

COVID-19

Quand un risque biologique devient numérique

Analyser la crise dans la crise



Nicolas Arpagian – VP Stratégie & Affaires publiques



@cyberguerre

[OrangeCyberdefense.com](https://www.OrangeCyberdefense.com)

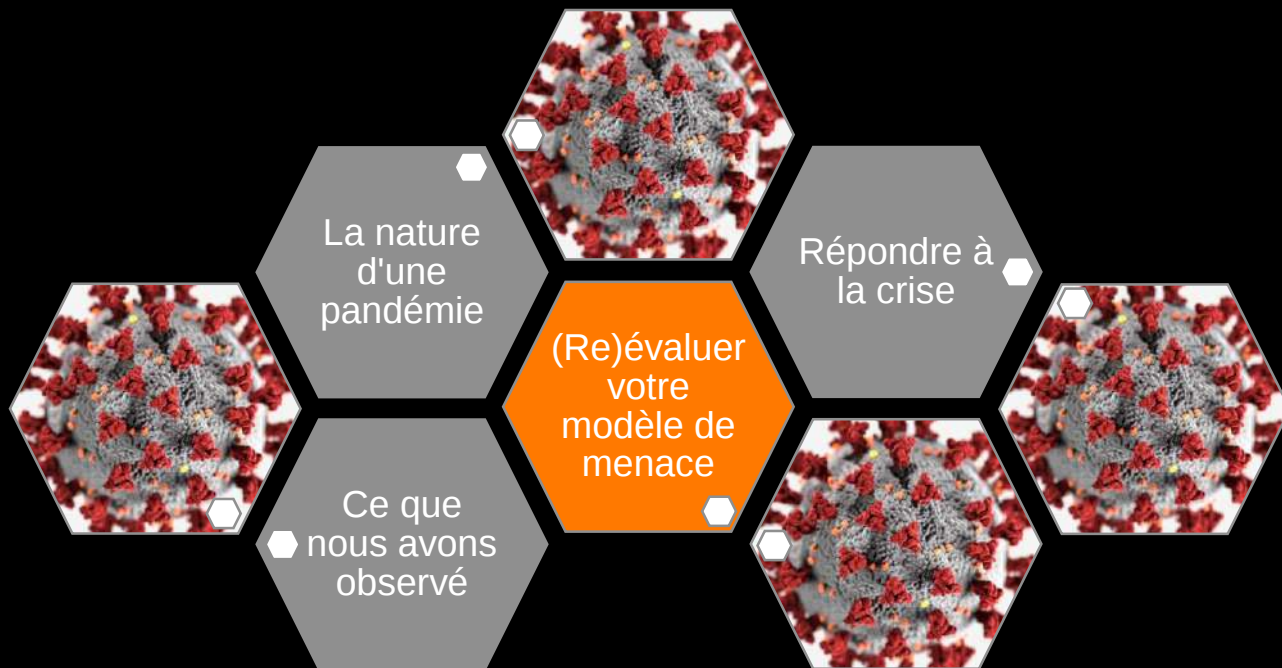


Avec nos remerciements

- 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



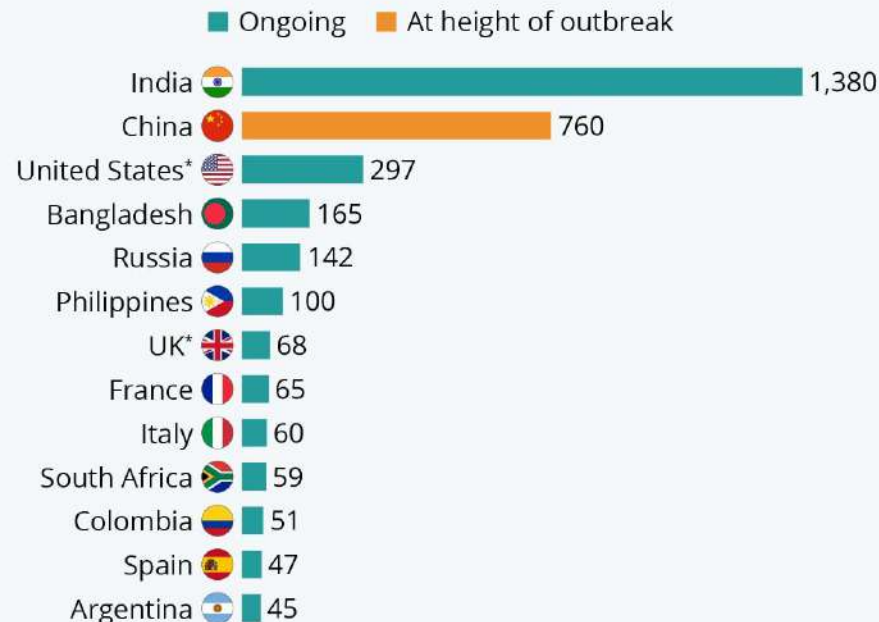
1. La nature d'une pandémie



“Untiers”.

The Size of Coronavirus Lockdowns

Number of people placed on enforced lockdown due to the coronavirus pandemic, per country (in million people)



* At least partly enforced

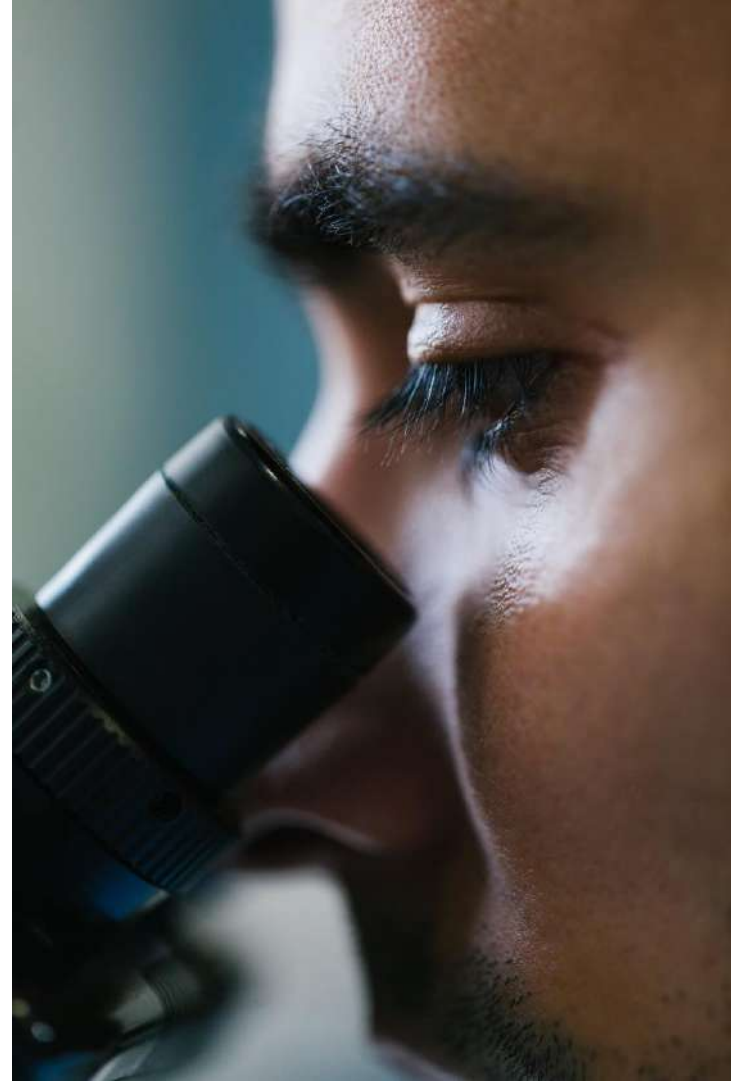
Source: Media reports



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

- 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*

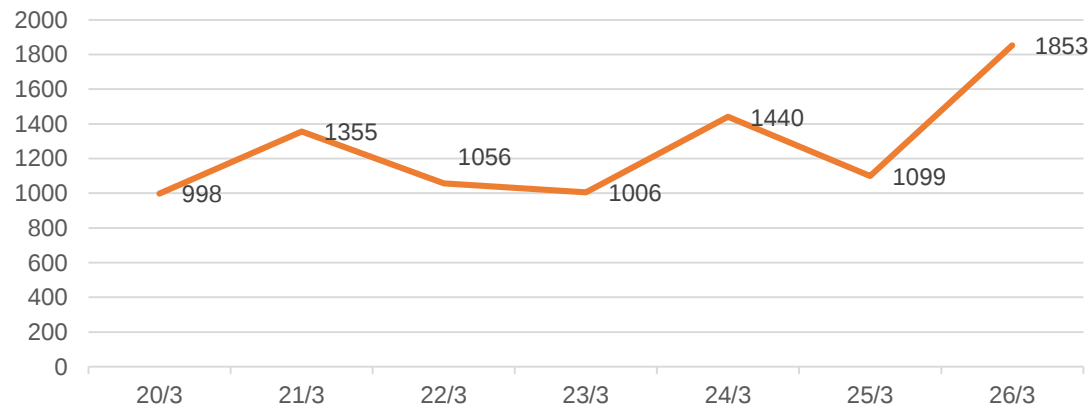
MAKE DONATION

Chat with live
support now



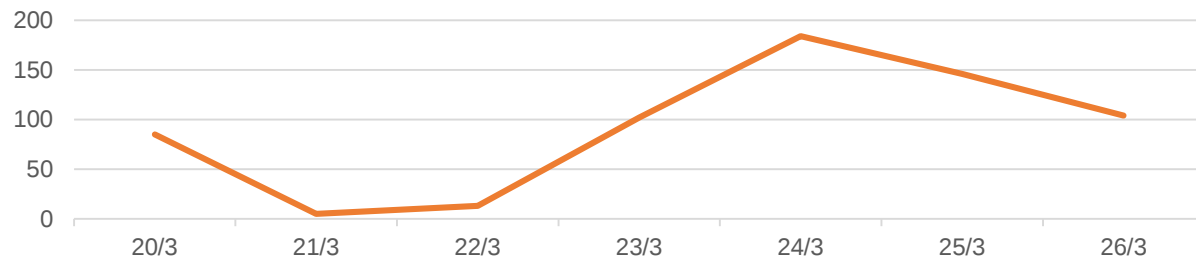
L'appât idéal

Domaines enregistrés liés au COVID-19



L'appât idéal

Nombre de courriers électroniques potentiellement frauduleux transmis par les clients du CERT



L'appât idéal



Les malwares s'adaptent



Les malwares s'adaptent



COVID-19-CRYPT

C/ASM Powerful Runtime Crypter



About

Covid-19-Crypt is a unique crypter offering the best cryptography has. It is written in C/ASM, and is a Native output. It's purpose is to deliver files in a completely undetected way, both runtime and scantime. Uniquely equipped with a Ring3-unhooker engine, this crypter will not only deliver your payload undetected, but make your payload more powerful once executing. Fully bypasses Ring-3 hooks and does not trigger Ring-0 hooks.



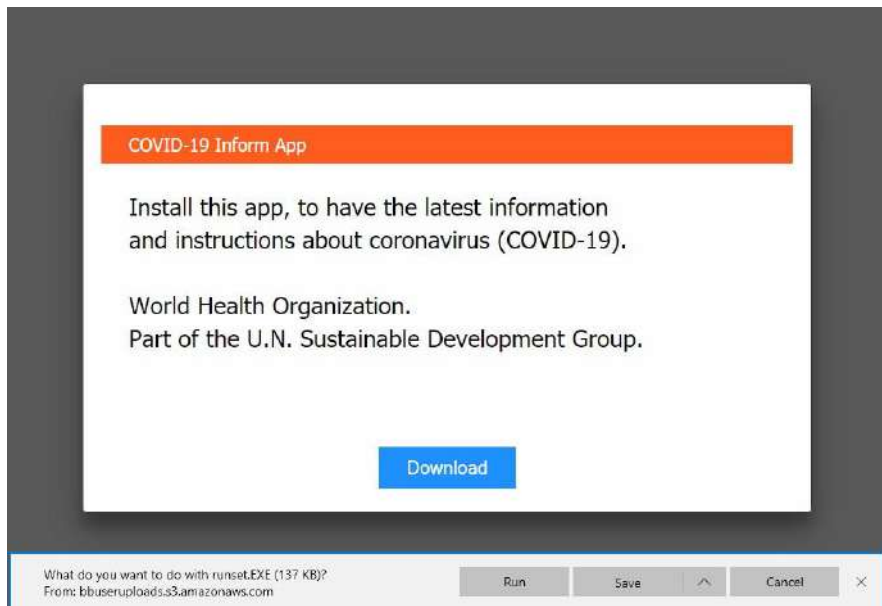
Applications mobiles malveillantes



Applications mobiles malveillantes

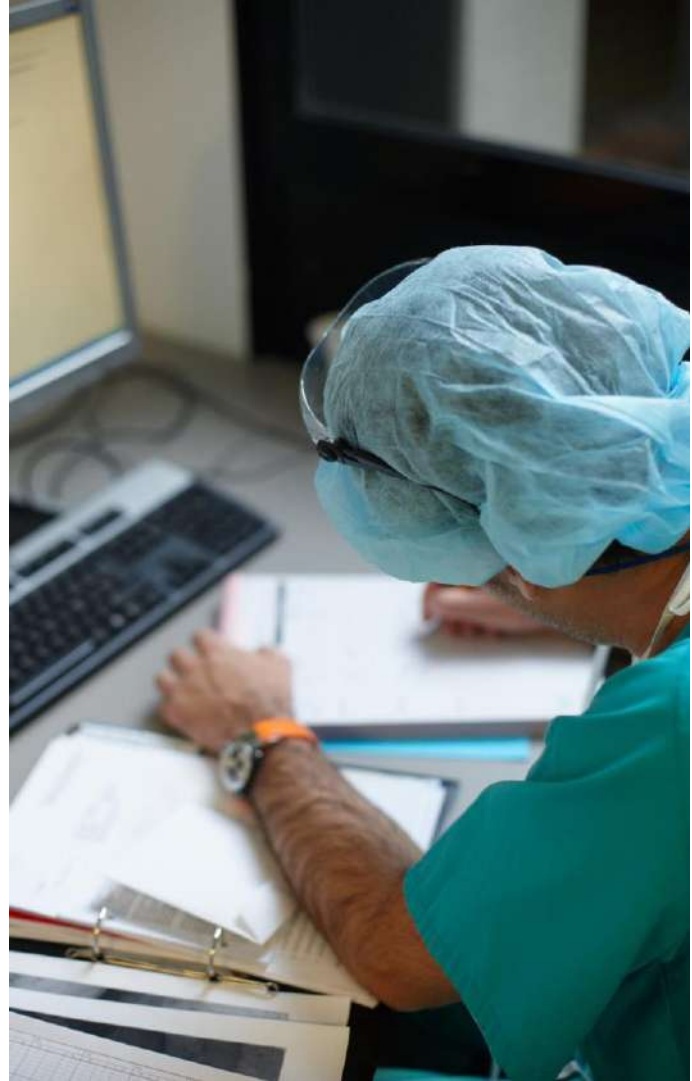
<https://labs.bitdefender.com/2020/03/android-apps-and-malware-capitalize-on-coronavirus/>

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

Press release MazeTeam (14/03/2020)

1. In case of unsuccessful negotiations with our clients or in case of the agreement breach, Maze Team will use all the gathered data for its benefit. All the gathered data can be sold, published, used for printing or for impersonation spoofing of the company, its owners and its business partners. All the responsibility is on the company that allowed sensitive data to be leaked and being careless about it even after leak.
2. Maze Team will never publish, share with third parties or use in any other way the data from the client in case of positive agreement with the client.
3. Maze Team is not dealing with social objects.
4. Maze Team is not dealing with private clients.

with the major Securities and Financial Regulation, and we acknowledge them on all and is not reached.

activity and provides the major mass media with press releases of the successful status.

gathered financial information with major Financial Regulation.

/"Experts" discussing our activity and our team. We are greatly Professionals who can't tell the difference between phishing and lateral chaining attacks and slowly move from one target to another as we long provider. As long as such so called Professional will work in IT and

and network administrators who are trying to hide the information of the culprits. They are making everything just the worst. We were really work administrators were trying to hide the leak by offering us the ngs, access to private laptops of the company's president or even the rotary. Funny but it's true.

accounts or bitcoin wallets of the company's executives. We are doing proposals are accepted. All the leaked data will be published as well as in breach of the agreement.

ambitious persons who don't care about their partners and workers

of private info, also from the reason is politics. The person in charge of agreement (this point), this decision leads to major material loss for his business partners and a

U.S.A.C. - this company just don't care about their clients, no we have to publish on the ts and the leaked data of company's researchers for social services, and virus virus. They have gone searching for money and never returned.

company's president was too much involved by the personal email. It was unacceptable for us, some dirty hackers- so he sends the offering to take to other servers, known as if correctly, researchers, personal data are slowly looking to the internet. Sadly the noble house.

4. DISHOTES (Mijn domein dubbel.com) - French hotel provider. Managing company helps us to hack over 20 hotels. No pricing, just pure backing through the giant holes in the security system of the hotel. As a result the leak of personal data, passport copies and credit card info of some well known persons, public, musicians, famous sportsmen and a few presidents of some countries. We have even found a few contacts with French Security Company for protection against cyber software. 2 million euro a year. They're in charge of the job just trying to avoid communication. Let's see what they do after we will publish the personal info of their guests and the name of the company that guaranteed the security.

5. Eleonorestele - Not gay, Colombian company building the powerplants. Projects, money flow, nice financial schemes to money laundering for Ecuador followers. Their regulator strategy was trending us. Funny, but all the moment we have a great money offer from Venezuela intelligence. We think this is too rough. Anyway we are not going to wait for too long.

Those are 5 vivid examples of situations when ambitions and foolishness are leading to great financial loss that can be easily avoided.

Soon we will provide more press releases and Top 5 Stupid client

Fake news



Ancien crime, nouveau crime



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



The image shows a 'Private Industry Notification' card from the FBI Cyber Division. The card has a dark blue background with a geometric pattern. At the top left is the FBI seal. To its right, the text 'Private Industry Notification' is written in a large, stylized font. Below this, 'FEDERAL BUREAU OF INVESTIGATION • CYBER DIVISION' is printed. A date '30 March 2020' is on the left. A PIN number '20200330-001' is at the bottom left. A disclaimer paragraph is in the center. A 'TLP: WHITE' label is at the top right. At the bottom, there is contact information for the FBI, including a website, email, and phone number. The title of the notification, 'Kwampirs Malware Employed in Ongoing Cyber Supply Chain Campaign Targeting Global Industries, including Healthcare Sector', is at the very bottom.

TLP: WHITE

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION • CYBER DIVISION

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.

30 March 2020

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

Internet sous tension



COVID-19 customer update 27 March

Boots is proud to support the Government and the NHS in testing NHS staff for COVID-19 at drive through testing stations.

Testing will not take place in store and we will not be selling COVID-19 testing kits.

[Find out more](#)

Hello, you're in a virtual queue

We're limiting the amount of people shopping the website to help ensure everyone gets what they need.

Please do not close this page.



Number of users in queue ahead of you: **146364**

Your estimated wait time is: **more than an hour**

Status last updated: 12:51:37

File d'attente virtuelle

<https://www.thesun.co.uk/money/11276203/boots-shoppers-queue-hour-website/>



Les préoccupations de la vidéoconférence



Dr David Day
@drdavidjday

Avoid [#Zoom](#) unless you know how lock it down. We have just had a quick 30 minute scrum hack and found it very simple to find and join others meetings zia brute force. We also managed to take over others audio (our own in tests). This is possible even if there is a password set!

1:06 PM · Mar 26, 2020 · [Twitter for Android](#)



Dr David Day
@drdavidjday

Case in point re: [#Zoom samuraisecurity.co.uk/zoom-default-i...](#)



The Impacttologist @impacttologist · Mar 27

After a few weeks of using @zoom for small meetings, I attempted to run my first public webinar on it today.

Got hacked.

People sharing porn links & shouting obscenities.

Hit "mute all" straight away - nothing!

Had to pull the plug.

Learning; use all the security features!

10:17 AM · Mar 28, 2020 · [Twitter for Android](#)

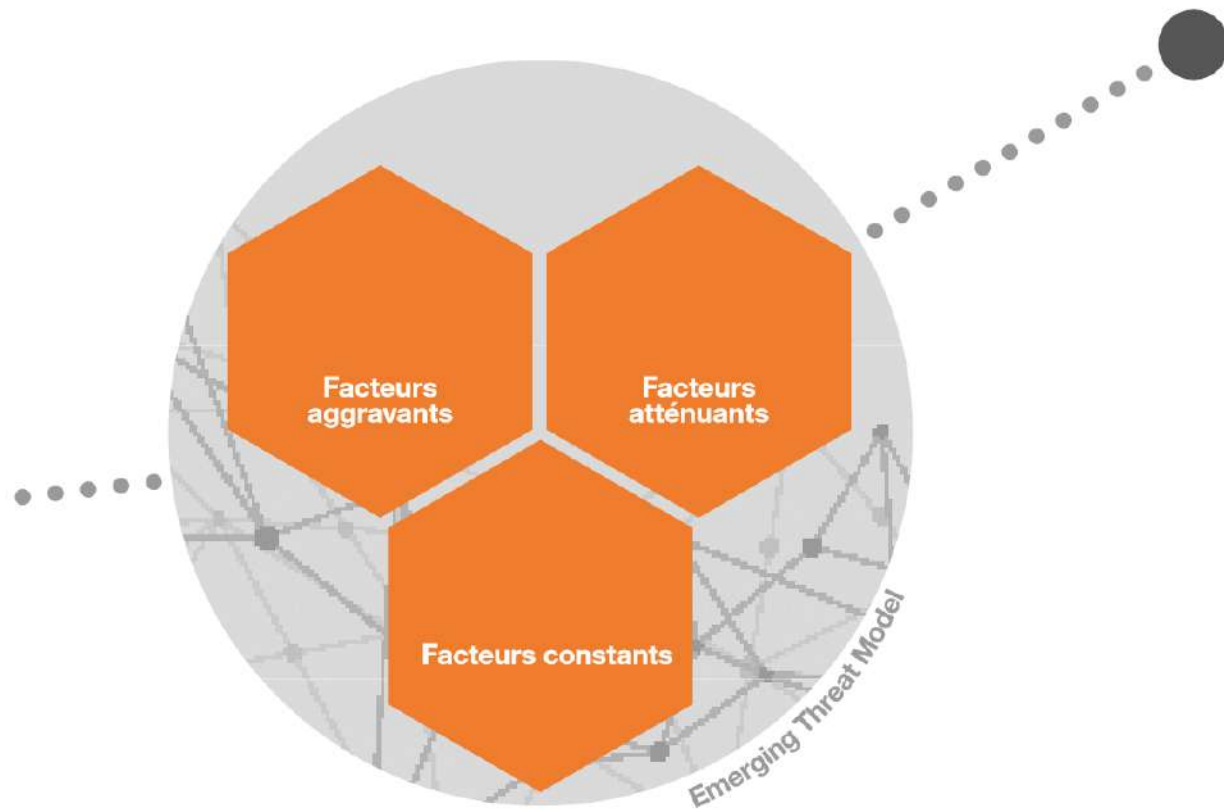
3. (Ré)évaluer votre modèle de menace



Mais quelles sont les véritables menaces ?



Modèle de menace émergente



Facteurs atténuants

NO AVATAR

Пользователь

Joined: Mar 29, 2020

Messages: 2

Reaction score: 3

Points: 8

Report

Fireburn, perceptron and V...

Today at 1:59 AM

I would kindly ask everyone

HDD-drive

Пользователь

Joined: Jun 5, 2019

Messages: 24

Reaction score: 3

Points: 4

Report

Hackers asking

Posted Tuesday at 12:26 PM

Report post

MoreTrust

В связи с сложившейся в мире ситуацией, Мы предоставляем на все наши услуги discount в размере 20% по промо-коду: COVID-2019 до конца апреля. Сидите дома и берегите себя и своих близких.

Due to the current situation in the world, we provide a 20% discount on all our services with a promotional code: COVID-2019 until the end of April.

Sit at home and take care of yourself and your loved ones.

Quote

MoreTrust Service - SMTP&PMTA Trust Redirects Trust Domains

Jabber:

Telegram:

Threat actor offering a 20% discount on spamming services

Source: Group-IB

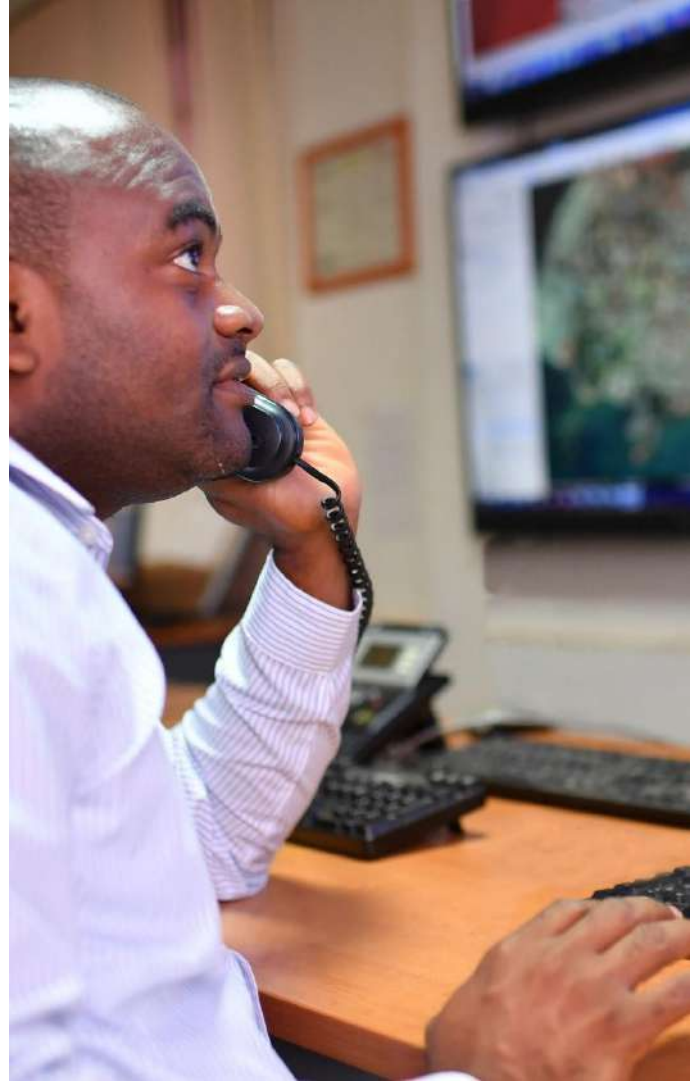
<https://www.bleepingcomputer.com/news/security/hackers-struggle-morally-and-economically-over-coronavirus/>

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

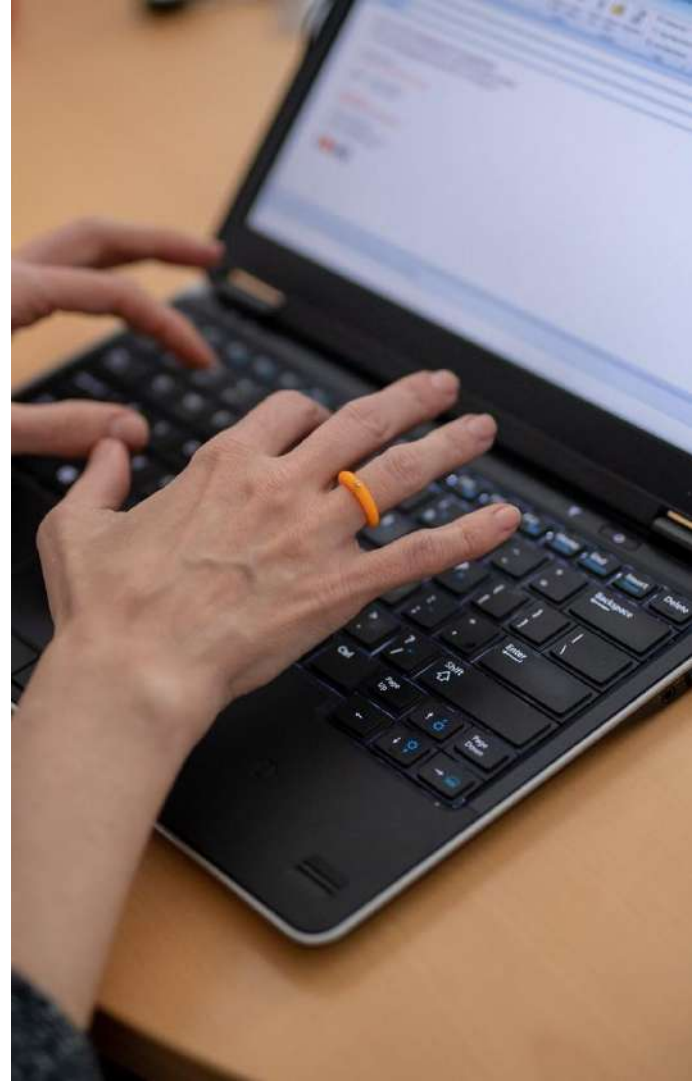


Mettre de l'ordre dans ses idées



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'entreprise



Merci !



Nicolas Arpagian – VP Stratégie & Affaires publiques

@cyberguerre



Charl van der Walt – Head of Security Research

@charlvdwalt

Pour toute question

- packteam.oed@orange.com
- Votre contact commercial Orange habituel