RÉPUBLIQUE FRANÇAISE

Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR

Assistance et prévention en sécurité numérique

Dispositif national de sensibilisation, prévention et d'assistance aux victimes

CYBER CERCLE

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

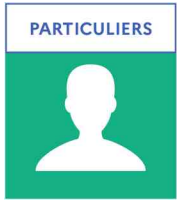
LES MISSIONS DU DISPOSITIF

1. **ASSISTER LES VICTIMES** d'actes de cybermalveillance

2. **INFORMER & SENSIBILISER** à la sécurité numérique

3. **OBSERVER & ANTICIPER** le risque numérique

QUI EST CONCERNÉ ?



RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

CYBERMALVEILLANCE.GOUV.FR EN QUELQUES CHIFFRES

56

organisations membres
(publiques et privées) du GIP ACYMA

1250

prestataires référencés
sur l'ensemble du territoire

173 000

victimes assistées
En 2021 (+65%)

2 482 000

visiteurs uniques
en 2021 (+101%)

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

56 MEMBRES RÉUNIS AUTOUR D'UN PARTENARIAT PUBLIC- PRIVÉ

PREMIER MINISTRE

MINISTÈRE DE L'ÉCONOMIE, DES FINANCES ET DE LA SOUVERAINETÉ INDUSTRIELLE ET NUMÉRIQUE

MINISTÈRE DE L'INTÉRIEUR

MINISTÈRE DE LA JUSTICE

MINISTÈRE DE L'ÉDUCATION NATIONALE ET DE LA JEUNESSE

MINISTÈRE DES ARMÉES

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

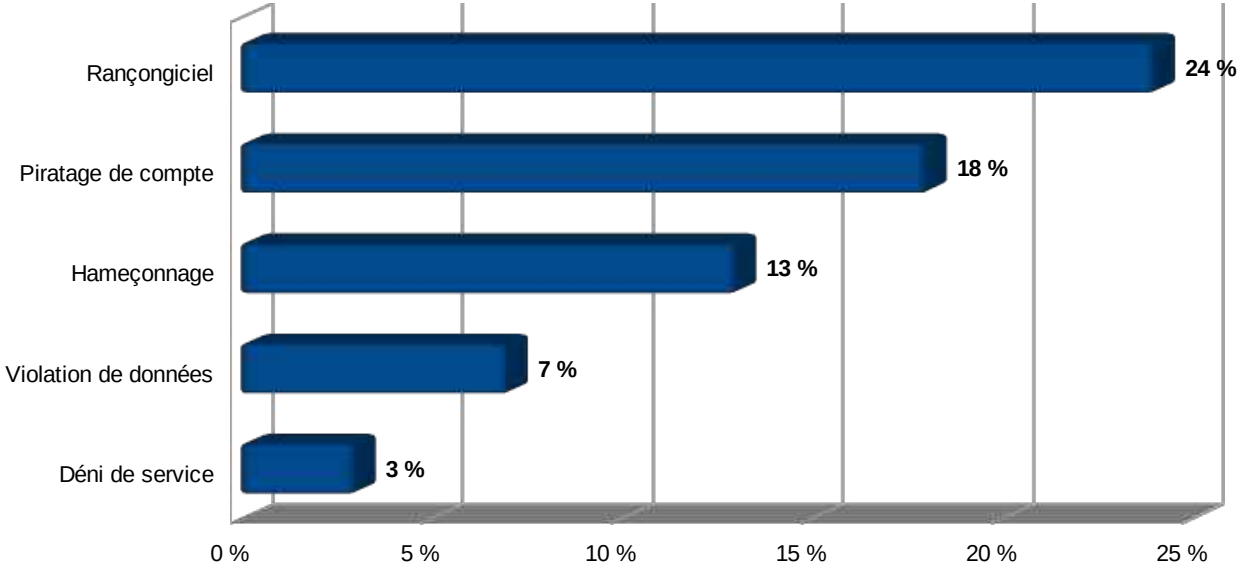
Parcours d'assistance aux victimes et tendances des menaces cyber

LE PARCOURS VICTIME

- **Un outil destiné à la remédiation**
  - Établir un diagnostic
    - Avec des questions adaptatives
    - Mettre un nom sur la cybermalveillance
  - Proposer des conseils personnalisés
    - Premières mesures
    - Identifier le bon interlocuteur
  - Mettre en relation
    - Avec un prestataire référencé (assistance)
    - Proximité géographique
  - Un outil qui évolue
    - Traitement de la demande et satisfaction

PRINCIPALES RECHERCHES D'ASSISTANCE EN 2021

Pour les entreprises et associations :



49
types d'incidents
traités

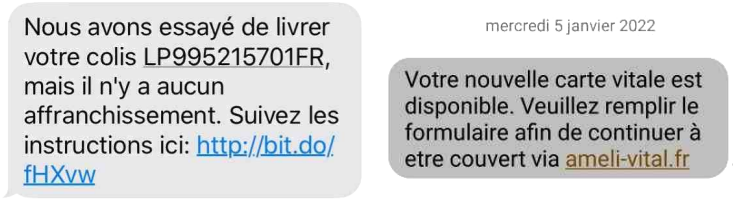
DES CYBERMALVEILLANCES ...

- L'hameçonnage (phishing) : « la mère des attaques »
  - Menace prédominante qui s'est professionnalisée
  - Développement important des attaques par SMS

- Le piratage de compte
  - Origines diverses
  - Cause d'autres malveillances

... QUI S'ADAPTENT AUX CONTEXTES

- Crise sanitaire
- Évènements sportifs, conflits



LES RANÇONGICIELS

- 1ère menace pour les professionnels
- Tous types et tailles d'organisations ciblées en nombre
- Un écosystème cybercriminel redoutable qui fonctionne en cartel
- Pluralité et sophistication
- Vol de données avec menace de divulgation pour accentuer la pression depuis fin 2019

Le Parisien

Hauts-de-Seine

Les hackers de Lockbit 2.0 revendiquent la cyberattaque contre la mairie de Saint-Cloud

Les cybercriminels menacent de publier les données dérobées lors de l'attaque survenue dans la nuit du 20 au 21 janvier. La mairie assure que le rétablissement des systèmes informatiques est en bonne voie. Le groupe de hackers a aussi revendiqué, ce jeudi, une attaque contre le ministère de la Justice.

RÉPUBLIQUE FRANÇAISE

Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR

Assistance et prévention en sécurité numérique

Réagir en cas de Cyber attaque

LES PREMIERS RÉFLEXES

- **Alertez immédiatement** votre support informatique

- **Isolez** les systèmes attaqués

- **Constituez** une équipe de gestion de crise

- **Documentez** les évènements et actions réalisées

PILOTER LA CRISE

- Mettez en place des **solutions de secours**

- **Déclarez** le sinistre
  - Assurance, banque
  - CNIL (dans les 72h si données personnelles impactées)
  - Déposez plainte

- **Identifiez** l'origine et l'étendue de l'attaque puis **corrigez**

- **Gérez votre communication** avec le juste niveau de transparence

SORTIR DE LA CRISE

- **Faites une remise en service** progressive et contrôlée

- **En surveillant son fonctionnement**

- **Tirez les enseignements de l'attaque**
  - Définissez les plans d'action et d'investissements

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

UN SUPPORT MÉTHODOLOGIQUE

- **Pour les dirigeants**
  - Trois étapes clés
  - Une liste de points d'attention essentiels
  - Une aide à la gestion de crise

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/cyberattaque-que-faire-guide-dirigeants

Diagnostiquer et accompagner

LE PARCOURS DE SÉCURISATION

- **Un outil destiné à l'accompagnement**
  - Des TPE-PME / Associations / Collectivités
  - Pour répondre à leurs besoins
    - Installation / maintenance / assistance
  - Dans de nombreux domaines techniques
    - Serveurs, postes fixes/nomades
    - Infrastructure, sauvegarde, site web
    - Téléphonie fixe/mobile
  - Être mis en relation
    - Avec un professionnel labellisé « ExpertCyber »
    - Spécialisé dans le domaine recherché
    - www.securisation.cybermalveillance.gouv.fr

EXPERT CYBER
LABEL SÉCURITÉ NUMÉRIQUE
Cybermalveillance.gouv.fr
RÉPUBLIQUE FRANÇAISE

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

LES ALERTES CYBERSÉCURITÉ

- **Sur les réseaux sociaux « grand public » et professionnels**

- **Via des organisations et réseaux professionnels**


ALERTE CYBERSÉCURITÉ

Failles de sécurité critiques dans les produits Apple

Date de l'alerte : 11 mai 2021

Risque(s)

Vol, voire destruction, de vos données suite à la prise de contrôle à distance de vos équipements concernés.

Description

Des **failles de sécurité critiques** ont été corrigées dans les **systèmes d'exploitation d'Apple** et de son **navigateur Internet Safari**. L'exploitation de ces failles peut permettre la prise de contrôle à distance des équipements concernés et le vol, voire la destruction, d'informations confidentielles par des cybercriminels.

Selon le constructeur, **des attaques en cours exploitant ces vulnérabilités seraient constatées**.

Système(s) concerné(s)

- **macOS Big Sur** : versions antérieures à 11.3.1
- **iOS** : versions antérieures à 14.5.1
- **watchOS** : versions antérieures à 7.4.1
- **iPadOS** : versions antérieures à 14.5.1
- **Apple Safari** : versions antérieures à 14.1

Mesure(s) à prendre

Mettre à jour au plus vite les équipements concernés avec les correctifs de sécurité mis à disposition par Apple.

Procédures

- Pour iOS, iPadOS : https://support.apple.com/fr-fr/HT204204
- Pour MacOS et Safari : https://support.apple.com/fr-fr/HT201541
- Pour watchOS : https://support.apple.com/fr-fr/HT204641

Besoin d'assistance ?

Vous pouvez trouver sur Cybermalveillance.gouv.fr des prestataires de proximité susceptibles de vous apporter leur soutien dans la mise en œuvre de ces mesures en cliquant ici.

Référence(s)

- ANSSI / CERT-FR : https://www.cert.ssi.gouv.fr/actualite/CERTFR-2021-ACT-018/
- CVE-2021-30661 - CVE-2021-30663 - CVE-2021-30665 - CVE-2021-30666

Aller plus loin avec Cybermalveillance.gouv.fr :
Pourquoi et comment bien gérer ses mises à jour ?

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

SENSIBILISATION ET PRÉVENTION

Objectifs :

- Sensibiliser aux risques
- Partager les bonnes pratiques
- Alerter

Publics :

- Particuliers
- Entreprises
- Collectivités

17 thématiques

6 types de contenus :

- Fiches pratiques/réflexes
- Vidéos
- Mémos et infographie
- Alertes sur les réseaux sociaux @cybervictimes
- Articles

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/liste-des-ressources-mises-a-disposition

RÉPUBLIQUE FRANÇAISE

Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR

Assistance et prévention en sécurité numérique

Nos ressources de sensibilisation

www.cybermalveillance.gouv.fr

@cybervictimes

@cybervictimes

@cybermalveillancegouvfr