Cyber-menaces et Sécurité des nouvelles technologies

Gendarmerie nationale

Major Claude LAHOUSSE

Sommaire

- Statistiques générales
- Profils et motivations des cyber-attaquants
- Les différents types de menaces
- Liens utiles
- Echange / questions diverses

Gendarmerie nationale

Statistiques générales : Les pros

81%

des entreprises françaises ont été visées par une cyberattaque en 2015

9 semaines

en moyenne pour réparer les dégâts

773 000€

En moyenne pour se remettre d'une attaque

- Frais juridiques
- Compensations clients
- Ressources tiers
- Amendes & coûts de mise aux normes

Gendarmerie nationale

Statistiques générales : Les particuliers

Plus de 90 000 victimes ont été assistées sur la plateforme Cybermalveillance.gouv.fr en 2019, contre 28 855 en 2018, soit une augmentation de plus de 210%. Parmi ces victimes, 90 % sont des particuliers, souvent plus vulnérables et désarmés face aux incidents de sécurité qui les frappent.

- Il apparaît que 2021 a été une année particulièrement propice aux escroqueries, notamment par courrier électronique ou SMS. Cela s'appelle du hameçonnage, ou phishing en anglais. "Environ 2,5 millions de visiteurs se sont rendus sur cybermalveillance.gouv.fr en 2021. 1,3 million d'entre eux […] s'y sont rendus pour consulter des contenus relatifs au hameçonnage",
- Ces chiffres ne prennent pas en compte les personnes qui n'osent pas se manifester.

Profils et motivations des cyber-attaquants

LUCRATIVE

Cyber-mercenaires
Officines
Escrocs

IDÉOLOGIQUE

Hacktivistes
Cyber-terroristes
Cyber-patriotes

ÉTATIQUE

Unités spécialisées

LUDIQUE

Adolescents désœuvrés ou non (script-kiddies)

TECHNIQUE

Hackers chevronnés

PATHOLOGIQUE

Vengeurs
Employés mécontents

Gendarmerie nationale

Principaux types de menaces

- **L'hameçonnage (phishing)**
- **Les arnaques au faux support technique**
- **Les rançongiciels (ransomwares)**
- **Les arnaques au chantage à la webcam prétendue piratée**
- **Divers**

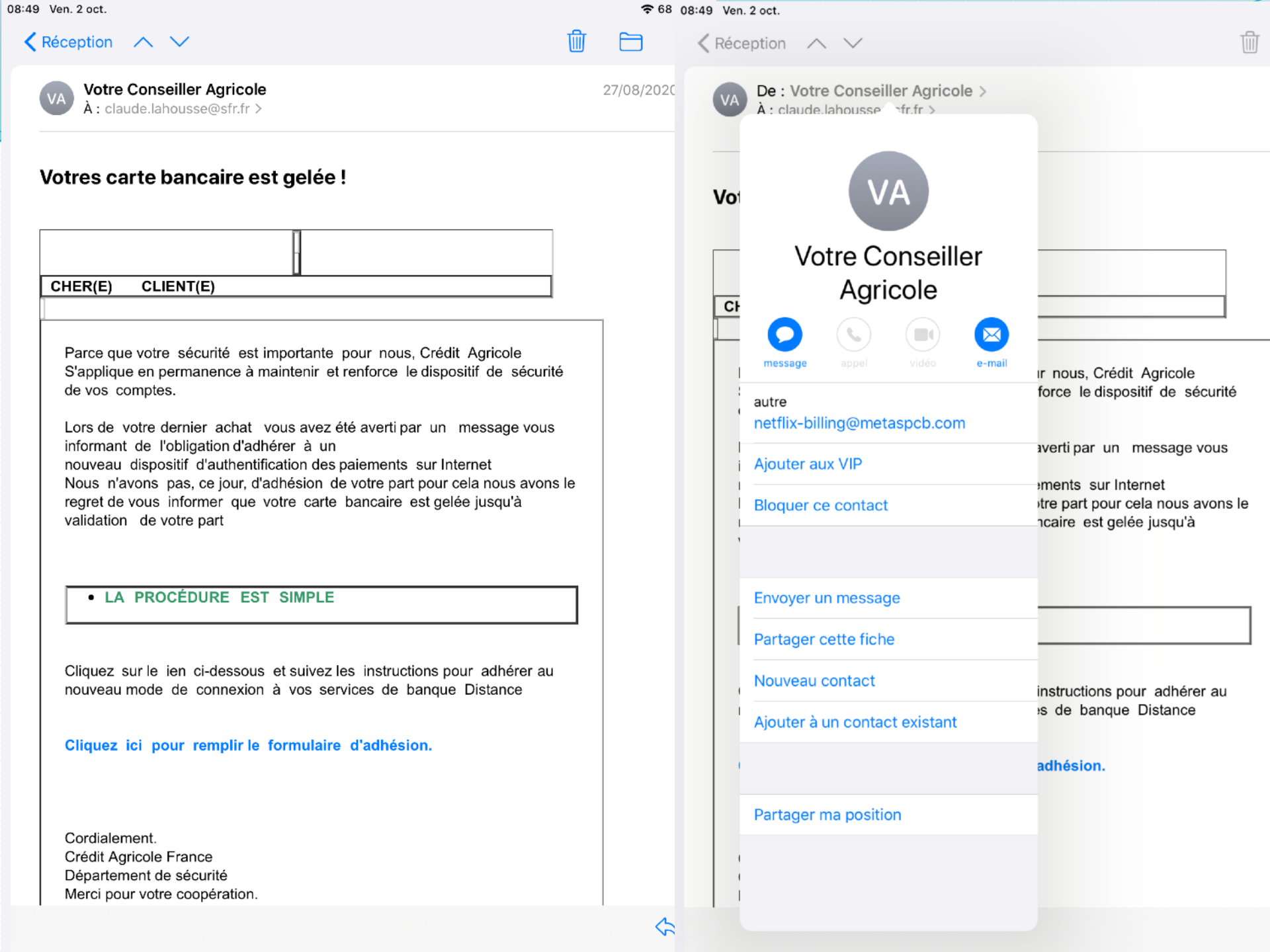
Gendarmerie nationale

L'hameçonnage (phishing)

L'hameçonnage est une technique frauduleuse destinée à leurrer l'internaute pour l'inciter à communiquer des données personnelles (comptes d'accès, mots de passe…) et/ou bancaires en se faisant passer pour un tiers de confiance. Il peut s'agir d'un faux message, SMS ou appel téléphonique de banque, de réseau social, d'opérateur de téléphonie, de fournisseur d'énergie, de site de commerce en ligne, d'administrations, etc.

Objectif : **Voler des informations personnelles ou professionnelles** (comptes, mots de passe, données bancaires…) pour en faire un usage frauduleux.

Gendarmerie nationale


08:49 Ven. 2 oct.
68
Réception
VA
Votre Conseiller Agricole
À : claude.lahousse@sfr.fr >
27/08/2020
Votres carte bancaire est gelée !
CHER(E) CLIENT(E)
Parce que votre sécurité est importante pour nous, Crédit Agricole S'applique en permanence à maintenir et renforce le dispositif de sécurité de vos comptes.
Lors de votre dernier achat vous avez été averti par un message vous informant de l'obligation d'adhérer à un nouveau dispositif d'authentification des paiements sur Internet
Nous n'avons pas, ce jour, d'adhésion de votre part pour cela nous avons le regret de vous informer que votre carte bancaire est gelée jusqu'à validation de votre part
LA PROCÉDURE EST SIMPLE
Cliquez sur le ien ci-dessous et suivez les instructions pour adhérer au nouveau mode de connexion à vos services de banque Distance
Cliquez ici pour remplir le formulaire d'adhésion.
Cordialement.
Crédit Agricole France
Département de sécurité
Merci pour votre coopération.
08:49 Ven. 2 oct.
Réception
De : Votre Conseiller Agricole >
Votre Conseiller Agricole
message
appel
vidéo
e-mail
autre
netflix-billing@metaspcb.com
Ajouter aux VIP
Bloquer ce contact
Envoyer un message
Partager cette fiche
Nouveau contact
Ajouter à un contact existant
Partager ma position

SS De : Suivi - Service-Public.fr
À : claude.lahousse@sfr.fr
aujourd'hui à 01:47

IMPORTANT ! OBTENIR VOTRE NOUVELLE CARTE VITALE V3 !

Service-Public

Chèr(e) client(e),

Nous vous informons que Le Service public, a enfin dévoilé sa nouvelle carte vitale V3. La nouvelle carte vitale bénéficie des derniéres avancées technologique en matiére de sécurité ,Fiable,pratique et sure.

OBTENIR VOTRE NOUVELLE CARTE VITALE V3.

INSCRIVERZ-VOUS EN LIGNE ?

Vous recevrez votre nouvelle carte Vitale V3 sous un délai de 24h.

SS De : Suivi - Service-Public.fr
À : claude.lahousse[illegible]sfr.fr

SS

Suivi - Service-Public.

message appel vidéo e-mail

autre
akhna@demandevitale3.com

Ajouter aux VIP

Bloquer ce contact

Envoyer un message

Partager cette fiche

Nouveau contact

Ajouter à un contact existant

ERREUR!

- Veuillez entrer une Nom valide
- Veuillez entrer une Prénom valide
- Veuillez entrer une Date de naissance valide
- Veuillez entrer une Adresse email valide
- Veuillez entrer une Mot de pass valide

Mettre à jour la carte

La mise à jour de la carte vitale doit se faire annuellement. Cette opération actualise les droits et garantit une prise en charge efficace des dépenses de santé.

Nom

PB

De : PASCAL BASTIAN >
21 septembre 2020 à 13:03

PASCAL

Salut,
J'espère que tu vas bien.
Puis-je t'ecris ?

Trouvé(e) dans la boîte Envoyés de Sfr

C

Claude
À : PASCAL BASTIAN >

21/09/2020

Oui

> Le 21 sept. 2020 à 13:03, PASCAL BASTIAN <pascal.basstian@sfr.fr> a écrit :

Plus

PB

PASCAL BASTIAN
À : Claude >

21/09/2020

Plus

PB **PASCAL BASTIAN** 21/09/2020
À : Claude >

À vrai dire, ces dernières semaines n'ont pas été faciles pour moi, des crampes intestinales et des douleurs abdominales insupportable.
Ces douleurs m'ont poussé à aller consulter un médecin qui m'a envoyé faire une coloscopie en urgence ce matin, du coup, je risque d'être bloqué quelques jours en attendant les résultats. Je croise bien les doigts dans tous les cas, je te tiendrai informer.

Je t'envoie ce message, car j'ai un petit service à te demander, j'ai du mal à trouver des coupons de recharges NEO-SURF comme je le fais habituellement, c'est devenu un vrai casse-tête, ici impossible d'en trouver. et les points de vente sont à proximité de chez toi.

Pourrais-tu te rendre s'il te plait chez les buralistes(TABAC) et me prendre des recharges NEO-SURF d'une valeur de 200€ ??? C'est-à-dire 02 recharges NEO-SURF de 100€ pour ma carte prépayée que j'utilise pour mes déplacements et certaines dépenses.

Quand tu les auras, transmets-moi les codes de rechargement des coupons par mail ou si possible me faire un scan ainsi que le moyen adéquat pour le remboursement
ou donne moi ton RIB je te ferai un virement à l'instant .

Je t'appellerai dès que mon portable sera en service.
Tu peux t'en occuper maintenant STP ?
Je surveille ma messagerie pour te lire au plus vite.

Bises

MINISTÈRE DE L'INTÉRIEUR

DIRECTION GÉNÉRALE DE LA GENDARMERIE

DIRECTION DE PROTECTION DES MINEURS

A votre attention :

CONVOCATION EN JUSTICE
Pour les nécessités d'une enquête judiciaire
(Article 390-1 du Code de procédure pénale)

Je suis Mr Christian RODRIGUEZ, directeur général de la gendarmerie nationale en collaboration avec L'Office Européen De Police (Europol). Je vous contacte peu après une saisie informatique de cyber-infiltration (Autorisée, notamment en matière de pédopornographie, Site Pornographique, Cyber pornographie, pour vous informer que vous faites l'objet de plusieurs poursuites judiciaires en vigueur :

- **LA PÉDOPORNOGRAPHIE**
- **SITE PORNOGRAPHIQUE**
- **CYBER PORNOGRAPHIE**
- **DÉTOURNEMENT DE MINEURS**

Vous êtes prié de vous faire entendre par mail à l'adresse : bmp.crodriguez@gmail.com en nous écrivant vos justifications afin qu'elles soient mises en examen et vérifiées de sorte à évaluer les sanctions ; cela dans un délai strict de 72 heures. Passé ce délai, nous nous verrons dans l'obligation de transmettre notre rapport à Mme Maryvonne CAILLIBOTTE, procureur adjoint de la République près du tribunal de grande instance de Versailles et spécialiste de cybercriminalité pour établir un mandat d'arrêt à votre encontre, et vous serez fiché comme délinquant sexuel. Votre dossier sera également transmis aux médias pour une diffusion où votre famille, vos proches et toute l'Europe entière verront ce que vous faites devant votre ordinateur.

Maintenant vous êtes avertis.

Cordialement,

Gle. Christian RODRIGUEZ,
Directeur général de la gendarmerie nationale.

DIRECTION CENTRALE DE LA GENDARMERIE
BRIGADE DE PROTECTION DES MINEURS
Adresse : 4 rue Claude-Bernard 92130 Issy-les-Moulineaux
Intervention 7j/7j – 24h/24h
EUROPOL

DIRECTEUR GÉNÉRAL
GENDARMERIE NATIONALE

Les Arnaques au faux support technique

L'arnaque au faux support technique consiste à effrayer la victime, par SMS, téléphone, chat, courriel, ou par l'apparition d'un message qui bloque son ordinateur, lui indiquant un problème technique grave et un risque de perte de ses données ou de l'usage de son équipement afin de la pousser à contacter un prétendu support technique officiel (Microsoft, Apple, Google…), pour ensuite la convaincre de payer un pseudo-dépannage informatique et/ ou à acheter des logiciels inutiles, voire nuisibles. Si la victime refuse de payer, les criminels peuvent la menacer de détruire ses fichiers ou de divulguer ses informations personnelles.

Les Arnaques au faux support technique (suite)

Objectif : **Soutirer de l'argent** à la victime en la poussant à laisser prendre le contrôle de sa machine pour faire semblant de la lui dépanner et lui installer des logiciels et/ou faire souscrire des abonnements qui lui seront facturés.

Gendarmerie nationale

Votre ordinateur a été verrouillé.

Votre ordinateur nous a averti qu'il était infecté par un virus et un logiciel espion. Les données suivantes sont à risque:

- Identifiant Facebook, identifiants de messagerie
- Information de carte de crédit, accès bancaires
- Fichiers sur cet ordinateur

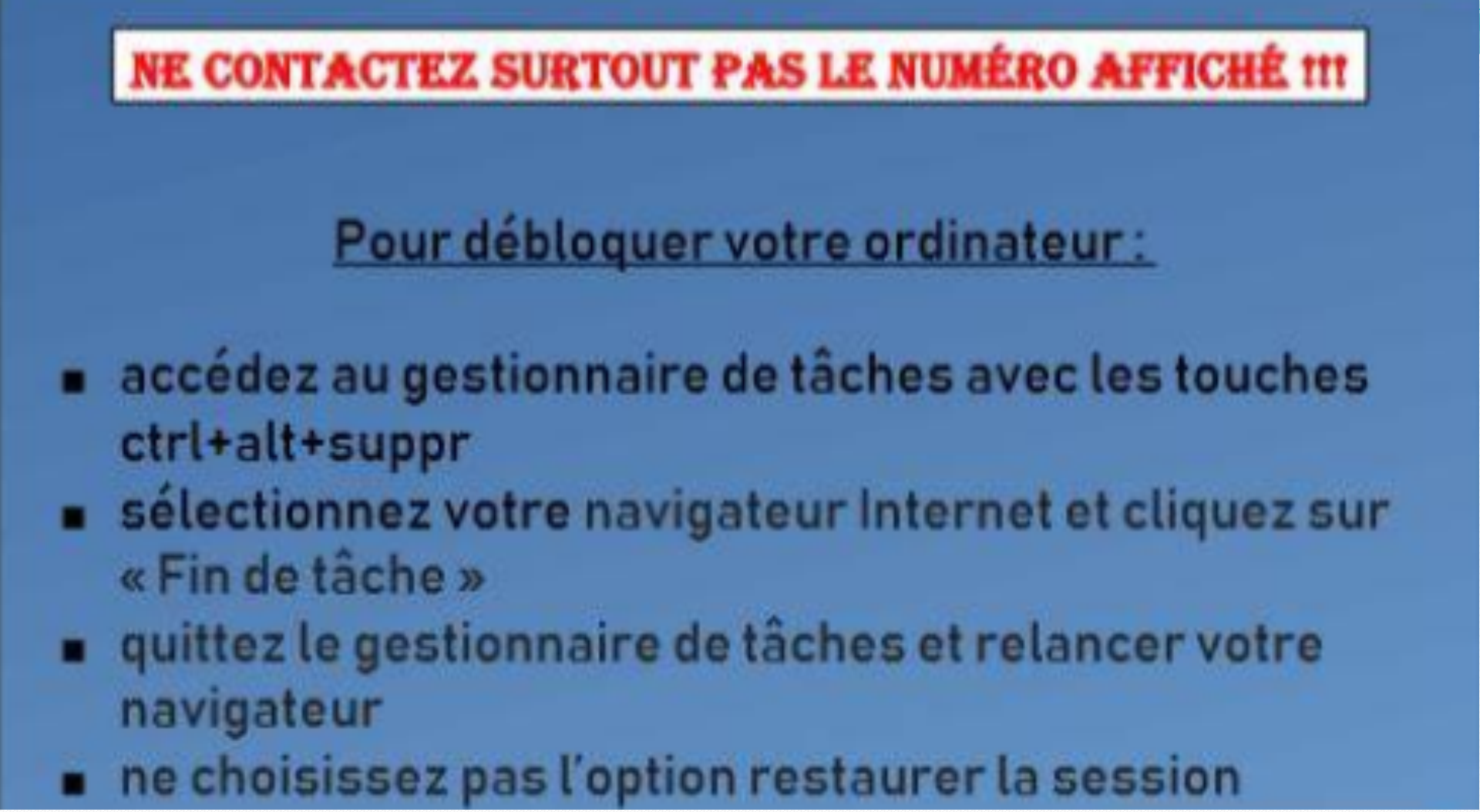
Ne redémarrez pas votre ordinateur et contactez Windows, sinon nous ne pourrons garantir la sécurité de vos données.

Pour plus d'informations sur ce problème et sur les solutions possibles, consultez le site https://www.windows.com/stopcode

Si vous contactez l'assistance, transmettez-leur ces informations:

Code d'arrêt: VIRUS

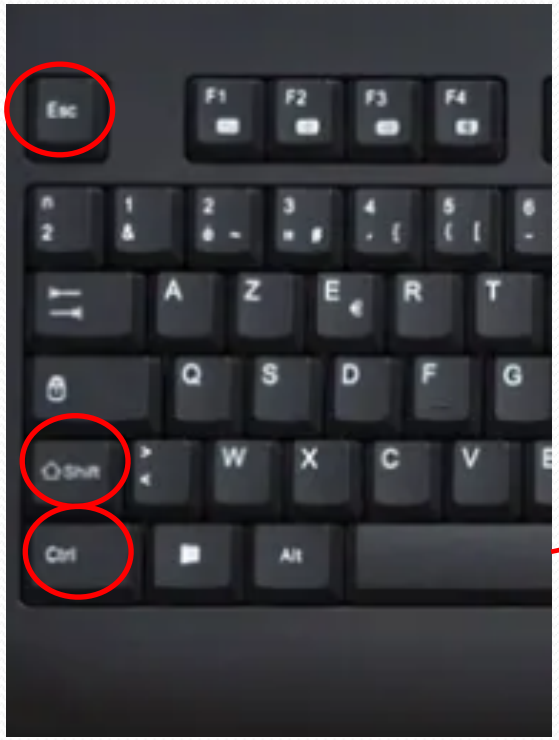
Appelez le support technique Windows: 09 72 51 43 50 (Appel gratuit)

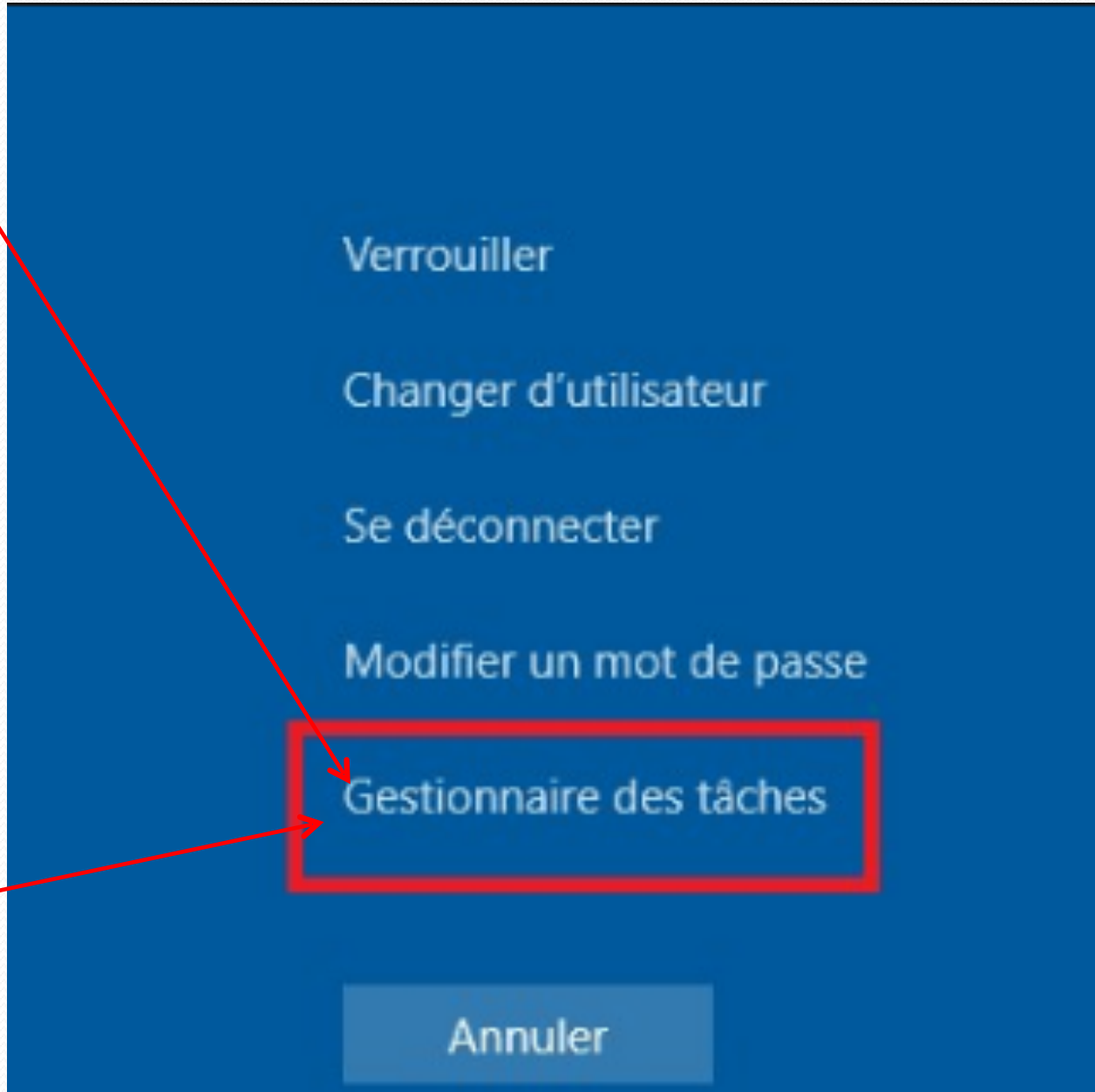


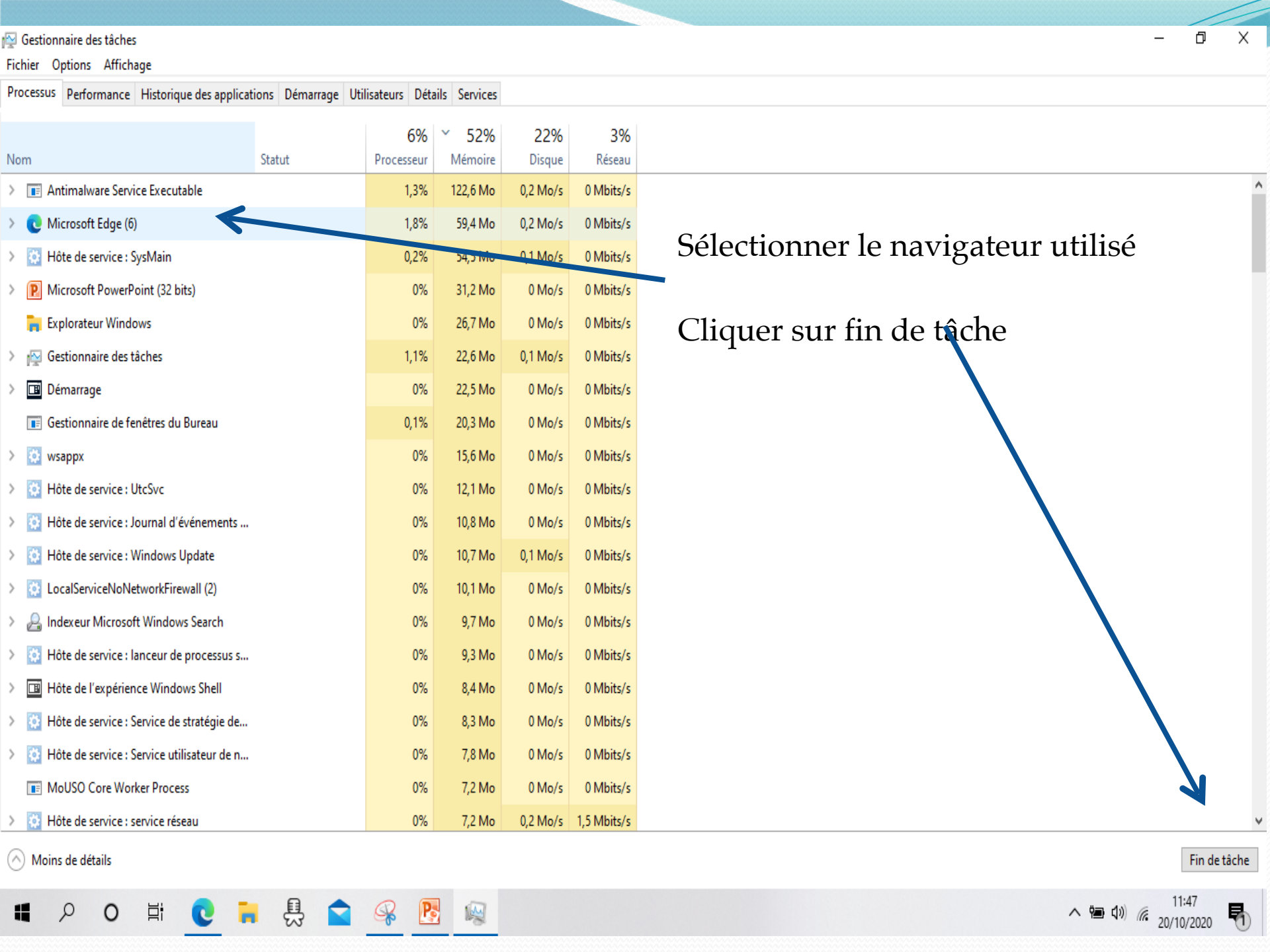
A l'issue, signalez l'escroquerie :
· soit sur le site du gouvernement dédié aux contenus illicites, www.internet-signalement.gouv.fr à la rubrique escroquerie
· soit par téléphone via le numéro vert gratuit mis en place par le gouvernement : 0 805 805 817."


Quand tout va mal,
fais ça:
Ctrl + alt
+ suppr

OU

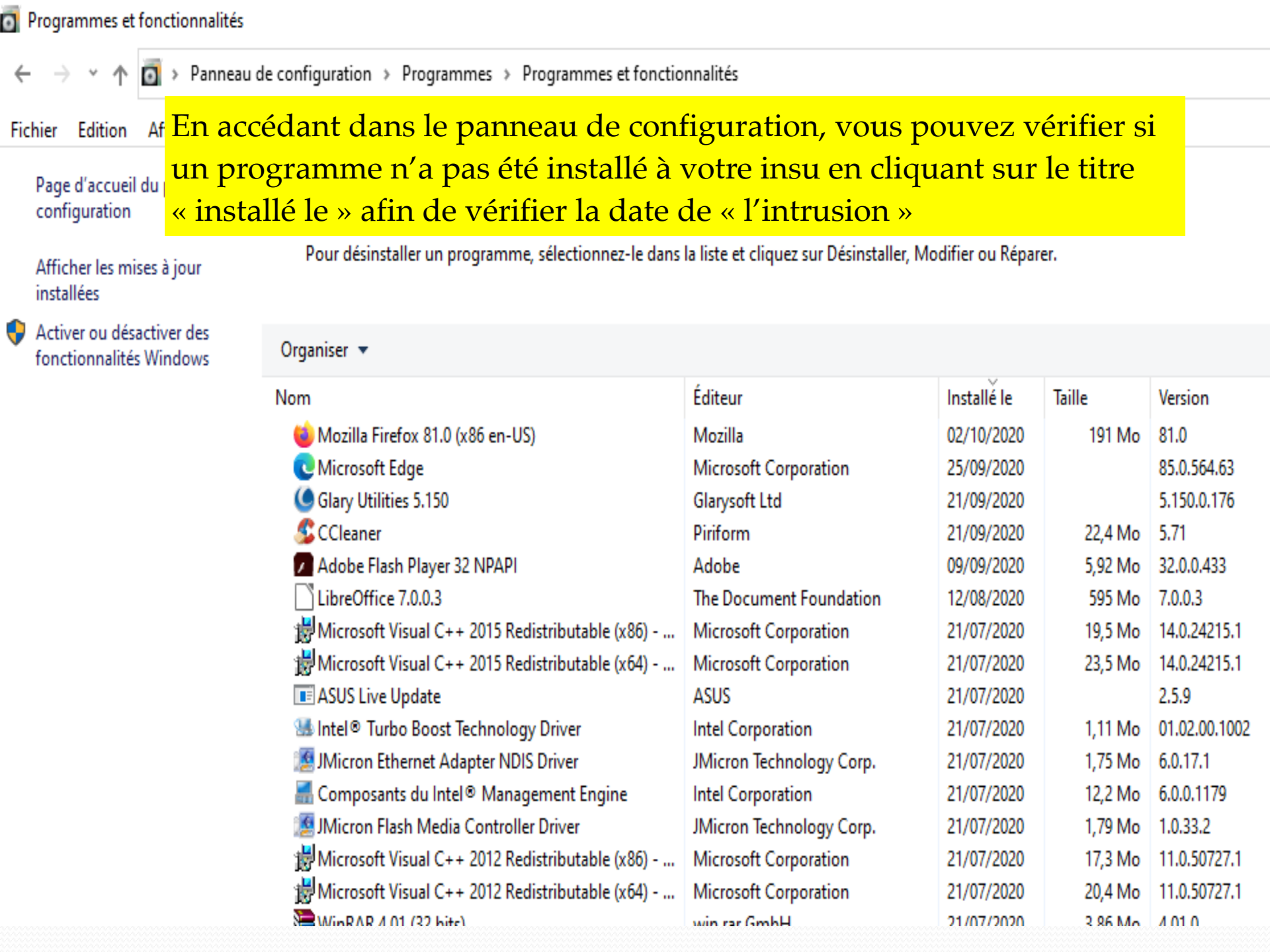

Esc
F1
F2
F3
F4
A
Z
E
R
T
Q
S
D
F
G
W
X
C
V
Ctrl
Alt


Verrouiller
Changer d'utilisateur
Se déconnecter
Modifier un mot de passe
Gestionnaire des tâches
Annuler



Sélectionner le navigateur utilisé

Cliquer sur fin de tâche


Programmes et fonctionnalités
Panneau de configuration › Programmes › Programmes et fonctionnalités
Fichier Edition Af
En accédant dans le panneau de configuration, vous pouvez vérifier si un programme n'a pas été installé à votre insu en cliquant sur le titre « installé le » afin de vérifier la date de « l'intrusion »
Page d'accueil du configuration
Afficher les mises à jour installées
Activer ou désactiver des fonctionnalités Windows
Pour désinstaller un programme, sélectionnez-le dans la liste et cliquez sur Désinstaller, Modifier ou Réparer.
Organiser
Nom
Éditeur
Installé le
Taille
Version
Mozilla Firefox 81.0 (x86 en-US) Mozilla 02/10/2020 191 Mo 81.0
Microsoft Edge Microsoft Corporation 25/09/2020 85.0.564.63
Glary Utilities 5.150 Glarysoft Ltd 21/09/2020 5.150.0.176
CCleaner Piriform 21/09/2020 22,4 Mo 5.71
Adobe Flash Player 32 NPAPI Adobe 09/09/2020 5,92 Mo 32.0.0.433
LibreOffice 7.0.0.3 The Document Foundation 12/08/2020 595 Mo 7.0.0.3
Microsoft Visual C++ 2015 Redistributable (x86) - ... Microsoft Corporation 21/07/2020 19,5 Mo 14.0.24215.1
Microsoft Visual C++ 2015 Redistributable (x64) - ... Microsoft Corporation 21/07/2020 23,5 Mo 14.0.24215.1
ASUS Live Update ASUS 21/07/2020 2.5.9
Intel® Turbo Boost Technology Driver Intel Corporation 21/07/2020 1,11 Mo 01.02.00.1002
JMicron Ethernet Adapter NDIS Driver JMicron Technology Corp. 21/07/2020 1,75 Mo 6.0.17.1
Composants du Intel® Management Engine Intel Corporation 21/07/2020 12,2 Mo 6.0.0.1179
JMicron Flash Media Controller Driver JMicron Technology Corp. 21/07/2020 1,79 Mo 1.0.33.2
Microsoft Visual C++ 2012 Redistributable (x86) - ... Microsoft Corporation 21/07/2020 17,3 Mo 11.0.50727.1
Microsoft Visual C++ 2012 Redistributable (x64) - ... Microsoft Corporation 21/07/2020 20,4 Mo 11.0.50727.1
WinRAR 4.01 (32 bits) win.rar GmbH 21/07/2020 3,86 Mo 4.01.0

Les rançongiciels (ransomwares)

Les rançongiciels sont des logiciels malveillants qui bloquent l'accès à l'ordinateur ou à des fichiers en les chiffrant et qui réclament à la victime le paiement d'une rançon pour en obtenir de nouveau l'accès. La machine peut être infectée après l'ouverture d'une pièce jointe, ou après avoir cliqué sur un lien malveillant reçu dans des courriels, ou parfois simplement en naviguant sur des sites compromis, ou encore suite à une intrusion sur le système. Dans la majorité des cas, les cybercriminels exploitent des vulnérabilités connues dans les logiciels, mais dont les correctifs n'ont pas été mis à jour par les victimes.

Gendarmerie nationale

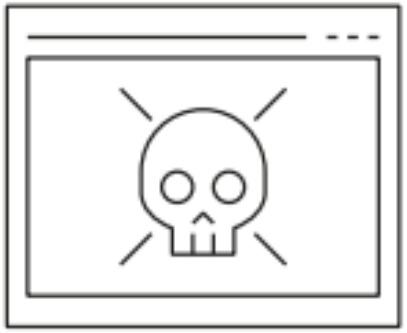
Les rançongiciels (suite)

Objectif : **Extorquer de l'argent** à la victime en échange de la promesse (pas toujours tenue) de retrouver l'accès aux données corrompues. Certaines attaques visent parfois simplement à endommager le système de la victime pour lui faire subir des pertes d'exploitation et porter atteinte à son image.

Gendarmerie nationale

Alerte aux rançongiciels

Vos données en otage, contre de l'argent !



Vous êtes de plus en plus nombreux à recevoir des messages douteux avec des pièces jointes et/ou des liens qui sont piégés, ***NE CLIQUEZ PAS DESSUS !***

Un virus pourrait chiffrer vos données et exiger une rançon. La payer ne garantit pas la récupération de l'intégralité de vos données.

Il est constaté de plus en plus d'**escroqueries** par des emails qui contiennent des pièces jointes et/ou des liens piégés. **Ces messages frauduleux sont maintenant plus difficiles à détecter** par les utilisateurs car ils sont bien souvent de parfaites copies, avec de vrais logos et sans faute d'orthographe.

VOICI QUELQUES RÈGLES DE BON SENS QU'IL FAUT ABSOLUMENT RESPECTER :

Ces réflexes sont indispensables et peuvent sauver votre entreprise !

N'ouvrez pas les messages dont la provenance ou la forme est douteuse.
Apprenez à distinguer des emails piégés en deux minutes sur :
https://www.hack-academy.fr/candidats/willy

Effectuez des sauvegardes régulières de vos données.
Déplacez physiquement la sauvegarde de votre réseau et placez-la en lieu sûr.
Assurez-vous aussi qu'elle fonctionne.

Mettez à jour vos principaux outils : Windows, antivirus, lecteur PDF, navigateur, etc.
Et si possible, désactivez les macros des solutions de bureautique qui permettent d'effectuer des tâches de manière automatisée. Cette règle évitera la propagation des rançongiciels via les vulnérabilités des applications.

Créer un compte « utilisateur » et n'utilisez que celui-ci, une fois votre ordinateur configuré.
Cette règle ralentira l'escroc dans ses actions malveillantes.

Les arnaques au chantage à la webcam prétendue piratée

Vous avez reçu un message (mail) d'un supposé pirate anonyme ou « hacker » qui prétend avoir piraté votre ordinateur. Il vous menace de publier des images compromettantes prises à votre insu avec votre webcam et vous demande une rançon en monnaie virtuelle ? Pas de panique, ce ne sont que des tentatives d'arnaques au chantage à la webcam prétendue piratée !

Gendarmerie nationale

Les arnaques au chantage à la webcam prétendue piratée

- 1. De quoi s'agit-il ?
- 2. Arnaques au chantage à la webcam prétendue piratée : faut-il avoir peur ?
- 3. Comment font-ils pour avoir ces informations ?
- 4. Que faut-il faire si on reçoit ce type de message ?
- 5. Arnaques au chantage à la webcam prétendue piratée : et si vous avez payé la rançon ?

Gendarmerie nationale

Divers

- **Carte PCS – Néo Surf……**
- **Crypto monnaies : bit coins**
- **Localiser une adresse iban**
- **La plate forme Police-Gendarmerie THESEE,**

Gendarmerie nationale

CALCULER UN IBAN

fr.iban.com

TROUVER L'IBAN À PARTIR DU NUMÉRO DE COMPTE ET DE L'AGENCE DE LA BANQUE

France (FR)

Code banque:

16806

Branch Code:

00820

Numéro de compte:

xxxxxxxx123

CALCULER

Details for 16806 - [redacted]	
IBAN	FR7616806008200[redacted] Check IBAN
RIB	1680600820[redacted]
BIC	AGRIFRPP868
BANK	CRCAM CENTRE FRANCE
ADDRESS	44 46 PL D ALLIER
CITY	MOULINS
ZIP	03000
COUNTRY	FRANCE

Les différents types de menaces (Conclusion)

Que faire pour éviter qu'un piratage se produise réellement ?

Même si dans le cas évoqué dans cet article, il ne s'agit essentiellement que d'une supercherie, vos équipements sont exposés à de vraies attaques informatiques. Voici quelques mesures simples de sécurité qui permettent de réduire considérablement les risques de piratages :

- **Faites régulièrement les mises à jour** de sécurité de tous vos appareils.
- **Utilisez un antivirus** et tenez-le à jour.
- **Évitez les sites dangereux** tels que les sites de téléchargements ou de vidéos en ligne (*streaming*) illégaux.
- **Utilisez des mots de passe solides**, différents sur tous les sites et changez les régulièrement.
- **Ne répondez pas, ne cliquez pas sur les liens, n'ouvrez pas les pièces jointes de messages d'expéditeurs inconnus** ou d'expéditeurs connus mais dont la structure du message est inhabituelle ou vide.
- **Masquer votre webcam** quand vous ne vous en servez pas (un simple morceau de ruban adhésif opaque sur l'objectif peut suffire).

Gendarmerie nationale

NOUVEAU

DEPUIS LE 15/03/2022

THESEE

PLATEFORME DE PLAINTE EN LIGNE POUR LES VICTIMES D'E-ESCROQUERIES

(RÉSERVÉ AUX PARTICULIERS)

- **Qu'est ce qu'une e-escroquerie ?**
- **- Piratage de compte mail ou de réseau social avec demande d'argent :**
  Votre adresse mail ou votre profil sur les réseaux a été piraté et de l'argent a été demandé à un de vos contacts en votre nom.
- **- Escroquerie à la petite annonce, faux acheteur ou faux vendeur :**
  Vous avez été escroqué(e) par un faux acheteur suite à la vente d'un produit en ligne sur un site de petites annonces.
- **- Fausse location :**
  Vous avez été escroqué(e) à l'occasion d'une démarche pour louer un bien immobilier en ligne.
- **- Ransomware :**
  Les fichiers de votre ordinateur, tablette ou téléphone mobile ont été cryptés et une rançon vous est demandée
- **- Chantage en ligne :**
  Vous faites l'objet de menaces en ligne de diffusion d'images portant atteinte à votre honneur.
- **- Escroquerie aux sentiments :**
  Lors d'une relation en ligne, vous avez été incité(e) par des moyens frauduleux à verser de l'argent.
- **- Faux site de vente :**
  Vous avez été escroqué(e) lors d'un achat sur un site de vente en ligne frauduleux.

- **Une prise en charge par des policiers experts**
- Si vous êtes un particulier et que vous faites face à une escroquerie sur internet, vous pouvez déposer en quelques clics votre plainte en ligne.
- **Comment faire ?**
- 1) Se rendre sur la rubrique "Arnaque sur internet" du site du service public.
- 2) Se laisser guider pour personnaliser votre démarche.
- 3) S'identifier grâce à *France Connect et ses fournisseurs d'identité (impôts, AMELI, La Poste...)*
- 4) Remplir le formulaire.
- 5) Après validation par un enquêteur, vous recevez votre plainte dans votre espace personnel.
- A savoir : vous avez aussi la possibilité de faire un signalement de manière anonyme.
- **Votre déclaration est importante et contribue, grâce à une expertise centralisée, à une recherche plus efficace des auteurs.**

Liens Utiles

Liens utiles (suite)

- https://www.cybermalveillance.gouv.fr/
- https://www.gendarmerie.interieur.gouv.fr/a-votre-contact/contacter-la-gendarmerie/discuter-avec-un-gendarme-de-la-brigade-numerique
- https://www.service-public.fr/ rubrique "Arnaque sur internet"

Gendarmerie nationale