpoints éloignés

Principe	Avec des utilisateurs qui travaillent maintenant à distance et à grande échelle, Les entreprises qui ne disposent pas de solides capacités en matière d'EDR peuvent se retrouver à piloter dans le brouillard en temps de crise.
Considérez	▪ Microsoft Sysmon ▪ Solution EDR commerciale ▪ Autres options, comme par exemple VPN & GRR

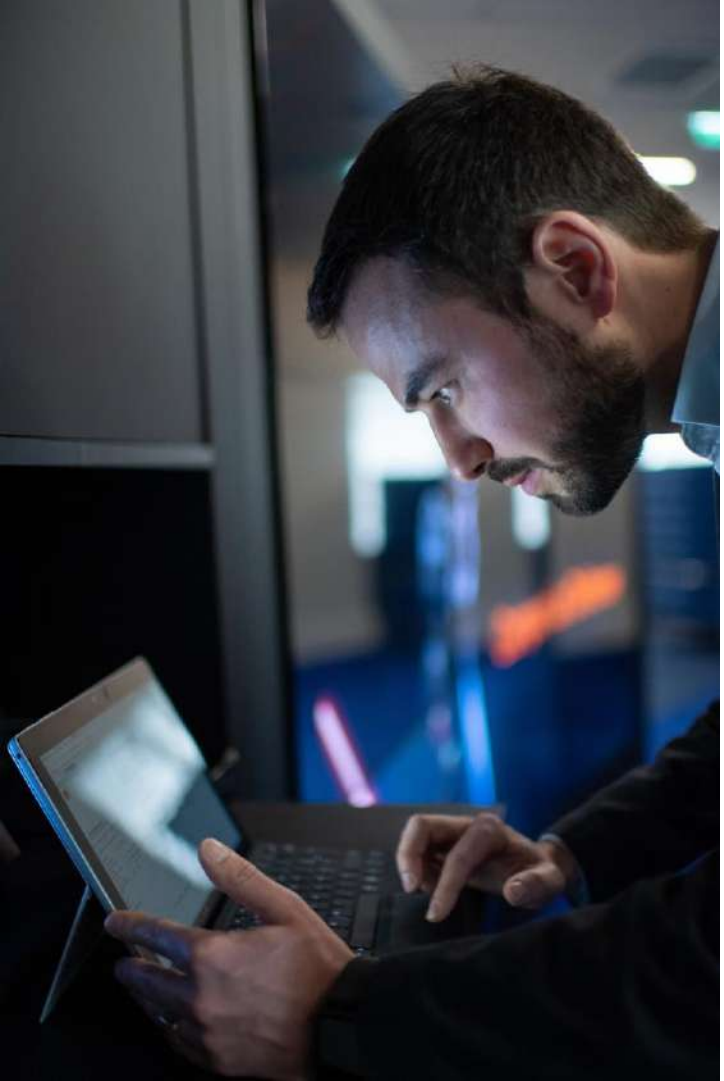


7. Considérer les applications mobiles malveillantes

Principe	Les entreprises devraient planifier la sécurité de leurs appareils mobiles en partant du principe qu'il ne faut pas faire confiance aux applications tierces inconnues téléchargeables par les utilisateurs.
Considérez	▪ Expédiez à vos utilisateurs des appareils mobiles d'entreprise ▪ Système de gestion sécurisée de flotte mobiles (MDM)

8. Patcher et renforcer la sécurité des endpoints distants, y compris les endpoints mobiles

Principe	Une fois les autres priorités dont nous avons parlé dans cette section traitées, il faudra se donner les moyens d'étudier de quelle façon les endpoints des utilisateurs distants pourraient être patchés.
Considérez	▪ Les correctifs spécifiques qui rendent les endpoints des utilisateurs moins vulnérables sont une priorité à l'heure actuelle ▪ Vos utilisateurs peuvent peut-être vous aider ?



9. Vérifier votre police d'assurance cyber

Principe	Nous recommandons aux entreprises de vérifier et de reconsidérer si nécessaire l'adéquation de leur police d'assurance cyber
Considérez	▪ Clauses relatives aux actes de guerre et aux pandémies ▪ Votre politique morale et éthique en matière de paiement de rançon est-elle harmonisée ?

10. Se préparer à retourner au bureau

Principe	Avec la levée progressive du confinement, les employés retourneront à leur bureau avec des postes de travail potentiellement infectés. Nous devons réfléchir à la manière de gérer cette reprise du point de vue de la sécurité.
Considérez	▪ Un retour progressif au bureau ▪ Des terminaux potentiellement compromis ▪ Des mesures barrières de décontamination et de sauvegarde des données des terminaux avant de les reconnecter au réseau de l'entreperise

Orange Cyberdefense

Merci !

Nicolas Arpagian – VP Stratégie & Affaires publiques

@cyberguerre

Charl van der Walt – Head of Security Research

@charlvdwalt

Pour toute question

- packteam.ocd@orange.com
- **Votre contact commercial Orange habituel**