Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

DOSSIER DE PRESSE

LANCEMENT NATIONAL DU DISPOSITIF D'ASSISTANCE AUX VICTIMES DE CYBERMALVEILLANCE

CYBERMALVEILLANCE.GOUV.FR

@Cybervictimes #CyberMDirect
https://www.cybermalveillance.gouv.fr

17 OCTOBRE 2017

SOMMAIRE

Communiqué de presse

ÉVÉNEMENT
PARIS,17 OCTOBRE

LANCEMENT NATIONAL DE LA PLATEFORME CYBERMALVEILLANCE.GOUV.FR

Dans le cadre du Mois européen de la cybersécurité, le groupement d'intérêt public ACYMA ouvre au niveau national sa plateforme « cybermalveillance.gouv.fr », le dispositif d'assistance aux victimes de cybermalveillance. La conférence du 17 octobre sera l'occasion de revenir sur la phase d'expérimentation dans la région des Hauts-de-France lancée en mai 2017.

724 mises en relation victimes/prestataires au total pendant la phase d'expérimentation
83 % des incidents de cybermalveillance déclarés comme des virus
44 % du total des incidents déclarés « virus » correspondent à des attaques de type rançongiciel

Représentative du territoire national par la diversité du taux d'urbanisation de ses départements et par l'implication des acteurs locaux dans la sécurité du numérique, la région a permis de ressortir un certain nombre de données, confirmant l'importance de la création d'un dispositif s'adressant en priorité aux TPE/PME, particuliers et collectivités territoriales.

LES INTERVENANTS

Louis Gautier, Secrétaire général de la défense et de la sécurité nationale (SGDSN)
Jérôme Notin, Directeur général du Dispositif national d'assistance aux victimes de cybermalveillance
Bernard Spitz, Président de la Fédération Française des Assurances
Mounir Mahjoubi, Secrétaire d'Etat chargé du numérique

LE PROGRAMME

Présentation des enjeux et de la plateforme
Retour d'expérience de l'expérimentation dans les Hauts-de-France
Témoignage d'un membre du GIP ACYMA
Conclusion

La conférence sera également retransmise en direct sur Twitter et Facebook.
#CyberMDirect

LA PLATEFORME « CYBERMALVEILLANCE.GOUV.FR » QU'EST-CE QUE C'EST ?

« Cybermalveillance.gouv.fr » est la solution vers laquelle peuvent se tourner les victimes d'actes de cybermalveillance. C'est le **guichet unique** qui met en relation ces victimes avec des prestataires spécialisés et de proximité, présents sur l'ensemble du territoire national.

Son public ?

Tous les victimes d'attaques informatiques qui ne disposent pas de compétences et/ou de ressources en sécurité numérique : les particuliers, les entreprises (PME et TPE) et les collectivités territoriales. L'actualité récente a montré que ces acteurs sont vulnérables aux attaques informatiques, qui peuvent les affecter directement ou indirectement avec des conséquences parfois dramatiques : vol de données personnelles ou clients, dysfonctionnement voire interruption d'activité aux conséquences économiques et salariales graves, allant jusqu'à la fermeture d'entreprises.

Ses missions ?

• **mettre en relation** des victimes d'actes de cybermalveillance avec des prestataires de proximité susceptibles de réparer leurs systèmes en proposant des solutions adaptées aux besoins identifiés lors d'un diagnostic de la situation réalisé en ligne ;

• **informer et sensibiliser** les internautes à la sécurité du numérique : qu'est-ce qu'un rançongiciel ? Comment me protéger ? Qui alerter en cas de problèmes ? La plateforme « cybermalveillance.gouv.fr » se veut être le portail privilégié de contenus de sensibilisation et d'informations vers laquelle peut se tourner le citoyen numérique ;

• favoriser la création d'un **observatoire du risque numérique** permettant d'analyser l'évolution de la menace cyber et des réponses apportées.

SES SERVICES ?

Ils s'illustrent à travers deux parcours :

* **Parcours 1** « Vous êtes victime d'acte de cybermalveillance » qui propose :
  - un accompagnement à la réalisation d'un diagnostic en ligne pour identifier l'incident de sécurité ;
  - une mise en relation avec les prestataires de proximité susceptibles de les assister techniquement ;
  - une fiche «réflexes» pour comprendre l'incident et les bonnes pratiques à adopter pour s'en prémunir ;
  - les informations à fournir pour le dépôt de plainte auprès des services de police ou de la gendarmerie ;
  - la possibilité de noter et commenter la prestation pour permettre l'évaluation des prestataires.

* **Parcours 2** « Vous êtes un prestataire et vous souhaitez être référencé » qui propose :
  - les renseignements sur votre société ;
  - l'adhésion à une charte d'engagement reprenant les conditions éthiques et pratiques indispensables au référencement sur la plateforme.

Retrouvez plus d'informations sur les parcours « victimes » et « prestataires » dans le dossier de presse du 30 mai 2017 disponible sur www.cybermalveillance.gouv.fr.

Au 17 octobre 2017,
près de **1 123 prestataires** sont référencés sur la plateforme
et couvrent toutes les prestations nécessaires
pour **l'ensemble du territoire français.**

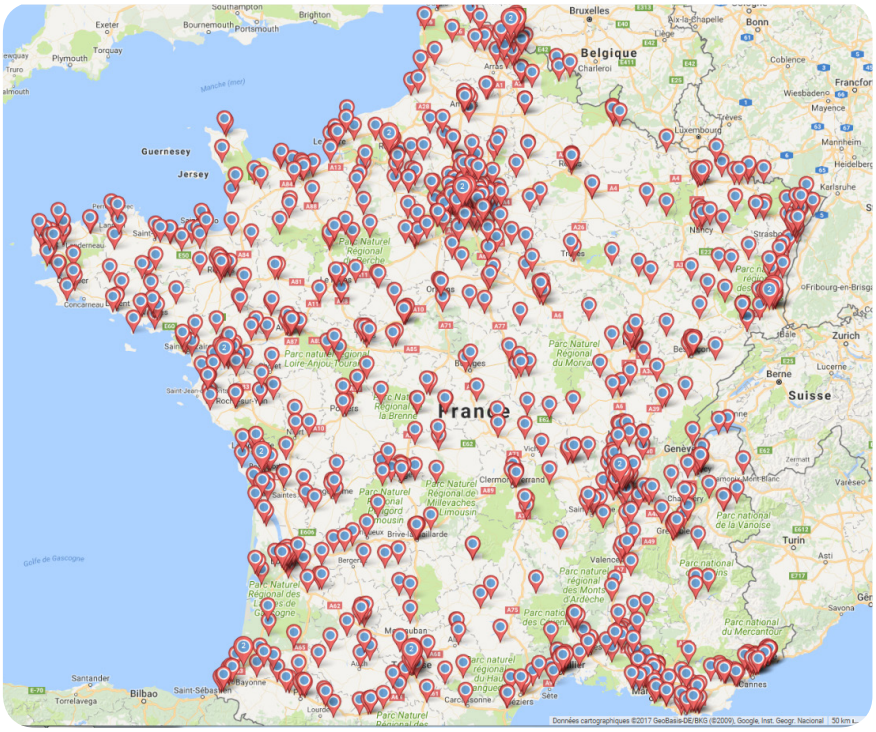

Fig 1 : Carte nationale de prestataires de proximité référencés sur la plateforme.
© GIP_ACYMA

RETOUR D'EXPÉRIENCE
CYBERMALVEILLANCE.GOUV.FR DANS LES HAUTS-DE-FRANCE

Une première phase d'expérimentation de la plateforme « Cybermalveillance.gouv.fr » a été lancée dans la région des Hauts-de-France lancée en **mai 2017**.

Représentative du territoire national par la diversité du taux d'urbanisation de ses départements et par l'implication des acteurs locaux dans la sécurité du numérique, la région a permis de ressortir un certain nombre de données, confirmant l'importance de la création d'un dispositif s'adressant en priorité aux PME/TPE, particuliers et collectivités territoriales.

724 parcours «victimes» depuis la phase d'expérimentation

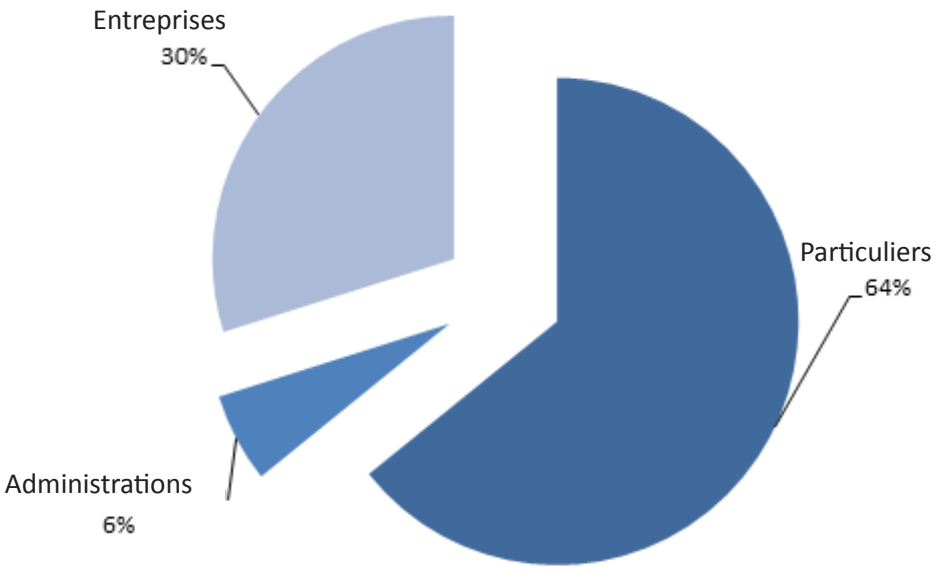

Fig 2 : Répartition des victimes ayant utilisé la plateforme (mai-oct. 2017)
© GIP_ACYMA

** données obtenues après un premier filtrage des résultats recensés sur la plateforme éliminant la phase de test de la plateforme.*

Ce premier retour d'expérience dénote l'intérêt des particuliers pour la plateforme et le besoin d'être accompagné efficacement dans la gestion de leur problème.

De quels types d'attaques parlons-nous ?

83 % des incidents de cybermalveillance sont déclarés par tous les publics comme des **virus**
44 % des incidents déclarés « virus » correspondent à des attaques de type **rançongiciel.**

*** Les particuliers** sur les postes de travail

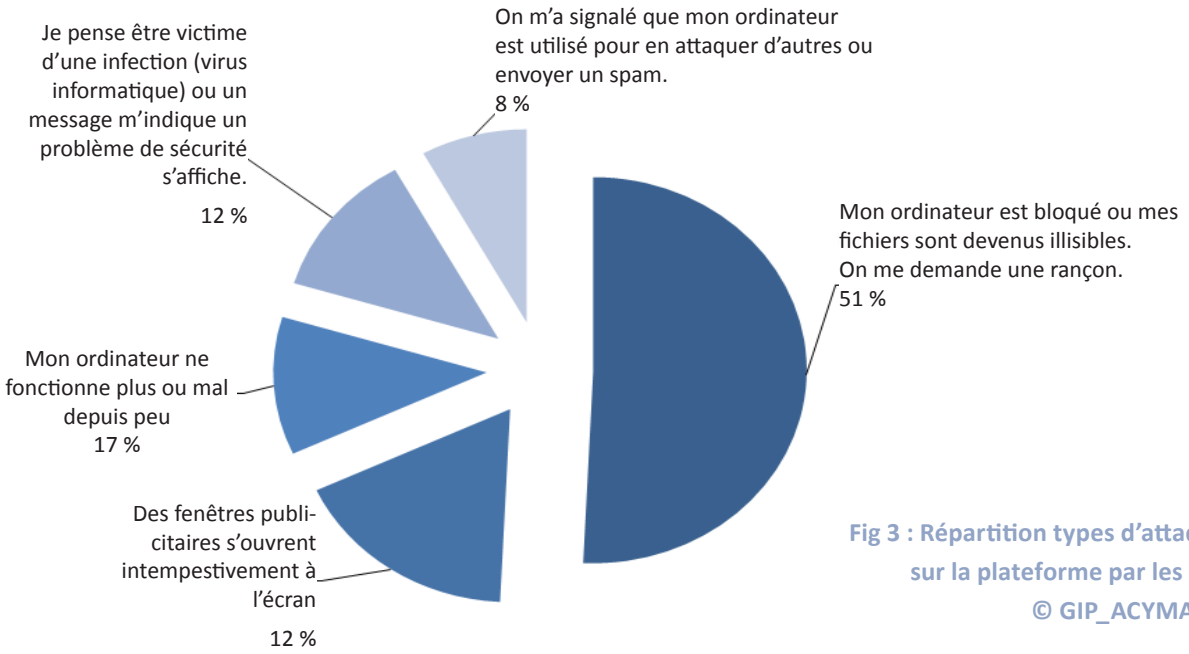

Fig 3 : Répartition types d'attaques référencées sur la plateforme par les particuliers
© GIP_ACYMA

* administrations et des entreprises* sur les postes de travail

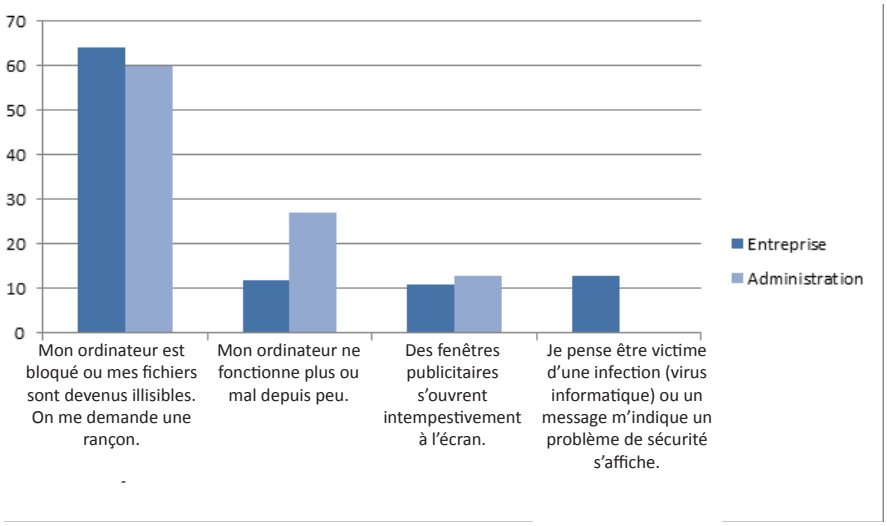

Fig 4 : Répartition types d'attaques référencées sur la plateforme par les entreprises et les administrations
© GIP_ACYMA

L'analyse de ses résultats permet de :

* prioriser les thèmes des campagnes de sensibilisation à mener au niveau national en fonction des types d'attaques relevées (ex: rançongiciel) et/ou des supports attaquées (ordinateurs, supports mobiles, etc.) ;

* enrichir, à terme, les rapports de l'observatoire du risque numérique.

Cette première phase de déploiement dans les Hauts-de-France aura permis de confirmer l'importance d'une communication pédagogique sur les rançongiciels. Qu'est-ce que c'est ? Comment s'en prémunir ? Quels réflexes adopter dès maintenant pour ne pas en être victime ?

Ce sujet avait déjà été identifié comme l'un des enjeux de la sensibilisation du grand public aux actes de cybermalveillance.
> Retrouvez la fiche réflexe et la vidéo de rançongiciel sur la plateforme « Cybermalveillance.gouv.fr ».

Zoom ciblant les sites Internet

Les données à comparer sont différentes dès lors que l'on rentre dans la sphère professionnelle. Par exemple, la répartition du type d'incident constaté sur les sites Internet.*

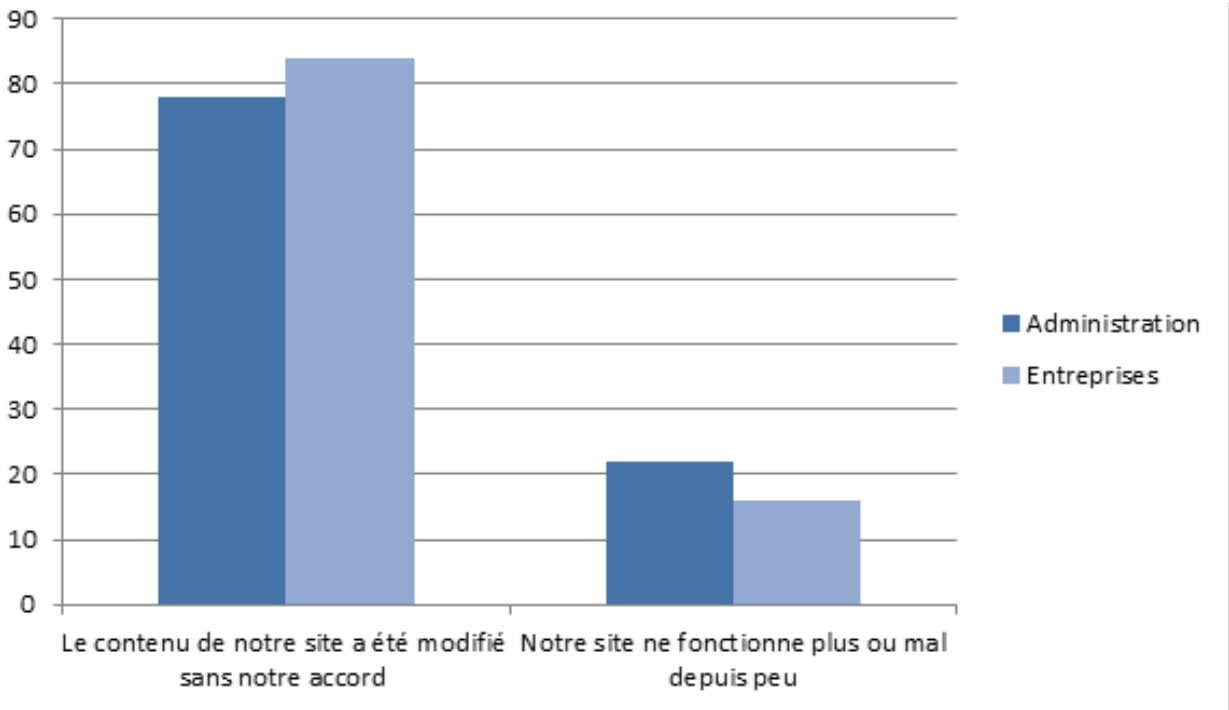

Fig 5 : Typologie des attaques sur les sites Internet
© GIP_ACYMA

D'autres résultats de la phase d'expérimentation seront présentés lors la conférence du 17 octobre.

** Comparaison des statistiques compte tenu du taux de réponse significativement différents entre administrations (43) et entreprises (216).*

Perspectives en 2018

Une version 2.0 de la plateforme est d'ores et déjà à l'étude afin de proposer une expérience utilisateur optimale: une navigation encore plus intuitive ainsi qu'une amélioration de la visibilité et une catégorisation des différents types de contenus de sensibilisation qui viendront enrichir la plateforme tout au long de l'année.

Si les résultats de cette première expérience sont positifs compte tenu du nombre de mises en relation grâce à la plateforme en peu de temps et à une forte mobilisation des prestataires, l'enjeu majeur des prochains mois sera la promotion de la plateforme «Cybermalveillance.gouv.fr» auprès de ses publics cibles.

LE GIP ACYMA

Le dispositif «Cybermalveillance.gouv.fr» est défini et piloté par le groupement d'intérêt public ACYMA, une structure légale permettant l'implication financière et opérationnelle d'acteurs publics et privés. Les membres du GIP sont répartis en 4 collèges rassemblant des représentants de l'Etat, des victimes (utilisateurs), des prestataires et des fournisseurs de solutions.
Ses missions :

* référencer et animer le réseau de prestataires de solutions présents sur l'ensemble du territoire
* lancer des campagnes d'information et de sensibilisation au niveau national sur la sécurité numérique
* mettre en place un observatoire du risque numérique.

Pour mener à bien ces missions, le Directeur général **M. Jérôme NOTIN**, est entouré d'une équipe de 5 personnes (effectif 2017).

LE COLLÈGE « ÉTATIQUES »

Premier ministre / SGDSN / ANSSI
Ministère de l'Economie et des Finances
Ministère de la Justice
Ministère de l'Intérieur
Secrétariat d'Etat chargé du numérique

LE COLLÈGE « UTILISATEURS »

Association e-Enfance
CCI France
Consommation, logement et cadre de vie (CLCV)
Confédération des petites et moyennes entreprises (CPME)

LE COLLÈGE « PRESTATAIRES »

Cinov-IT
Conseil National du Logiciel Libre (CNLL)
La fédération Entreprises du Bureau et du Numérique (Eben)
Syntec numérique

LE COLLÈGE « OFFREURS DE SOLUTIONS »

Fédération Française de l'Assurance (FFA)

Ils ont déposé leur candidature pour être membre en 2018 :
Bouygues Telecom ; Orange Cyberdefense ; Atempo-Wooxo ; Kaspersky Lab ; Eset ; Microsoft ; Stormshield

Pour en savoir plus, rendez-vous sur
https://www.cybermalveillance.gouv.fr/

Contact presse
Presse@cybermalveillance.gouv.fr