NORMANDIE CYBER

CENTRE DE RÉPONSE AUX INCIDENTS CYBER

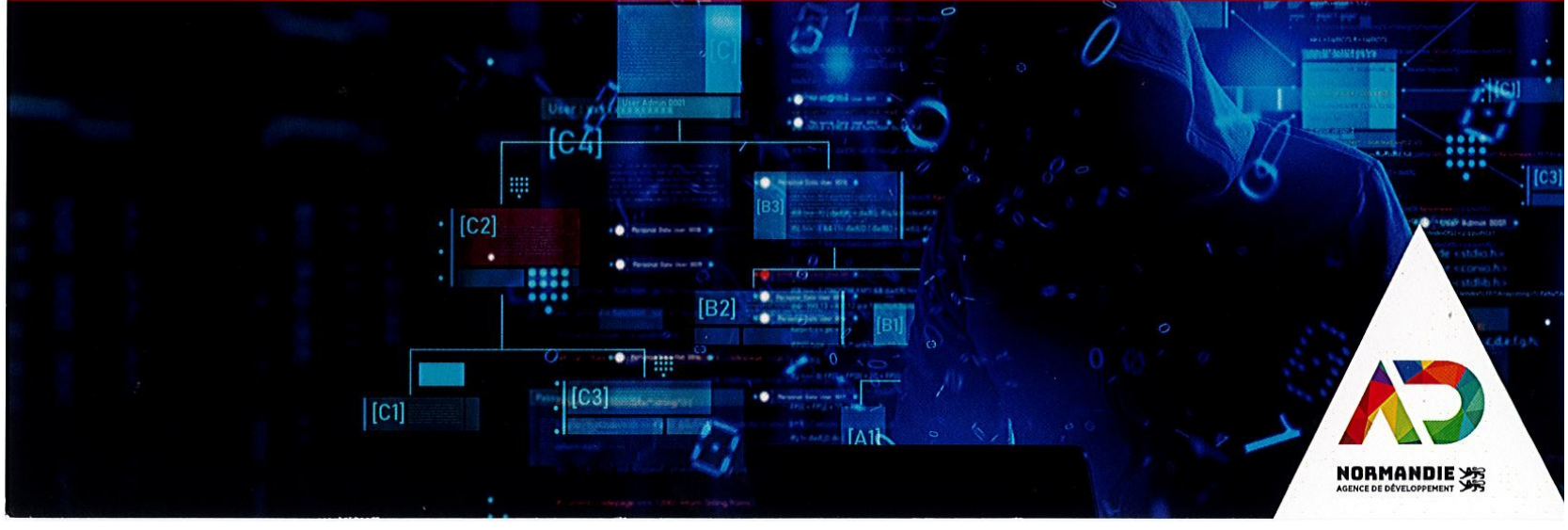
Avec le soutien de :

RÉGION NORMANDIE

ANSSI

NUMÉRO D'APPEL D'URGENCE [service gratuit - prix d'un appel local]

0 808 800 001

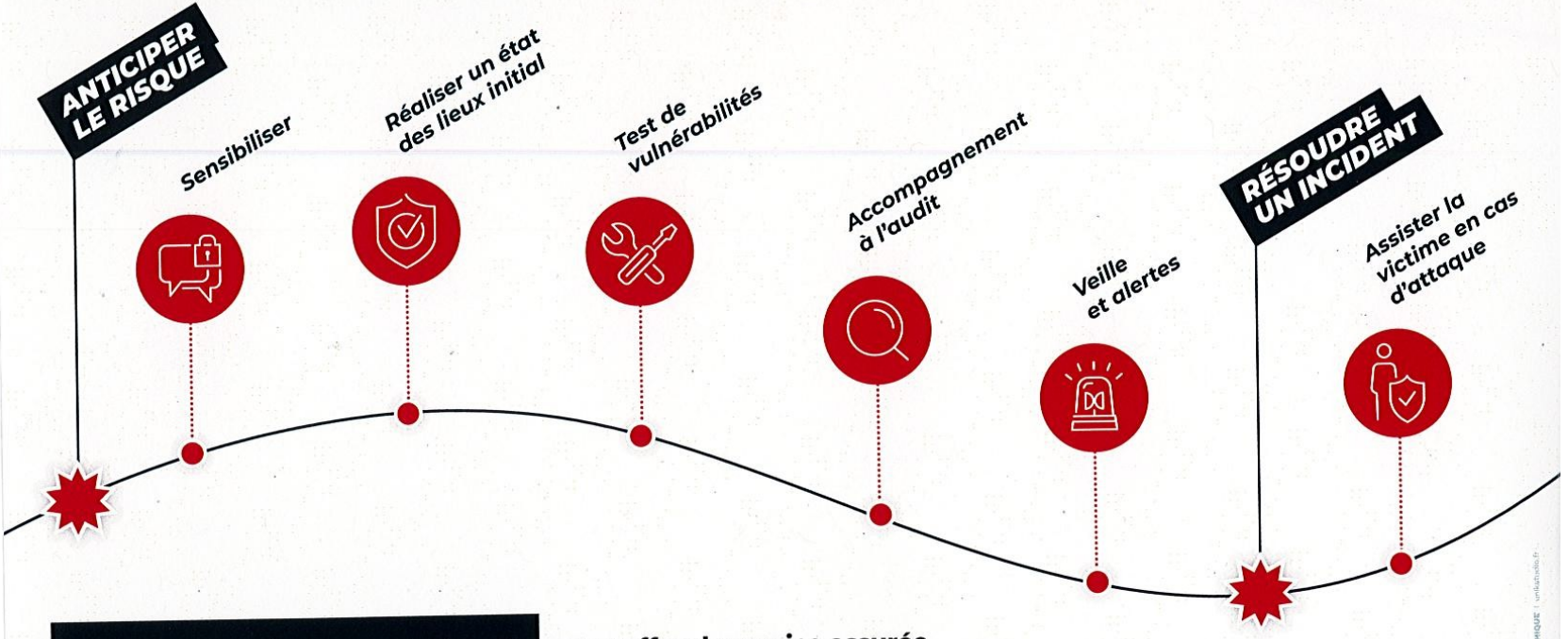


NORMANDIE AGENCE DE DÉVELOPPEMENT

NORMANDIE CYBER

CENTRE DE RÉPONSE AUX INCIDENTS CYBER

NORMANDIE CYBER est un centre de réponse de proximité destiné aux entreprises et collectivités de taille intermédiaire pour les accompagner dans toutes leurs démarches en matière de sécurité numérique.



Ayez le réflexe de nous contacter au

0 808 800 001

Une offre de service assurée par l'AD Normandie, en partenariat avec l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).

ACTION DE LA GENDARMERIE

DANS LE CYBERESPACE

2023 – Région Normandie

CYBER MOIS

UN ÉCOSYSTÈME CYBERCRIMINEL PLUS SOPHISTIQUÉ ET PROFESSIONNEL

Une menace sérieuse…

CYBERMENACES 2022

94 266

Total des faits cyber en gendarmerie

- **64 464** escroqueries et abus de confiance
- **6 424** atteintes à la dignité et à la personnalité
- **5 530** atteintes aux STAD
  (systèmes de traitement automatisé de données)
- **5 012** menaces et chantages
- **1 178** atteintes aux mineurs

Source : gendarmerie nationale

1 plainte / 250 faits
tentés ou commis.

6 000 Md€
coût mondial
de la cyberdélinquance.

…trop peu prise en compte

Une menace numérique infinie, rapide, protéiforme, internationale et… dangereuse pour la stabilité démocratique

64,6 % de la population mondiale utilise **internet**

59,9 % de la population mondiale utilise les **réseaux sociaux**
13,5 nouveaux usagers / seconde !

29 milliards d'**objets connectés** d'ici 2030

LES PRINCIPALES CYBERMENACES

CYBERMENACE = ADVERSAIRE + VULNÉRABILITÉ(S) + MODE D'ACTION

ADVERSAIRES

- États-nations
- Menaces internes
- Cybercriminels
- Amateurs de sensations fortes
- Groupes terroristes
- Hacktivistes

Motivations

- Mécontentement
- Satisfaction
- Violence idéologique
- Idéologique
- Gains financiers
- Géopolitique

VULNÉRABILITÉS

- Failles humaines

Exploitation d'une erreur ou d'un comportement humain :
- *brancher une clé USB inconnue*
- *hameçonnage*
- *fraude au président*

Absence de culture cyber des personnels

- Failles techniques

- Problème de mises à jour
- Mauvaise sauvegarde des données
- absence de confidentialité
- mauvaise gestion de la disponibilité

- Failles physiques

- Manque de surveillance des accès aux serveurs
- Absence ou mauvais contrôle et identification des personnels
- Non application des règles d'inclusion et d'exclusion
- Problème de protection des locaux

MODES D'ACTION

- Ingénierie sociale
  82 % des violations de données reposent sur un facteur humain
- Utilisation d'outils pour rançonner les victimes
  60 % des organisations ont payé la rançon
- Saturation d'un réseau, d'un système, d'un service
- Logiciels malveillants
  En juin 2022, Plus de 10 millions de téléchargements par le biais de logiciels publicitaires
- Attaques sur la chaîne d'approvisionnement
  En 2021, ils représentent 17 % des attaques
- Campagne de désinformation / Défacement de site internet

LE RANÇONGICIEL

Un rançongiciel ou *ransomware* est un **logiciel malveillant** qui bloque l'accès à l'ordinateur ou à des fichiers en les **chiffrant** et qui réclame à la victime le paiement d'une **rançon** pour en obtenir de nouveau l'accès.

Motivations

Extorsion/Atteinte à l'image

Moyens d'action

- Vulnérabilités
- Campagnes d'hameçonnage ciblé
- Attaque par force brute sur les réseaux de l'entreprise

Effets

- Chiffrement des données
- Exfiltration des données
- Effacement des sauvegardes
- Suppression des traces

Impacts

Récupération potentielle d'une partie ou de toutes les données

OU

- Publication de données
- Perte de données

Une attaque par rançongiciel

toutes les 11 secondes dans le monde....

58 secondes...

Moins de 1000 euros....

LE RANÇONGICIEL

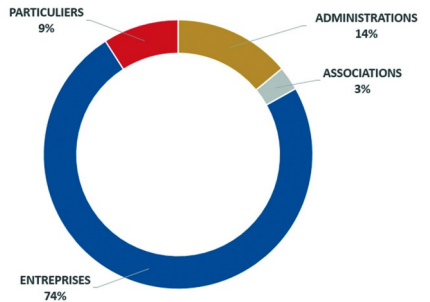
308 … attaques **enregistrées** en 2021 par la gendarmerie

36 % … des faits cyber r**ecensés** en 2021 par la gendarmerie

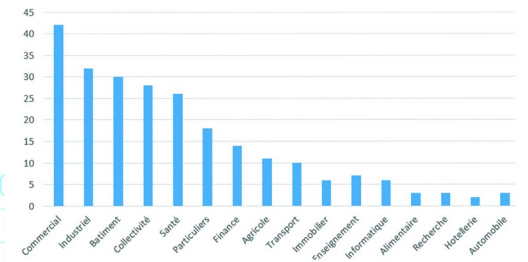
30 % … des victimes auraient **payé** la rançon

1000 … attaques auraient **abouti** en 2021 et toutes n'ont pas fait l'objet d'un dépôt de plainte…

Typologie des victimes



Typologie des secteurs



Typologie des secteurs ciblés en 2022
(Source : données judiciaires Gendarmerie nationale)

QUELQUES EXEMPLES

Essonne : l'hôpital Sud Francilien victime d'une cyberattaque, une rançon de 10 millions de dollars demandée

Les pirates informatiques ont réussi à bloquer tout le réseau informatique de l'hôpital.

Pierre de Cossette - franceinfo
Radio France

Publié le 22/08/2022 11:12 Mis à jour le 22/08/2022 11:42

Corse: cyberattaque d'un hôpital, les soins de radiologie et oncologie suspendus

Par Le Figaro avec AFP
Publié le 29/03/2022 à 16:24, mis à jour le 29/03/2022 à 16:44

Écouter cet article 00:00/01:43

LADEPECHE.fr

Lot : trois hôpitaux victimes d'une tentative d'arnaque, les gendarmes contre-attaquent

Les Echos

Idées Économie Politique Entreprises Finance - Marchés Bourse Monde Tech-Médias Start-up Régions Patrimoine

En Allemagne, une première cyberattaque mortelle

L'attaque informatique contre l'hôpital de Düsseldorf s'est terminée par le décès d'une patiente en état critique. Disparus dans la nature, le ou les coupables font l'objet d'une enquête pour « homicide par négligence ».

Lire plus tard Commenter Partager Allemagne Florence Parly

La Ville et l'agglomération de Saumur victimes d'une cyberattaque

La Ville et la communauté d'agglomération de Saumur (Maine-et-Loire) l'ont annoncé dans un communiqué commun : elles font l'objet d'une cyberattaque depuis ce mercredi matin, 23 mars. Elles ont déposé plainte.

Ouest-France
Vincent COTINAT.
Publié le 23/03/2022 à 19h33

Le Parisien

High-tech

La ville d'Angers paralysée par une cyberattaque

Des pirates ont déployé un rançongiciel qui affecte tous les serveurs et fait tourner les services municipaux au ralenti.

Illustration. Les services municipaux d'Angers sont affectés par une cyberattaque par rançongiciel. LP/Olivier Arandel

Seine-Saint-Denis. Victime d'une cyberattaque, Bondy estime les dommages à 1,5 million d'euros

En novembre 2020, Bondy (Seine-Saint-Denis) avait été victime d'une cyberattaque. Depuis, la ville, qui a dû investir 1,5 milli
remise de cette situation, con

la gazette

Ouest-France
avec NG
Publié le 12/07/2022 à 14h24

Abonnez-vous

ÉCOUTER
LIRE PLUS TARD
PARTAGER
NEWSLETTER LA MATINALE

ACCUEIL > CLUB TECHNI.CITÉS > ACTUALITÉS TECHNIQUE > TOUTE L'ACTU TECHNIQUE > ACTUS EXPERTS TECHNIQUE > Une cyberattaque coûte 550 000 euros à la ville de Chalon-sur-Saône

CYBERSÉCURITÉ

Une cyberattaque coûte 550 000 euros à la ville de Chalon-sur-Saône

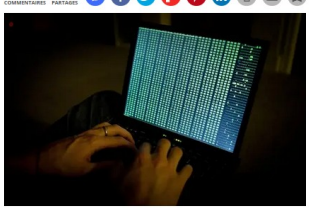
Publié le 29/07/2021 • Par Alexandre Léchenet • dans : actus experts technique, Régions

Annecy : Deux mois après la cyberattaque, les services informatiques de la ville toujours impactés

HACKER L'ensemble des sites de la ville devraient être reconstruits d'ici le 31 mars prochain

20 Minutes avec agence | Publié le 08/02/22 à 12h37 — Mis à jour le 08/02/22 à 12h37

2 COMMENTAIRES 21 PARTAGES



Le ou les hackers n'ont pas été identifiés. — A. GELEBART / 20 MINUTES

Écouter cet article Annecy : Deux mois après la cyberattaque, les services informatiques de l 00:00

Victimes d'une cyberattaque en novembre dernier, les services informatiques de la ville d'Annecy (Haute-Savoie) vont être encore perturbés pendant plusieurs semaines. L'objectif est pour l'heure de reconstruire la sécurité numérique, révèle *Le Dauphiné Libéré*.

À LIRE AUSSI

02/02/22 | RÉHABILITATION
Annecy : Deux ans après un violent incendie, le projet du nouvel Hôtel de...

03/02/22 | PLOUF
Haute-Savoie : Une pelle mécanique à la rescousse d'une vache tombée dans...

07/02/22 | SURVIVANT
Quatre ans après un crash d'avion en Savoie, un homme lourdement handicapé...

20 MINUTES

icipal du 20 juillet, le
-Saône a annoncé le
ue subie par la ville
agglomération en
eurs embauches sont

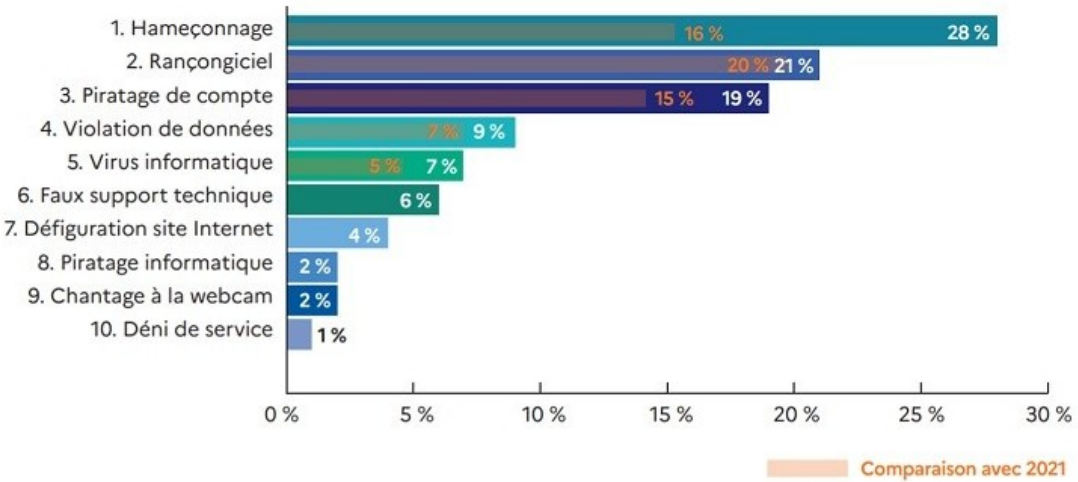
ZOOM SUR LES COLLECTIVITES TERRITORIALES

En 2022, 3510 collectivités sont venues chercher une assistance en ligne ce qui représente une augmentation de 67 %

Source : cybermalveillance.gouv.fr

23% des rançongiciels traités ou rapportés à l'ANSSI en 2022 émanent de collectivités territoriales (2ème place devant les établissements publics de santé 10 %)

Source : ANSSI



Principales recherches d'assistance pour les collectivités et administrations

Source : cybermalveillance.gouv.fr

QUELQUES CONSEILS...

Je suis victime d'un rançongiciel

1. **Déconnecter** mon appareil d'internet et du réseau informatique
2. Au travail, **alerter** immédiatement le service ou prestataire informatique
3. **Ne pas payer** la rançon
4. **Conserver** les preuves numériques en neutralisant le matériel infecté
5. **Déposer** plainte
6. Faites-vous assister au besoin par des professionnels qualifiés

Je me protège d'une attaque

1. **Sensibiliser** mes proches et mes collaborateurs
2. **Appliquer régulièrement** les mises à jour de sécurité
3. **Tenir à jour** son antivirus
4. **Se méfier** des e-mails douteux
5. **Ne pas installer** des applications ou logiciels à l'origine douteuse
6. **Privilégier** une navigation sécurisée sur le Web et **séparer** l'usage personnel de l'usage professionnel
7. **Sauvegarder** régulièrement ses données sur un support amovible
8. **Privilégier** l'utilisation d'un compte utilisateur pour les tâches courantes
9. **Utiliser** des mots de passe complexes et les **changer** régulièrement
10. **Éteindre** l'ordinateur en cas de non-utilisation

LES ESCROQUERIES BASÉES SUR L'USURPATION D'IDENTITÉ

Ensemble des techniques frauduleuses destinées à **leurrer** l'internaute pour l'**inciter à communiquer** des données personnelles et/ou bancaires **en se faisant passer pour un tiers de confiance.**

MAIL

L'**hameçonnage**
L' **harponnage**
L'**arnaque au président…**

SMS

Le **Smishing**

APPEL

Le **Vishing**

QUELQUES CHIFFRES

1ère

L'hameçonnage est la 1ère Cybermalveillance tous publics confondus

Source : www.cybermalveillance.gouv.fr

96 %

… des escroqueries sont réalisées par mail

Source : www.tessian.com

39 %

… des faits d'escroquerie et abus de confiance en gendarmerie ont une origine cyber

Source : gendarmerie nationale

800

… signalements par jour d'escroquerie à la carte bancaire sur PERCEV@L

Source : Perceval – Gendarmerie nationale

QUELQUES EXEMPLES

L'Assurance Maladie — mon compte — mon parcours d'assuré

Bonjour ,

Nous vous informons que vous avez un remboursement en attente d'un montant de **169,20 €** sur votre espace personnel.

La carte enregistrée sur votre espace personnel n'a pas été créditée pour le motif suivant :

Le numéro de mobile enregistré sur votre espace personnel ne correspond pas à celui associé à votre compte bancaire.

Détails de remboursement:

Référence : AWL-20/982KDJ

Monta

Pour

méth

Votre

18 53

Exe

MENU ouest france — Rechercher ville, actualité, fait divers...

Accueil / Faits divers / Arnaques

Une arnaque à la carte Vitale cible les victimes par SMS

Une nouvelle arnaque à la carte Vitale s'est massivement répandue ces derniers mois. Les victimes sont contactées par SMS pour renouveler ce document et doivent préalablement fournir des informations à caractère personnel.

Ouest-France
Maxime FETTWEIS.
Publié le 21/04/2022 à 11h00

Abonnez-vous

ÉCOUTER
LIRE PLUS TARD
PARTAGER
NEWSLETTER TU L'AS LU ?

Une nouvelle arnaque à la carte Vitale aurait déjà ciblé plusieurs milliers de personnes | CHARLES JOSSE / OUEST-FRANCE

Une campagne de phishing imitant de grands groupes sévit en France

Un hackeur a lancé depuis quelques mois une vaste opération de phishing par SMS pour arnaquer les internautes français, rapporte Phonandroid.

Par LePoint.fr

Publié le 14/06/2022 à 02h17 - Modifié le 14/06/2022 à 06h36

Je m'abonne à **1€** le 1er mois

Netflix, la Fnac, la Banque populaire, la Caisse d'épargne, l'Assurance maladie… Un pirate informatique a récemment usurpé les noms de grands sites, marques ou services publics pour mettre au point une campagne de phishing et arnaquer des centaines et des centaines d'internautes français. Le hackeur, plus malin que les arnaqueurs ordinaires, a commencé à opérer par SMS en se faisant passer pour l'Assurance maladie et en tentant de convaincre ses victimes que leurs cartes vitales étaient périmées, rapporte Phonandroid.

Dans chaque SMS, le pirate informatique a intégré un lien qui renvoie vers un site imitant à la quasi-perfection l'interface de l'Assurance maladie. À quelques détails près : l'URL n'est pas le bon et les « L » du texte ont été remplacés par des « i » majuscules. Cette subtilité, repérée par le journaliste spécialisé Damien Bancal, est trompeuse à l'œil nu, mais elle permet aussi de passer à travers les filets des outils de surveillance en matière de cybercriminalité.

MENU ouest france — Rechercher ville, actualité, fait divers...

Accueil / High Tech / Téléphonie

Attention, ces SMS de réception de colis cachent une campagne d'hameçonnage de pirates chinois

Une campagne d'hameçonn
actuellement sur le territoire
dérober les données des sn

Ouest-France
avec agence
Publié le 04/08/2022 à 12h52

Abonnez-vous

ÉCOUTER
LIRE PLUS TARD
PARTAGER
NEWSLETTER GAMING

MENU **Le Point**

Le monde judiciaire français ciblé par une vaste cyberattaque

Magistrats, procureurs, avocats… De nombreuses personnes chargées de dossiers sensibles ont été visées par des hackers. Une enquête a été ouverte.

Source AFP

Publié le 06/09/2020 à 15h15 - Modifié le 06/09/2020 à 18h22

Je m'abonne à **1€** le 1er mois

Le monde judiciaire français sous la menace de hackers. Le parquet de Paris a ouvert une enquête préliminaire, vendredi 4 septembre 2020, après une cyberattaque qui a tenté d'atteindre des acteurs de la justice, a en effet appris l'Agence France-Presse dimanche de source judiciaire.

Selon *Le Journal du dimanche*, cette cyberattaque a ciblé le procureur de Paris, Rémy Heitz, mais aussi des magistrats ou des avocats parisiens chargés de dossiers sensibles. Une source proche du dossier a toutefois précisé que cette attaque était d'ampleur plus large, ne se limitant pas au tribunal judiciaire de Paris.

« E-mail curieux »

FOVI – L'ARNAQUE AU PRÉSIDENT

URGENT

CONFIDENTIEL

À L'ÉTRANGER

L'**escroquerie aux faux ordres de virement** (FOVI) désigne un type d'arnaque qui, par **persuasion**, **menaces** ou **pressions** diverses, vise à amener la victime à **réaliser un virement** de fonds non planifié. Parfois présenté comme émanant d'un dirigeant et ayant un **caractère « urgent et confidentiel »**, on parle alors « d'**arnaque au Président** ».
Dans certains cas, cette fraude fait suite au **piratage** et à l'utilisation de la messagerie de la personne ou entité usurpée.

INFO EUROPE 1 – «Arnaque au président» : 2,5 millions d'euros détournés d'une société de production de cinéma

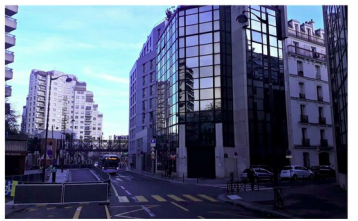
nformations recueillies par Europe 1, un réseau de de "l'arnaque au président" vient d'être démantelé

Le Parisien

Faits divers

«Arnaque au président» : 33 millions dérobés au promoteur immobilier parisien

Des escrocs dits «aux faux ordres de virement» sont parvenus à s'emparer de plus de 33 millions d'euros dans les caisses de la société Sefri-Cime, à Paris. Une comptable a été flouée avant de faire des transferts d'argent sur des comptes européens pour une pseudo entrée en Bourse. Une technique qui prospère depuis dix ans.

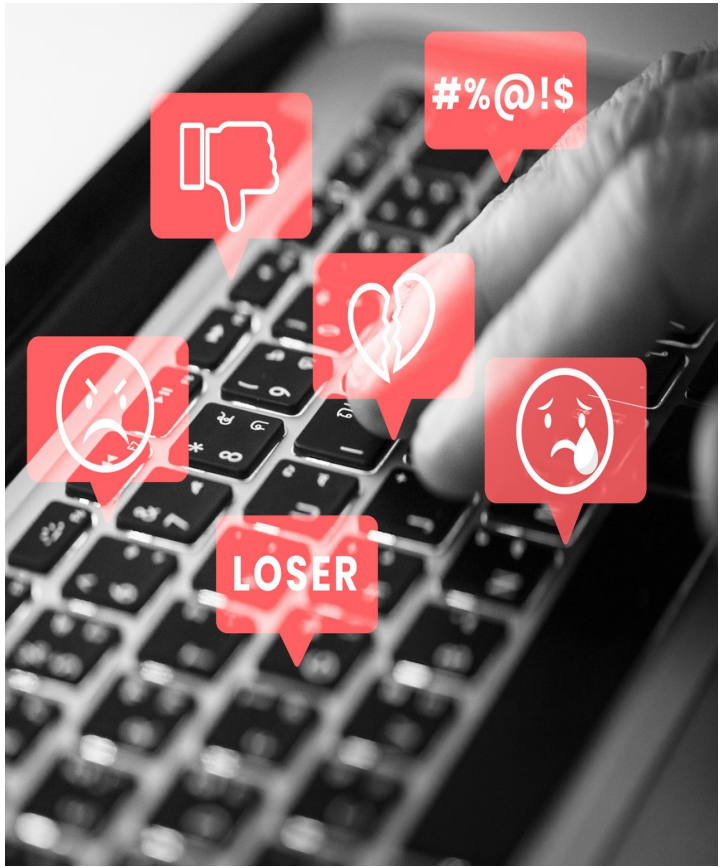


Les Echos

Michelin victime de « l'arnaque au président »

Le fabricant de pneumatiques s'est fait dérober 1,6 million d'euros au moyen de l'arnaque dite « du président ».

LE CYBERHARCÈLEMENT



On parle de cyberharcèlement lorsqu'une ou plusieurs personnes utilisent les **moyens de communication numériques,** de manière **délibérée et répétée** dans le temps, pour **porter atteinte à l'intégrité morale** d'une personne.

Les moyens → Téléphones portables, messageries instantanées, forums, chats, jeux en ligne, e-mails, réseaux sociaux, sites de partage…

Les formes → Intimidations, insultes, moqueries, menaces, propagation rumeurs, piratage de compte, usurpation d'identité, publication de photos ou vidéos…

LE CYBERHARCÈLEMENT

20 %

des **6/18 ans** ont déjà été confrontés à une situation de cyberharcèlement

Source : Association e-Enfance

205 973

… écoliers et collégiens ont été sensibilisés en 2021 aux dangers d'internet dans le cadre des opérations « permis internet » de la gendarmerie nationale

Source : gendarmerie nationale

40 %

… des moins de 50 ans disent avoir subi des attaques répétées sur les réseaux sociaux.

Source : https://fr.statista.com

693

… faits de cyberharcèlement enregistrés en 2021 par la gendarmerie. Soit une augmentation de 12 % !

Source : gendarmerie nationale

QUELQUES CONSEILS…

Je suis victime de cyberharcèlement :

1. **Ne pas répondre** pour ne pas attiser la haine
2. **Se confier** à une personne de confiance, ne pas rester seul
3. **Conserver** les preuves numériques (captures d'écran)
4. **Se protéger** en se déconnectant des réseaux, **bloquer** les auteurs
5. **Demander** le retrait des contenus aux hébergeurs
6. **Déposer** plainte

Je me protège du cyberharcèlement :

1. **Sensibiliser** mes proches et mes collaborateurs aux dangers de l'utilisation d'internet et des réseaux sociaux
2. **Protéger** sa vie privée et professionnelle sur internet et sur les réseaux sociaux
3. Témoin, ne **pas commenter** ou **relayer** les propos, photos ou vidéos
4. **Signaler** les faits de harcèlement et les auteurs

Les dispositifs de signalement en ligne :
– Plateforme PHAROS
– Contacter la brigade numérique de la gendarmerie ou la plateforme de l'association e-enfance au 3018

LES TRAFICS ILLICITES EN LIGNE

Les trafics illicites en ligne représentent l'ensemble des domaines de la **criminalité traditionnelle** (Trafics d'être humain, trafics de stupéfiants, trafics d'espèces protégées, de biens culturels, de médicaments…) **commis dans l'espace numérique,** devenu un véritable **outil facilitateur** pour les cybercriminels.

De plus en plus organisés, les cybertrafiquants privilégient aujourd'hui le **Dark Web,** garant d'une **anonymisation** complète et complexe leur permettant de se livrer à leurs activités criminelles.

ANONYMISATION
INTRAÇABILITÉ
CONFIDENTIALITÉ

FOCUS SUR LE DARK WEB

Comment y accéder ?

À l'aide d'un moteur de recherche à télécharger et installer sur l'ordinateur. Par exemple, Tor.

Pour qui ?

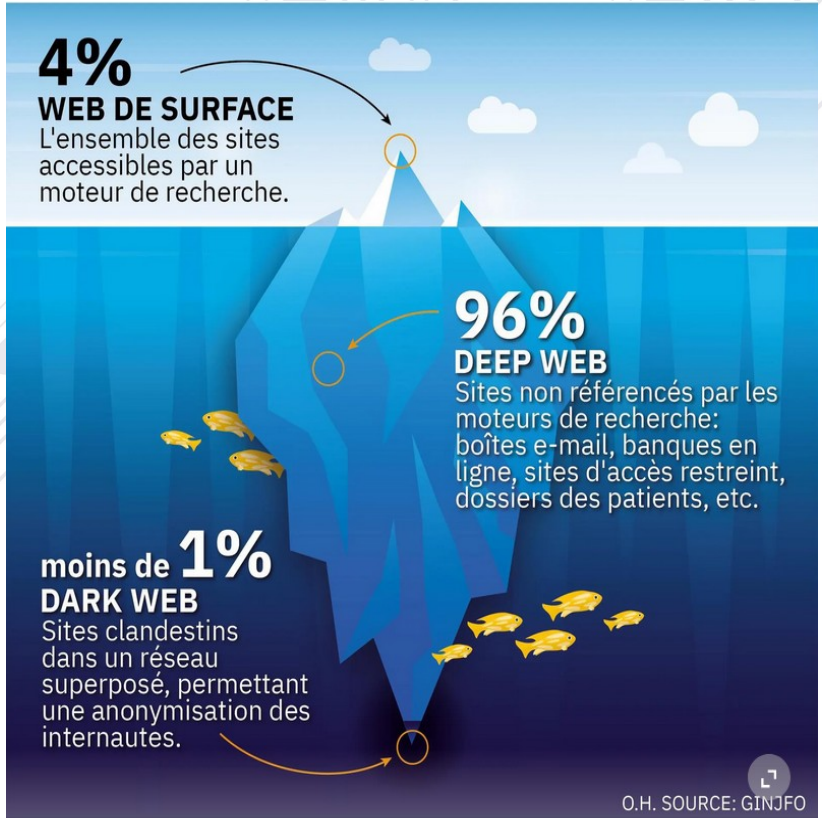
@ Tous les usagers d'internet.
@ Ne nécessite pas de compétences en informatique
@ Démocratisation de l'accès grâce à des « Tutos » que l'on retrouve sur l'internet classique
@ La navigation est libre, elle n'est pas interdite

Pourquoi ?

@ Se livrer à des activités illicites
@ Échapper au contrôle ou filtrage de certains pays ou certains hébergeurs

Que trouve-t-on ?

@ Du contenu licite, mais non régulé et référencé
@ Des contenus et produits illicites



QUELQUES EXEMPLES

Enquêtes

La S.R. de Lyon démantèle un trafic international de stupéfiants sur le Darknet

Auteur : Sirpa, Gendarmerie nationale - publié le 7 mai 2021
Temps de lecture: ≈2 min.

Un réseau familial structuré, l'exportation et de la vente à démantelé par les gendarme

En juillet 2018, un profil suspe de lutte contre les criminalités de livraisons de stupéfiants er Taïwan.

Après avoir réussi à échapper sur une messagerie chiffrée. L confie la poursuite des investi l'antenne du C3N dispose de c complexes sur les outils infor

Des investigations minutieuse des douanes américaines et l

Un laboratoire cl transformation

Les enquêteurs découvrent qu

actuVaucluse

Actu › Provence-Alpes-Côte d'Azur › Vaucluse › Lagnes

Lagnes. Il commandait de la drogue sur le dark web, les gendarmes interceptent le colis

Ce jeudi 2 septembre, la gendarmerie du Vaucluse a annoncé avoir saisi 100 cristaux de MDMA, une drogue dure qu'un habitant de Lagnes avait commandé sur le dark web.

franceinfo: vidéos radio jt magazines

Stupéfiants : cinq personnes interpellées pour avoir vendu via le darknet pour 7 millions d'euros de drogue dans 46 pays, dont la France

Les malfaiteurs utilisaient le fret postal pour faire passer leurs envois de drogue, a appris franceinfo jeudi. Plus de 2 300 envois ont ainsi été découverts, selon la gendarmerie.

franceinfo
Radio France

Une voiture de gendarmerie à Niort (Deux-Sèvres), le 17 mars 2022 (illustration). (NOEMIE GUILLOTIN / RADIO FRANCE)

Cinq personnes ont été interpellées pour avoir vendu via le darknet de la drogue dans 46 pays, dont la France, a appris franceinfo jeudi 21 avril auprès de la gendarmerie nationale. Après avoir été alerté par les autorités américaines, le parquet de Bobigny a ouvert une enquête préliminaire afin de procéder à des vérifications concernant l'affranchissement de lettres suivies. Elle a été confiée à la section de recherches des transports aériens (SRTA).

Au total, ces malfaiteurs ont pu affranchir plus de 2 300 envois pour 700 kg de produits stupéfiants (principalement de la MDMA, du LSD et de l'ecstasy), pour une valeur de près de 7 millions d'euros, estiment les enquêteurs. Les renseignements transmis par les enquêteurs de la SRTA à leurs homologues des services étrangers ont permis la saisie de 13 kg de drogues de synthèse.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

DOUANES & DROITS INDIRECTS

douane.gouv.fr
Le portail de la direction générale des douanes et droits indirects

Mon Espace Personnel
Se connecter S'inscrire

Particuliers Professionnels La douane Presse Services & Aide

Accueil › Actualités de la douane › Démantèlement du forum « Le Monde Parallèle » sur le Darknet

Actualités

Samedi 22 mai 2021
Cyber délinquance • Lutte contre la fraude et les trafics

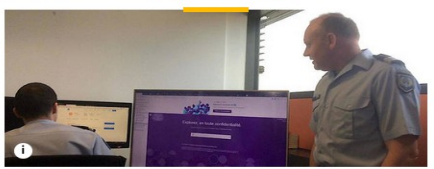
Démantèlement du forum « Le Monde Parallèle » sur le Darknet

MENU Le Point Tech & Net

Quand les cybergendarmes patrouillent sur le dark web

REPORTAGE. Installé à Cergy-Pontoise, le centre de lutte contre les criminalités numériques de la gendarmerie nationale surveille la Toile mondiale…

Par Baudouin Eschapasse



Publié le 22/01/2019 à 15h58 - Modifié le 22/01/2019 à 17h06

Je m'abonne à 1€ le 1er mois

Chez les gendarmes, on les surnomme, mi-sérieux, mi-goguenard : « les experts », en référence à une série télévisée américaine mettant en scène une unité de police scientifique réputée. Les 650 employés du pôle judiciaire de la gendarmerie nationale, implanté depuis mai 2015 sur le terrain de l'ancienne caserne du 22e régiment de dragons, à Cergy-Pontoise, s'en amusent. Mais ils reconnaissent aisément que les services abrités dans ce grand bâtiment de bois et de verre comptent parmi les plus « pointus » de la maréchaussée.

Spectaculaire opération au cœur du «dark web»: 150 pirates interpellés

Par **Christophe Cornevin**
Publié le 26/10/2021 à 11:44, mis à jour le 28/10/2021 à 07:37

Gendarmes et policiers français ont participé, sous l'égide d'Europol, à une opération planétaire débouchant sur l'interpellation de 150 cybercriminels dans le monde.

Au terme de plusieurs mois d'une traque mondiale menée dans le plus grand secret, les services de police et de gendarmerie de neuf pays viennent de réaliser un spectaculaire coup de filet au cœur même du «dark web». Là, dans les abysses de la Toile où les trafiquants pensaient pouvoir prospérer en toute anonymat, les agents spécialisés ont arrêté pas moins de 150 personnes impliquées dans la vente ou l'achat de plusieurs dizaines de milliers de biens et de services correspondant à toutes les facettes du crime organisé.

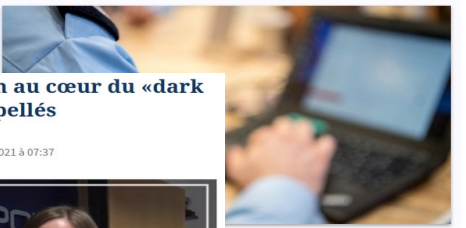
GENDinfo

ACCUEIL ACTUALITÉS SUR LE TERRAIN PAROLES DE GENDARMES ENQUÊTES DOSSIE

Enquêtes

Les cyber enquêteurs européens chassent les trafiquants du Darkweb

Auteur : Antoine Faure - publié le 28 octobre 2021
Temps de lecture: ≈2 min.



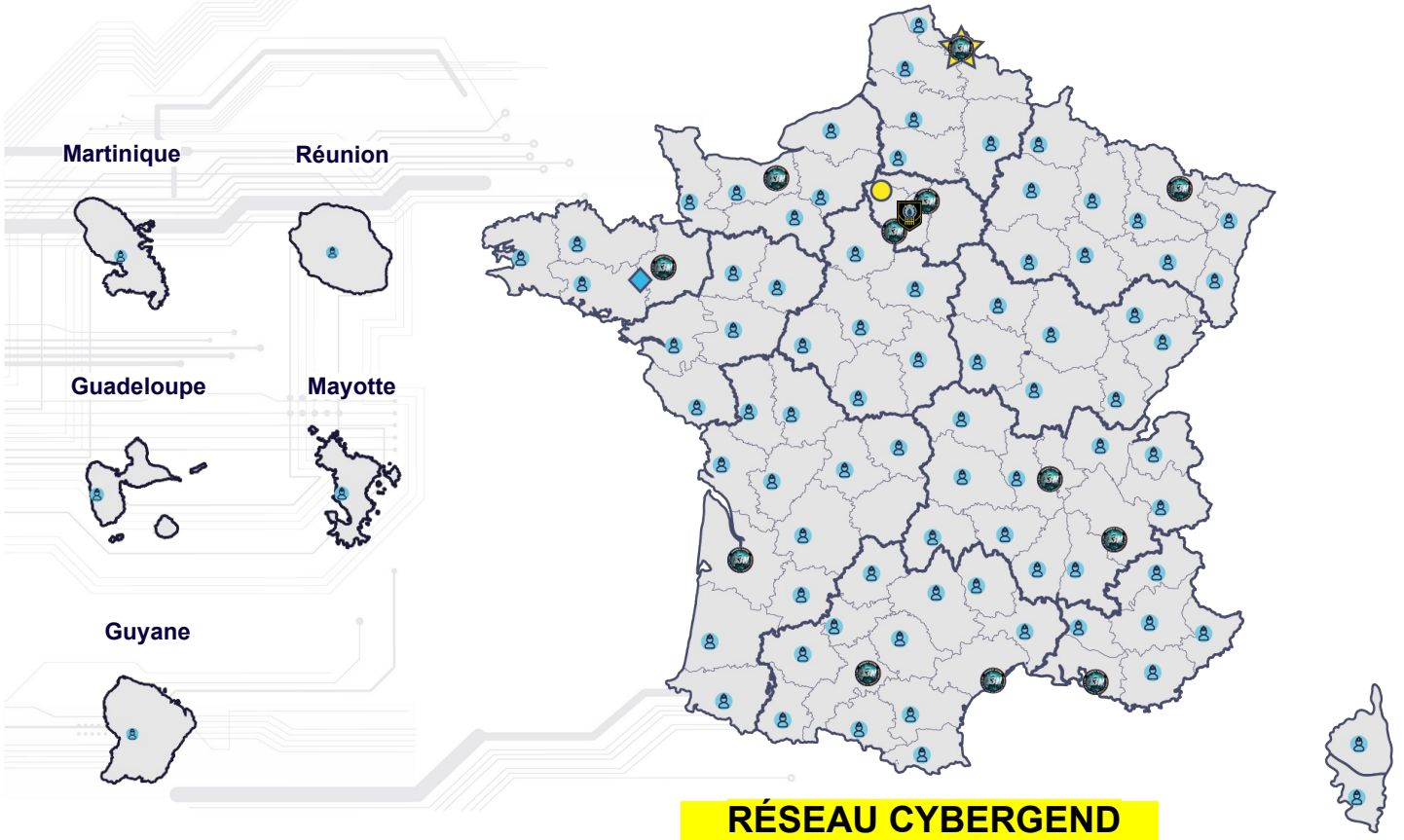
opéenne de police Europol, avec la reux pays, dont les enquêteurs de la tion de plus de 150 suspects qui se livraient de code de l'opération : DarkHunTOR.

e du commerce illégal sur le Web que vient enne de police Europol, basée à La Haye. Un de plus de 150 suspects. Et ce n'est qu'un

oins, ainsi que de la drogue et des armes ont grosses à ce jour concernant la version ».

séparées, mais complémentaires, en uisse, aux Pays-Bas, au Royaume-Uni et aux

UNE ALLONGE TERRITORIALE POUR UNE SÉCURITÉ NUMÉRIQUE DE PROXIMITÉ



RÉSEAU CYBERGEND

Légende

- **Etat-major** — Campus Cyber / Sèvres
- **SOLC**
- **Antennes C3N**
- **Centre de formation cyber** — Campus cyber de Lille
- **Division des opérations + Division technique** — Pontoise
- **Brigade numérique** — Rennes

4 MISSIONS DE LA GENDARMERIE DANS LE CYBERESPACE RÉPARTIES EN 4 COMPOSANTES DU COMCYBERGEND

Investigations & interventions numériques

Conduire les **investigations judiciaires** et mener des **actions de veille** dans l'espace numérique

Appui et opérations numériques

Traitement de la preuve numérique, appui aux enquêteurs et **développement des outils** informatiques

Prévention et proximité numérique

Assurer la **fonction contact** sur l'espace numérique tout en menant des **actions de prévention et de protection** contre les cybermenaces.

Stratégie et partenariats

Coordonner et animer le réseau cybergend, **développement des partenariats & coopération** internationale et **gestion de crises cyber** et des grands évènements

PRINCIPE DE SUBSIDIARITÉ ASSOCIÉ À UNE CAPACITÉ DE GESTION DE CRISE COMPLÉMENTAIRE

APPUI DU GIGN

APPUI RÉGIONAL

Niveau national

- Stratégie numérique
- Proximité numérique
- Investigations numériques
- Expertise numérique

Officiers de liaison
(*Armées, DGSE, etc*).

Niveau régional

- Antennes du C3N
- **Groupes cyber** des autres SR + des offices
- **Brigade numérique**

12
*(cible en 2027 = **30**)*

Niveau départemental

Sections opérationnelles de lutte contre les cybermenaces **SOLC**

3 NTECH

Niveau local

Enquêteurs numériques de proximité « ***cybergendarmes*** »

8 500
*(cible en 2024 = **10 000**)*

+ 350
« CyberRéservistes »

MERCI POUR VOTRE ATTENTION

Pour un pré-diagnostic cyber
Vous pouvez nous contacter à l'adresse :

cybermenaces-ggd76@gendarmerie.interieur.gouv.fr

CYBER MOIS

#Répondre présent pour la population, par les cybergendarmes

Vous êtes témoin ou victime : comment réagir ?

Victime

URGENT Agression physique – préjudice important	**17 ou 112**
NON URGENT Préjudice matériel et harcèlement	***www.pre-plainte-en-ligne.gouv.fr***
Escroquerie par Carte Bancaire (avant ou sans dépôt de plainte)	**Perceval gendarmerie** *www.service-public.fr*
e-Escroqueries (avant ou sans dépôt de plainte)	**Thésée police** *www.service-public.fr*
Cyberattaques (avant ou sans dépôt de plainte)	**Cybermalveillance** *www.cybermalveillance.gouv.fr*

Témoin

Questions à poser	**Brigade Numérique Gendarmerie** *www.gendarmerie.interieur.gouv.fr*
SIGNALER des contenus illicites sur internet	**PHAROS** *www.internet-signalement.gouv.fr*
SIGNALER des spams	**Signal Spam** *www.signal-spam.fr*

NORMANDIE CYBER

CENTRE DE RÉPONSE AUX INCIDENTS CYBER

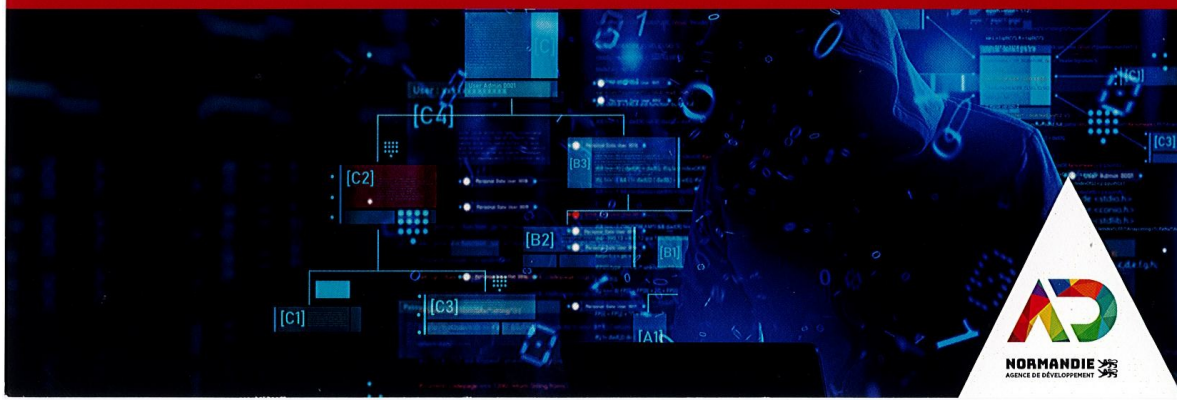
Avec le soutien de :

RÉGION NORMANDIE

ANSSI

NUMÉRO D'APPEL D'URGENCE [service gratuit - prix d'un appel local]

0 808 800 001



NORMANDIE CYBER

CENTRE DE RÉPONSE AUX INCIDENTS CYBER

NORMANDIE CYBER est un centre de réponse de proximité destiné aux entreprises et collectivités de taille intermédiaire pour les accompagner dans toutes leurs démarches en matière de sécurité numérique.

Ayez le réflexe de nous contacter au

0 808 800 001

Une offre de service assurée par l'AD Normandie, en partenariat avec l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).


ACTION DE LA GENDARMERIE
DANS LE CYBERESPACE
2023 – Région Normandie
CYBER
MOIS

UN ÉCOSYSTÈME CYBERCRIMINEL PLUS SOPHISTIQUÉ ET PROFESSIONNEL

Une menace sérieuse…

CYBERMENACES 2022

94 266

Total des faits cyber en gendarmerie

- **64 464** escroqueries et abus de confiance
- **6 424** atteintes à la dignité et à la personnalité
- **5 530** atteintes aux STAD (systèmes de traitement automatisé de données)
- **5 012** menaces et chantages
- **1 178** atteintes aux mineurs

Source : gendarmerie nationale

1 plainte / 250 faits tentés ou commis.

6 000 Md€
coût mondial
de la cyberdélinquance.

…trop peu prise en compte

Une menace numérique infinie, rapide, protéiforme, internationale et… dangereuse pour la stabilité démocratique

64,6 % de la population mondiale utilise **internet**

59,9 % de la population mondiale utilise les **réseaux sociaux**
13,5 nouveaux usagers / seconde !

29 milliards d'**objets connectés** d'ici 2030

LES PRINCIPALES CYBERMENACES

CYBERMENACE = ADVERSAIRE + VULNÉRABILITÉ(S) + MODE D'ACTION

ADVERSAIRES

- États-nations
- Menaces internes
- Cybercriminels
- Amateurs de sensations fortes
- Groupes terroristes
- Hacktivistes

Motivations

- Mécontentement
- Satisfaction
- Violence idéologique
- Idéologique
- Gains financiers
- Géopolitique

VULNÉRABILITÉS

- Failles humaines

Exploitation d'une erreur ou d'un comportement humain :
- *brancher une clé USB inconnue*
- *hameçonnage*
- *fraude au président*

Absence de culture cyber des personnels

- Failles techniques

- Problème de mises à jour
- Mauvaise sauvegarde des données
- absence de confidentialité
- mauvaise gestion de la disponibilité

- Failles physiques

- Manque de surveillance des accès aux serveurs
- Absence ou mauvais contrôle et identification des personnels
- Non application des règles d'inclusion et d'exclusion
- Problème de protection des locaux

MODES D'ACTION

- Ingénierie sociale
  82 % des violations de données reposent sur un facteur humain
- Utilisation d'outils pour rançonner les victimes
  60 % des organisations ont payé la rançon
- Saturation d'un réseau, d'un système, d'un service
- Logiciels malveillants
  En juin 2022, Plus de 10 millions de téléchargements par le biais de logiciels publicitaires
- Attaques sur la chaîne d'approvisionnement
  En 2021, ils représentent 17 % des attaques
- Campagne de désinformation / Défacement de site internet

MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

Gendarmerie nationale

LE RANÇONGICIEL

Un rançongiciel ou *ransomware* est un **logiciel malveillant** qui bloque l'accès à l'ordinateur ou à des fichiers en les **chiffrant** et qui réclame à la victime le paiement d'une **rançon** pour en obtenir de nouveau l'accès.

Motivations

Extorsion/Atteinte à l'image

Moyens d'action

- Vulnérabilités
- Campagnes d'hameçonnage ciblé
- Attaque par force brute sur les réseaux de l'entreprise

Effets

- Chiffrement des données
- Exfiltration des données
- Effacement des sauvegardes
- Suppression des traces

Impacts

Récupération potentielle d'une partie ou de toutes les données

OU

- Publication de données
- Perte de données

Une attaque par rançongiciel

toutes les 11 secondes dans le monde....

58 secondes...

Moins de 1000 euros....

LE RANÇONGICIEL

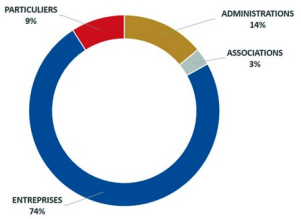
308 … attaques **enregistrées** en 2021 par la gendarmerie

36 % … des faits cyber r**ecensés** en 2021 par la gendarmerie

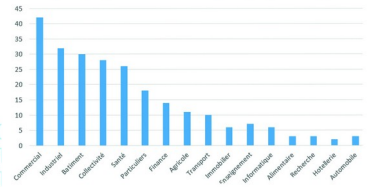
30 % … des victimes auraient **payé** la rançon

1000 … attaques auraient **abouti** en 2021 et toutes n'ont pas fait l'objet d'un dépôt de plainte…

Typologie des victimes



Typologie des secteurs



Typologie des secteurs ciblés en 2022
(Source : données judiciaires Gendarmerie nationale)

QUELQUES EXEMPLES

Essonne : l'hôpital Sud Francilien victime d'une cyberattaque, une rançon de 10 millions de dollars demandée

Les pirates informatiques ont réussi à bloquer tout le réseau informatique de l'hôpital.

Pierre de Cossette - franceinfo
Radio France

Publié le 22/08/2022 11:12 Mis à jour le 22/08/2022 11:42

Corse: cyberattaque d'un hôpital, les soins de radiologie et oncologie suspendus

Par Le Figaro avec AFP
Publié le 29/03/2022 à 16:24, mis à jour le 29/03/2022 à 16:44

Ecouter cet article

LADEPECHE.fr

Lot : trois hôpitaux victimes d'une tentative d'arnaque, les gendarmes contre-attaquent

Les Echos

Idées Économie Politique Entreprises Finance - Marchés Bourse Monde Tech-Médias Start-up Régions Patrimoine

En Allemagne, une première cyberattaque mortelle

L'attaque informatique contre l'hôpital de Düsseldorf s'est terminée par le décès d'une patiente en état critique. Disparus dans la nature, le ou les coupables font l'objet d'une enquête pour « homicide par négligence ».

Lire plus tard Commenter Partager Allemagne Florence Parly

La Ville et l'agglomération de Saumur victimes d'une cyberattaque

La Ville et la communauté d'agglomération de Saumur (Maine-et-Loire) l'ont annoncé dans un communiqué commun : elles font l'objet d'une cyberattaque depuis ce mercredi matin, 23 mars. Elles ont déposé plainte.

Ouest-France
Vincent COTINAT
Publié le 23/03/2022 à 19h33

le Parisien

High-tech

La ville d'Angers paralysée par une cyberattaque

Des pirates ont déployé un rançongiciel qui affecte tous les serveurs et fait tourner les services municipaux au ralenti.

Illustration. Les services municipaux d'Angers sont affectés par une cyberattaque par rançongiciel. LP/Olivier Arandel

ouest france

Seine-Saint-Denis. Victime d'une cyberattaque, Bondy estime les dommages à 1,5 million d'euros

En novembre 2020, Bondy (Seine-Saint-Denis) avait été victime d'une cyberattaque. Depuis, la ville, qui a dû investir 1,5 milli
remise de cette situation, con

la gazette

Ouest-France
avec NG
Publié le 12/07/2022 à 14h24

Abonnez-vous

ÉCOUTER LIRE PLUS TARD PARTAGER NEWSLETTER LA MATINALE

ACCUEIL > CLUB TECHNI.CITÉS > ACTUALITÉS TECHNIQUE > TOUTE L'ACTU TECHNIQUE > ACTUS EXPERTS TECHNIQUE > Une cyberattaque coûte 550 000 euros à la ville de Chalon-sur-Saône

CYBERSÉCURITÉ

Une cyberattaque coûte 550 000 euros à la ville de Chalon-sur-Saône

Publié le 29/07/2021 • Par Alexandre Lécheret • dans : actus experts technique, Régions

Annecy : Deux mois après la cyberattaque, les services informatiques de la ville toujours impactés

HACKER L'ensemble des sites de la ville devraient être reconstruits d'ici le 31 mars prochain

20 Minutes avec agence | Publié le 08/02/22 à 12h37 — Mis à jour le 08/02/22 à 12h37

2 commentaires 21 partages

À LIRE AUSSI

Écouter cet article Annecy : Deux mois après la cyberattaque, les services informatiques de l

Victimes d'une cyberattaque en novembre dernier, les services informatiques de la ville d'Annecy (Haute-Savoie) vont être encore perturbés pendant plusieurs semaines. L'objectif est pour l'heure de reconstruire la sécurité numérique, révèle Le Dauphiné Libéré.

icipal du 20 juillet, le -Saône a annoncé le ue subie par la ville agglomération en eurs embauches sont

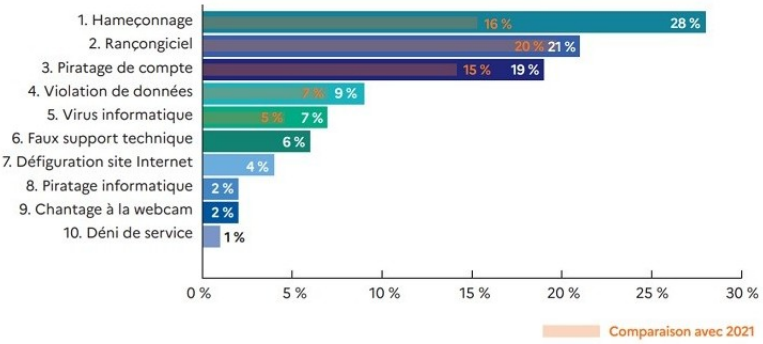
ZOOM SUR LES COLLECTIVITES TERRITORIALES

En 2022, 3510 collectivités sont venues chercher une assistance en ligne ce qui représente une augmentation de 67 %

Source : cybermalveillance.gouv.fr

23% des rançongiciels traités ou rapportés à l'ANSSI en 2022 émanent de collectivités territoriales (2ème place devant les établissements publics de santé 10 %)

Source : ANSSI



Principales recherches d'assistance pour les collectivités et administrations

Source : cybermalveillance.gouv.fr

QUELQUES CONSEILS...

Je suis victime d'un rançongiciel

1. **Déconnecter** mon appareil d'internet et du réseau informatique
2. Au travail, **alerter** immédiatement le service ou prestataire informatique
3. **Ne pas payer** la rançon
4. **Conserver** les preuves numériques en neutralisant le matériel infecté
5. **Déposer** plainte
6. Faites-vous assister au besoin par des professionnels qualifiés

Je me protège d'une attaque

1. **Sensibiliser** mes proches et mes collaborateurs
2. **Appliquer régulièrement** les mises à jour de sécurité
3. **Tenir à jour** son antivirus
4. **Se méfier** des e-mails douteux
5. **Ne pas installer** des applications ou logiciels à l'origine douteuse
6. **Privilégier** une navigation sécurisée sur le Web et **séparer** l'usage personnel de l'usage professionnel
7. **Sauvegarder** régulièrement ses données sur un support amovible
8. **Privilégier** l'utilisation d'un compte utilisateur pour les tâches courantes
9. **Utiliser** des mots de passe complexes et les **changer** régulièrement
10. **Éteindre** l'ordinateur en cas de non-utilisation

LES ESCROQUERIES BASÉES SUR L'USURPATION D'IDENTITÉ

Ensemble des techniques frauduleuses destinées à **leurrer** l'internaute pour l'**inciter à communiquer** des données personnelles et/ou bancaires **en se faisant passer pour un tiers de confiance.**

MAIL

L'**hameçonnage**
L' **harponnage**
L'**arnaque au président…**

SMS

Le **Smishing**

APPEL

Le **Vishing**

QUELQUES CHIFFRES

1ère

L'hameçonnage est la 1ère Cybermalveillance tous publics confondus

Source : www.cybermalveillance.gouv.fr

96 %

… des escroqueries sont réalisées par mail

Source : www.tessian.com

39 %

… des faits d'escroquerie et abus de confiance en gendarmerie ont une origine cyber

Source : gendarmerie nationale

800

… signalements par jour d'escroquerie à la carte bancaire sur PERCEV@L

Source : Perceval – Gendarmerie nationale

QUELQUES EXEMPLES

L'Assurance Maladie — mon compte — mon parcours d'assuré

Bonjour ,

Nous vous informons que vous avez un remboursement en attente d'un montant de **169,20 €** sur votre espace personnel.

La carte enregistrée sur votre espace personnel n'a pas été créditée pour le motif suivant :

Le numéro de mobile enregistré sur votre espace personnel ne correspond pas à celui associé à votre compte bancaire.

Détails de remboursement:

Référence : AWL-20/982KDJ

Monta

Pour

méth

Votre

18 53

Exe

ouest france — Rechercher ville, actualité, fait divers...

Accueil / Faits divers / Arnaques

Une arnaque à la carte Vitale cible les victimes par SMS

Une nouvelle arnaque à la carte Vitale s'est massivement répandue ces derniers mois. Les victimes sont contactées par SMS pour renouveler ce document et doivent préalablement fournir des informations à caractère personnel.

Ouest-France
Maxime FETTWEIS
Publié le 21/04/2022 à 11h00

Abonnez-vous

ÉCOUTER
LIRE PLUS TARD
PARTAGER
NEWSLETTER TU L'AS LU ?

Une nouvelle arnaque à la carte Vitale aurait déjà ciblé plusieurs milliers de personnes | CHARLES JOSSE / OUEST-FRANCE

Une campagne de phishing imitant de grands groupes sévit en France

Un hackeur a lancé depuis quelques mois une vaste opération de phishing par SMS pour arnaquer les internautes français, rapporte Phonandroid.

Par LePoint.fr

Publié le 14/06/2022 à 02h17 - Modifié le 14/06/2022 à 06h36

Je m'abonne à **1€** le 1er mois

Netflix, la Fnac, la Banque populaire, la Caisse d'épargne, l'Assurance maladie... Un pirate informatique a récemment usurpé les noms de grands sites, marques ou services publics pour mettre au point une campagne de phishing et arnaquer des centaines et des centaines d'internautes français. Le hackeur, plus malin que les arnaqueurs ordinaires, a commencé à opérer par SMS en se faisant passer pour l'Assurance maladie et en tentant de convaincre ses victimes que leurs cartes vitales étaient périmées, rapporte Phonandroid.

Dans chaque SMS, le pirate informatique a intégré un lien qui renvoie vers un site imitant à la quasi-perfection l'interface de l'Assurance maladie. À quelques détails près : l'URL n'est pas le bon et les « L » du texte ont été remplacés par des « i » majuscules. Cette subtilité, repérée par le journaliste spécialisé Damien Bancal, est trompeuse à l'œil nu, mais elle permet aussi de passer à travers les filets des outils de surveillance en matière de cybercriminalité.

ouest france — Rechercher ville, actualité, fait divers...

Accueil / High Tech / Téléphonie

Attention, ces SMS de réception de colis cachent une campagne d'hameçonnage de pirates chinois

Une campagne d'hameçonn
actuellement sur le territoire
dérober les données des sn

Ouest-France
avec agence
Publié le 04/08/2022 à 12h52

Abonnez-vous

ÉCOUTER
LIRE PLUS TARD
PARTAGER
NEWSLETTER GAMING

MENU — Le Point

Le monde judiciaire français ciblé par une vaste cyberattaque

Magistrats, procureurs, avocats... De nombreuses personnes chargées de dossiers sensibles ont été visées par des hackers. Une enquête a été ouverte.

Source AFP

Publié le 06/09/2020 à 15h15 - Modifié le 06/09/2020 à 18h22

Je m'abonne à **1€** le 1er mois

Le monde judiciaire français sous la menace de hackers. Le parquet de Paris a ouvert une enquête préliminaire, vendredi 4 septembre 2020, après une cyberattaque qui a tenté d'atteindre des acteurs de la justice, a en effet appris l'Agence France-Presse dimanche de source judiciaire.

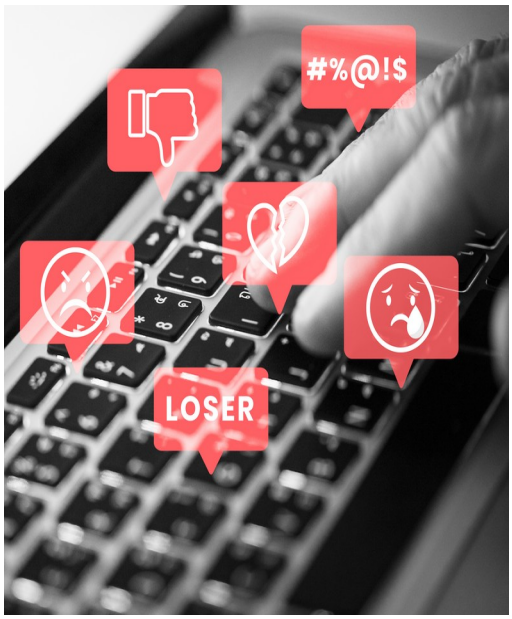
Selon *Le Journal du dimanche*, cette cyberattaque a ciblé le procureur de Paris, Rémy Heitz, mais aussi des magistrats ou des avocats parisiens chargés de dossiers sensibles. Une source proche du dossier a toutefois précisé que cette attaque était d'ampleur plus large, ne se limitant pas au tribunal judiciaire de Paris.

« E-mail curieux »

FOVI – L'ARNAQUE AU PRÉSIDENT

L'**escroquerie aux faux ordres de virement** (FOVI) désigne un type d'arnaque qui, par **persuasion**, **menaces** ou **pressions** diverses, vise à amener la victime à **réaliser un virement** de fonds non planifié. Parfois présenté comme émanant d'un dirigeant et ayant un **caractère « urgent et confidentiel »**, on parle alors « d'**arnaque au Président** ».
Dans certains cas, cette fraude fait suite au **piratage** et à l'utilisation de la messagerie de la personne ou entité usurpée.

LE CYBERHARCÈLEMENT



On parle de cyberharcèlement lorsqu'une ou plusieurs personnes utilisent les **moyens de communication numériques,** de manière **délibérée et répétée** dans le temps, pour **porter atteinte à l'intégrité morale** d'une personne.

Les moyens → Téléphones portables, messageries instantanées, forums, chats, jeux en ligne, e-mails, réseaux sociaux, sites de partage…

Les formes → Intimidations, insultes, moqueries, menaces, propagation rumeurs, piratage de compte, usurpation d'identité, publication de photos ou vidéos…

LE CYBERHARCÈLEMENT

20 % des **6/18 ans** ont déjà été confrontés à une situation de cyberharcèlement

Source : Association e-Enfance

205 973 … écoliers et collégiens ont été sensibilisés en 2021 aux dangers d'internet dans le cadre des opérations « permis internet » de la gendarmerie nationale

Source : gendarmerie nationale

40 % … des moins de 50 ans disent avoir subi des attaques répétées sur les réseaux sociaux.

Source : https://fr.statista.com

693 … faits de cyberharcèlement enregistrés en 2021 par la gendarmerie. Soit une augmentation de 12 % !

Source : gendarmerie nationale

QUELQUES CONSEILS…

Je suis victime de cyberharcèlement :

1. **Ne pas répondre** pour ne pas attiser la haine
2. **Se confier** à une personne de confiance, ne pas rester seul
3. **Conserver** les preuves numériques (captures d'écran)
4. **Se protéger** en se déconnectant des réseaux, **bloquer** les auteurs
5. **Demander** le retrait des contenus aux hébergeurs
6. **Déposer** plainte

Je me protège du cyberharcèlement :

1. **Sensibiliser** mes proches et mes collaborateurs aux dangers de l'utilisation d'internet et des réseaux sociaux
2. **Protéger** sa vie privée et professionnelle sur internet et sur les réseaux sociaux
3. Témoin, ne **pas commenter** ou **relayer** les propos, photos ou vidéos
4. **Signaler** les faits de harcèlement et les auteurs

Les dispositifs de signalement en ligne :
– Plateforme PHAROS
– Contacter la brigade numérique de la gendarmerie ou la plateforme de l'association e-enfance au 3018

LES TRAFICS ILLICITES EN LIGNE

Les trafics illicites en ligne représentent l'ensemble des domaines de la **criminalité traditionnelle** (Trafics d'être humain, trafics de stupéfiants, trafics d'espèces protégées, de biens culturels, de médicaments…) **commis dans l'espace numérique,** devenu un véritable **outil facilitateur** pour les cybercriminels.

De plus en plus organisés, les cybertrafiquants privilégient aujourd'hui le **Dark Web,** garant d'une **anonymisation** complète et complexe leur permettant de se livrer à leurs activités criminelles.

ANONYMISATION
INTRAÇABILITÉ
CONFIDENTIALITÉ

FOCUS SUR LE DARK WEB

Comment y accéder ?

À l'aide d'un moteur de recherche à télécharger et installer sur l'ordinateur. Par exemple, Tor.

Pour qui ?

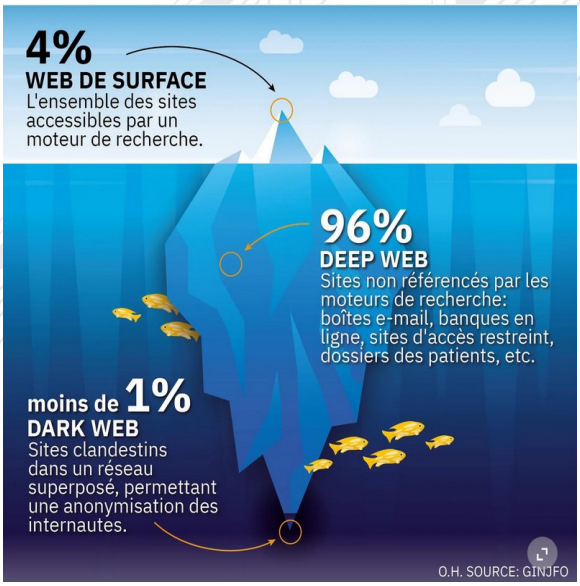
@ Tous les usagers d'internet.
@ Ne nécessite pas de compétences en informatique
@ Démocratisation de l'accès grâce à des « Tutos » que l'on retrouve sur l'internet classique
@ La navigation est libre, elle n'est pas interdite

Pourquoi ?

@ Se livrer à des activités illicites
@ Échapper au contrôle ou filtrage de certains pays ou certains hébergeurs

Que trouve-t-on ?

@ Du contenu licite, mais non régulé et référencé
@ Des contenus et produits illicites



QUELQUES EXEMPLES

Enquêtes

La S.R. de Lyon démantèle un trafic international de stupéfiants sur le Darknet

actuVaucluse

Lagnes. Il commandait de la drogue sur le dark web, les gendarmes interceptent le colis

Ce jeudi 2 septembre, la gendarmerie du Vaucluse a annoncé avoir saisi 100 cristaux de MDMA, une drogue dure qu'un habitant de Lagnes avait commandé sur le dark web.

franceinfo:

Stupéfiants : cinq personnes interpellées pour avoir vendu via le darknet pour 7 millions d'euros de drogue dans 46 pays, dont la France

Les malfaiteurs utilisaient le fret postal pour faire passer leurs envois de drogue, a appris franceinfo jeudi. Plus de 2 300 envois ont ainsi été découverts, selon la gendarmerie.

Cinq personnes ont été interpellées pour avoir vendu via le darknet de la drogue dans 46 pays, dont la France, a appris franceinfo jeudi 21 avril auprès de la gendarmerie nationale. Après avoir été alerté par les autorités américaines, le parquet de Bologne a ouvert une enquête préliminaire afin de procéder à des vérifications concernant l'affranchissement de lettres suivies. Elle a été confiée à la section de recherches des transports aériens (SRTA).

Au total, ces malfaiteurs ont pu affranchir plus de 2 300 envois pour 700 kg de produits stupéfiants (principalement de la MDMA, du LSD et de l'ecstasy), pour une valeur de près de 7 millions d'euros, estiment les enquêteurs. Les renseignements transmis par les enquêteurs de la SRTA à leurs homologues des services étrangers ont permis la saisie de 13 kg de drogues de synthèse.

douane.gouv.fr

Le portail de la direction générale des douanes et droits indirects

Particuliers | Professionnels | La douane | Presse

Actualités

Samedi 22 mai 2021

Cyber délinquance · Lutte contre la fraude et les trafics

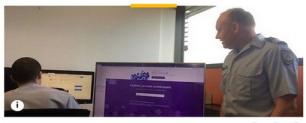
Démantèlement du forum « Le Monde Parallèle » sur le Darknet

Le Point Tech & Net

Quand les cybergendarmes patrouillent sur le dark web

REPORTAGE. Installé à Cergy-Pontoise, le centre de lutte contre les criminalités numériques de la gendarmerie nationale surveille la Toile mondiale…

Par Baudouin Eschapasse



Publié le 22/01/2019 à 15h58 - Modifié le 22/01/2019 à 17h06

Je m'abonne à 1€ le 1er mois

Chez les gendarmes, on les surnomme, mi-sérieux, mi-goguenard : « les experts », en référence à une série télévisée américaine mettant en scène une unité de police scientifique réputée. Les 650 employés du pôle judiciaire de la gendarmerie nationale, implanté depuis mai 2015 sur le terrain de l'ancienne caserne du 22e régiment de dragons, à Cergy-Pontoise, s'en amusent. Mais ils reconnaissent aisément que les services abrités dans ce grand bâtiment de bois et de verre comptent parmi les plus « pointus » de la maréchaussée.

Spectaculaire opération au cœur du «dark web»: 150 pirates interpellés

Par Christophe Cornevin

Publié le 26/10/2021 à 11:44, mis à jour le 28/10/2021 à 07:37

Gendarmes et policiers français ont participé, sous l'égide d'Europol, à une opération planétaire débouchant sur l'interpellation de 150 cybercriminels dans le monde.

Au terme de plusieurs mois d'une traque mondiale menée dans le plus grand secret, les services de police et de gendarmerie de neuf pays viennent de réaliser un spectaculaire coup de filet au cœur même du «dark web». Là, dans les abysses de la Toile où les trafiquants pensaient pouvoir prospérer en tout anonymat, les agents spécialisés ont arrêté pas moins de 150 personnes impliquées dans la vente ou l'achat de plusieurs dizaines de milliers de biens et de services correspondant à toutes les facettes du crime organisé.

GENDinfo

ACCUEIL | ACTUALITÉS | SUR LE TERRAIN | PAROLES DE GENDARMES | ENQUÊTES | DOSSI

Enquêtes

Les cyber enquêteurs européens chassent les trafiquants du Darkweb

Auteur : Antoine Faure - publié le 28 octobre 2021

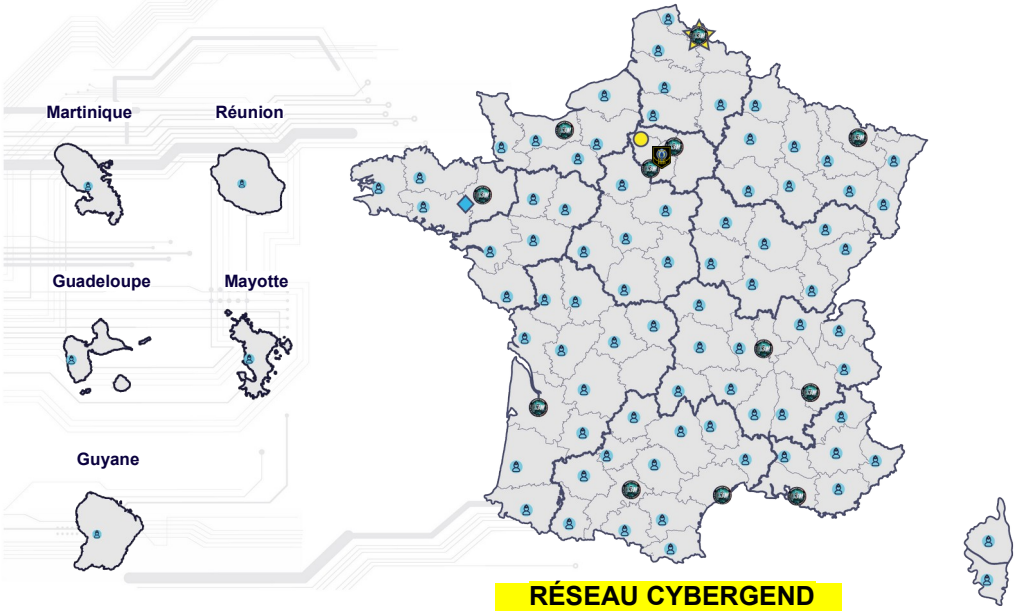
Temps de lecture: ≈2 min.

21

MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

Gendarmerie nationale

UNE ALLONGE TERRITORIALE POUR UNE SÉCURITÉ NUMÉRIQUE DE PROXIMITÉ



RÉSEAU CYBERGEND

Légende

- **Etat-major**
  Campus Cyber / Sèvres
- **SOLC**
- **Antennes C3N**
- **Centre de formation cyber**
  Campus cyber de Lille
- **Division des opérations + Division technique**
  Pontoise
- **Brigade numérique**
  Rennes

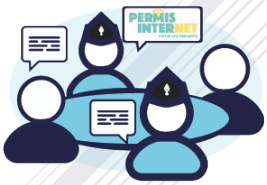
4 MISSIONS DE LA GENDARMERIE DANS LE CYBERESPACE RÉPARTIES EN 4 COMPOSANTES DU COMCYBERGEND

Investigations & interventions numériques

Conduire les **investigations judiciaires** et mener des **actions de veille** dans l'espace numérique

Appui et opérations numériques

Traitement de la preuve numérique, appui aux enquêteurs et **développement des outils** informatiques



Prévention et proximité numérique

Assurer la **fonction contact** sur l'espace numérique tout en menant des **actions de prévention et de protection** contre les cybermenaces.

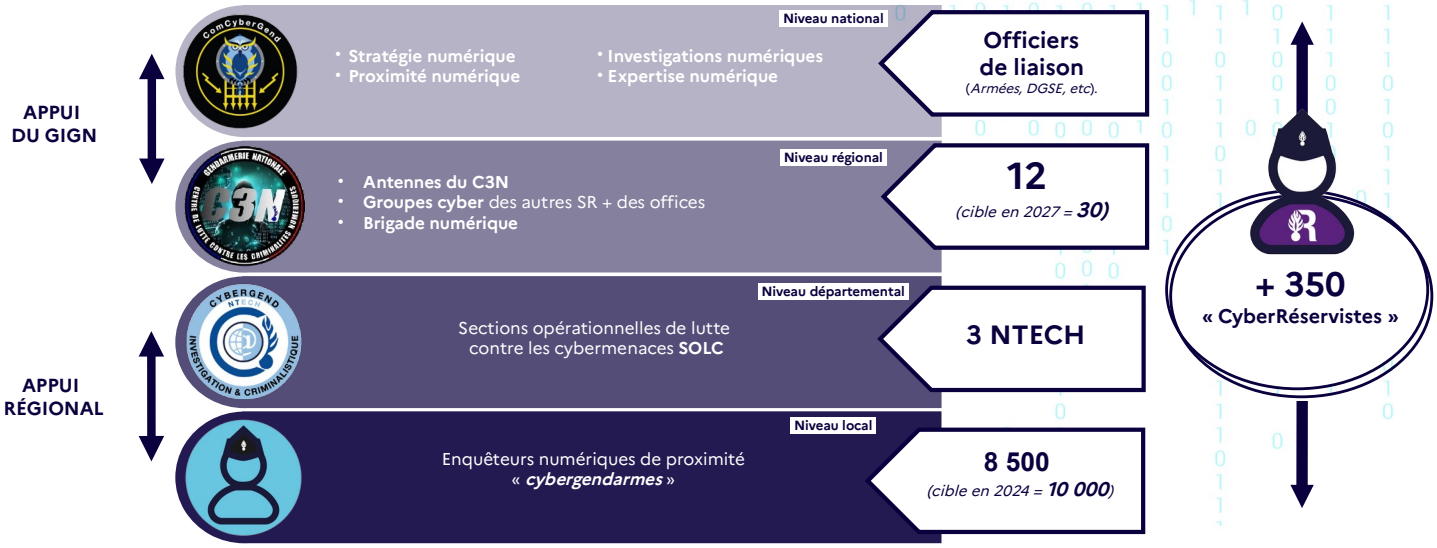
Stratégie et partenariats

Coordonner et animer le réseau cybergend, **développement des partenariats & coopération** internationale et **gestion de crises cyber** et des grands évènements

MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

Gendarmerie nationale

PRINCIPE DE SUBSIDIARITÉ ASSOCIÉ À UNE CAPACITÉ DE GESTION DE CRISE COMPLÉMENTAIRE



MERCI POUR VOTRE ATTENTION

Pour un pré-diagnostic cyber
Vous pouvez nous contacter à l'adresse :

cybermenaces-ggd76@gendarmerie.interieur.gouv.fr

CYBER MOIS

#Répondre présent pour la population, par les cybergendarmes

Vous êtes témoin ou victime : comment réagir ?

Victime	**URGENT** Agression physique – préjudice important	17 ou 112
	NON URGENT Préjudice matériel et harcèlement	*www.pre-plainte-en-ligne.gouv.fr*
	Escroquerie par Carte Bancaire (avant ou sans dépôt de plainte)	**Perceval gendarmerie** *www.service-public.fr*
	e-Escroqueries (avant ou sans dépôt de plainte)	**Thésée police** *www.service-public.fr*
	Cyberattaques (avant ou sans dépôt de plainte)	**Cybermalveillance** *www.cybermalveillance.gouv.fr*
Témoin	**Questions à poser**	**Brigade Numérique Gendarmerie** *www.gendarmerie.interieur.gouv.fr*
	SIGNALER des contenus illicites sur internet	**PHAROS** *www.internet-signalement.gouv.fr*
	SIGNALER des spams	**Signal Spam** *www.signal-spam.fr*