Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

RAPPORT D'ACTIVITÉ

2019

Dispositif national d'assistance aux victimes d'actes de cybermalveillance,
de sensibilisation des publics aux risques numériques et d'observation de la menace.

www.cybermalveillance.gouv.fr

SOMMAIRE

Directeur de la publication : Jérôme Notin
Responsable de la communication : Yamina Kerzale
Photos :
© Guillaume Lechat pp. 1, 3 bas, 6, 8, 10, 13 bas, 18, 19, 24, 25, 31
© Yamina Kerzale / Cybermalveillance.gouv.fr pp. 9, 14, 16, 17
© ANSSI p. 3 haut
© Freepik p. 5
© Photos fournies par les organismes concernés p 11. Tous droits réservés.

Conception graphique : Elsa Godet

www.cybermalveillance.gouv.fr
contact@cybermalveillance.gouv.fr

ÉDITO

GUILLAUME **POUPARD**

*Président du Conseil d'administration du GIP ACYMA**
Dispositif Cybermalveillance.gouv.fr

En octobre 2017, le dispositif Cybermalveillance.gouv.fr voyait le jour. C'était il y a deux ans seulement et pourtant, que de chemin parcouru ! La croissance des chiffres est éloquente mais cela démontre surtout une chose : avec l'appui de ses membres que je remercie chaleureusement, le GIP apporte une réponse unique à un public dont les problématiques le sont tout autant.

L'équation est assez simple car il n'y a que deux types d'organisations : celles qui ont été attaquées, et celles qui l'ignorent. Petite ou grosse, aucune n'échappe à ce constat mais toutes ne sont pas égales en termes de survie. Quand une TPE-PME est touchée, elle peut mettre la clé sous la porte tandis que la plupart du temps, un grand groupe s'en sortira, bien que fragilisé. De même, lorsqu'un particulier est victime d'une attaque, il a besoin d'une assistance dans les plus brefs délais car perdre sa vie numérique peut mener à de véritables drames.

Mais je sais aussi combien les décideurs et citoyens ont progressé dans la compréhension de ces enjeux ! Désormais, la sécurité doit faire partie du package de l'entreprise du XXIe siècle. J'irai même plus loin en disant que la sécurité doit être abordée avec enthousiasme et pédagogie comme doit continuer de le faire Cybermalveillance.gouv.fr. Avec le temps, je souhaite qu'il y ait beaucoup plus à gagner qu'à perdre et que chaque acteur prenne conscience des bénéfices d'un investissement dans la cybersécurité.

JÉRÔME **NOTIN**

Directeur général du GIP ACYMA
Dispositif Cybermalveillance.gouv.fr

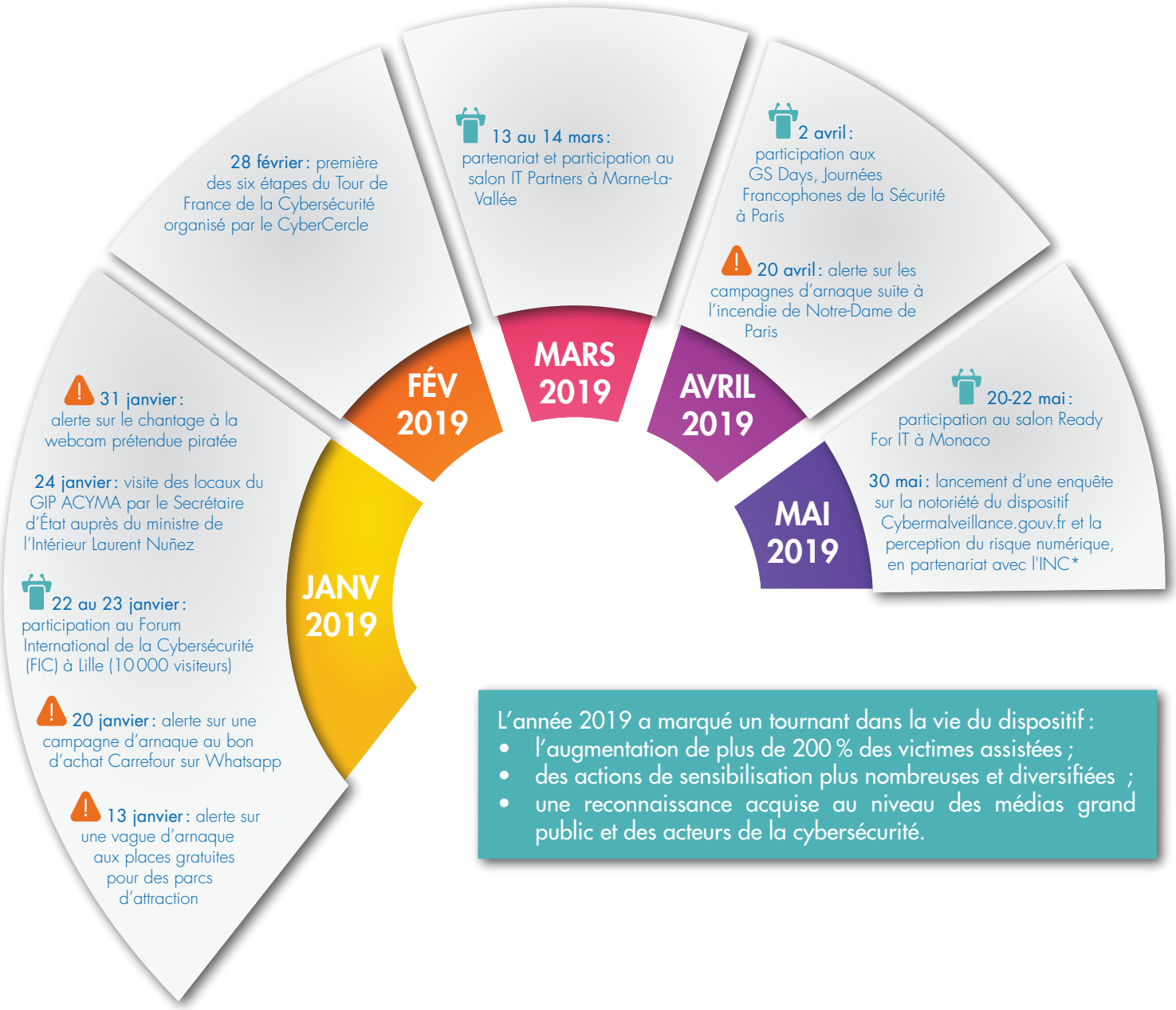
*2019 fut une année marquante pour notre jeune dispositif. Près de 9 Français sur 10 ont été confrontés à un acte de cybermalveillance, selon une étude menée cette année avec l'un de nos membres**. La menace cyber augmente depuis plusieurs années, le GIP s'est organisé pour y faire face efficacement : 40 membres issus des secteurs public et privé engagés dans le dispositif au service de l'intérêt général, un réseau de professionnels en sécurité informatique pour venir en aide aux victimes de cybermalveillances, des partenariats ciblés pour répondre à de nouvelles menaces, ainsi que des actions de sensibilisation auprès du plus large public à travers différents canaux (campagne télévisée, presse nationale et régionale, alertes sur les réseaux sociaux…) et la diffusion d'un kit de sensibilisation aux risques numériques ont ponctué cette année forte pour le GIP.*

Tant sur le plan quantitatif que qualitatif, les résultats sont conséquents : en 2019, ce sont plus de 90 000 victimes qui ont recherché de l'assistance sur Cybermalveillance.gouv.fr (+200 % par rapport à 2018). Le dispositif devient, par ailleurs, une référence en matière d'alerte sur la menace pour les médias et le grand public.

Tous ces éléments confirment la nécessité d'un tel dispositif. Cybermalveillance.gouv.fr. a trouvé sa place dans son écosystème et ceci, grâce à l'engagement au quotidien de ses membres et de ses agents. Des bases solides sont posées pour les années à venir, où de nouveaux défis seront à relever.

* GIP ACYMA : Groupement d'Intérêt Public (GIP) ACYMA Actions contre la cybermalveillance.
** Étude menée en juin 2019 avec l'Institut National de la Consommation (INC).

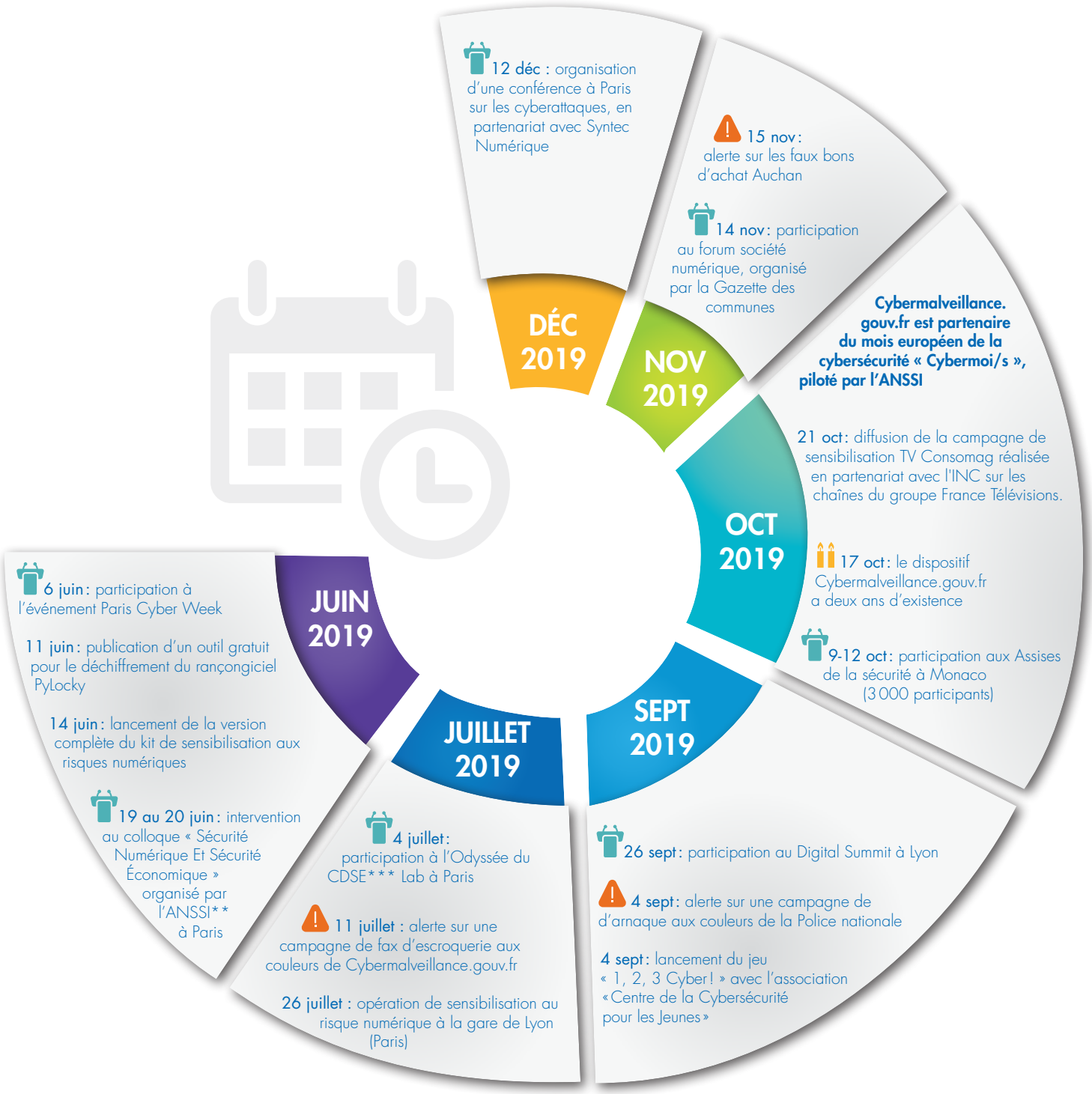
1. LES FAITS MARQUANTS DE L'ANNÉE 2019



L'année 2019 a marqué un tournant dans la vie du dispositif :

- l'augmentation de plus de 200 % des victimes assistées ;
- des actions de sensibilisation plus nombreuses et diversifiées ;
- une reconnaissance acquise au niveau des médias grand public et des acteurs de la cybersécurité.

* Institut National de la Consommation
** Agence Nationale de la Sécurité des Systèmes d'Information
*** Club des Directeurs de Sécurité & de Sûreté des Entreprises


DÉC 2019
12 déc : organisation d'une conférence à Paris sur les cyberattaques, en partenariat avec Syntec Numérique
NOV 2019
15 nov : alerte sur les faux bons d'achat Auchan
14 nov : participation au forum société numérique, organisé par la Gazette des communes
Cybermalveillance.gouv.fr est partenaire du mois européen de la cybersécurité « Cybermoi/s », piloté par l'ANSSI
OCT 2019
21 oct : diffusion de la campagne de sensibilisation TV Consomag réalisée en partenariat avec l'INC sur les chaînes du groupe France Télévisions.
17 oct : le dispositif Cybermalveillance.gouv.fr a deux ans d'existence
9-12 oct : participation aux Assises de la sécurité à Monaco (3 000 participants)
SEPT 2019
26 sept : participation au Digital Summit à Lyon
4 sept : alerte sur une campagne de d'arnaque aux couleurs de la Police nationale
4 sept : lancement du jeu « 1, 2, 3 Cyber ! » avec l'association « Centre de la Cybersécurité pour les Jeunes »
JUILLET 2019
4 juillet : participation à l'Odyssée du CDSE*** Lab à Paris
11 juillet : alerte sur une campagne de fax d'escroquerie aux couleurs de Cybermalveillance.gouv.fr
26 juillet : opération de sensibilisation au risque numérique à la gare de Lyon (Paris)
JUIN 2019
6 juin : participation à l'événement Paris Cyber Week
11 juin : publication d'un outil gratuit pour le déchiffrement du rançongiciel PyLocky
14 juin : lancement de la version complète du kit de sensibilisation aux risques numériques
19 au 20 juin : intervention au colloque « Sécurité Numérique Et Sécurité Économique » organisé par l'ANSSI** à Paris

FAIRE CONNAÎTRE LE DISPOSITIF AU PLUS GRAND NOMBRE, L'UN DES ENJEUX DE CYBERMALVEILLANCE.GOUV.FR

« Devenir le premier réflexe des citoyennes et des citoyens en matière d'assistance et de prévention du risque numérique », telle est la vocation du dispositif Cybermalveillance.gouv.fr au titre de sa mission d'intérêt général.

Particuliers, entreprises, associations ou collectivités : tous sont exposés quotidiennement à des cyberattaques. Afin de gagner en visibilité auprès de ces différents publics, Cybermalveillance.gouv.fr a orienté sa stratégie de communication sur la démultiplication et la diversification de ses actions et outils.

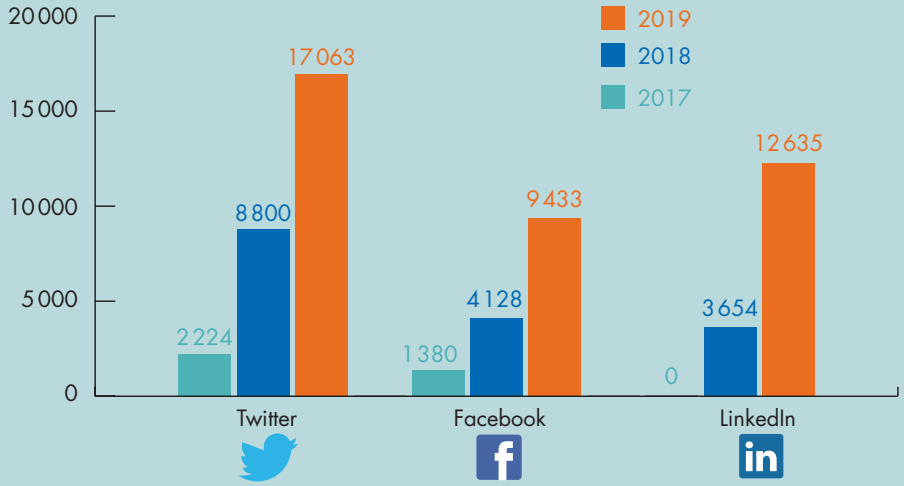
Quelques actions marquantes en 2019 :

- **LA PARTICIPATION À 5 SALONS PROFESSIONNELS** dont certains incontournables dans le domaine de la cybersécurité, et **50 interventions** (plus de 8 000 participants).
- **L'ORGANISATION OU CO-ORGANISATION DE DEUX ÉVÉNEMENTS DE SENSIBILISATION**, l'un s'adressant au grand public (opération en gare de Lyon à Paris) et le second destiné aux professionnels (conférence sur les cyberattaques en partenariat avec Syntec Numérique).
- **LA DÉCLINAISON DES CONTENUS EN DIFFÉRENTS FORMATS** (kit de sensibilisation, pochettes « mémos », vidéos, affiches sur les conseils en matière de sécurité numérique, flyers, quiz…).
- **DES RELATIONS MÉDIAS RENFORCÉES, AVEC LA RECRUDESCENCE DES CAS DE CYBERMALVEILLANCE** (20 communiqués de presse et alertes, 468 retombées médias).
- **UNE STRATÉGIE DE PUBLICATION** sur le site Internet alternant **contenus de fond** et **contenus d'actualité.**
- **LE DÉVELOPPEMENT DES RÉSEAUX SOCIAUX**, avec des alertes régulières.

ZOOM SUR LES RÉSEAUX SOCIAUX

Dès sa création, le dispositif Cybermalveillance.gouv.fr a utilisé les réseaux sociaux pour faire connaître son action et diffuser ses messages de prévention et d'assistance auprès de ses publics. L'année 2019 a vu une forte croissance de son activité sur ses réseaux sociaux.

Évolution du nombre d'abonnés sur les réseaux sociaux



PROGRESSION 2018-2019

+ 93,90%

+ 128,51%

+ 245,79%

Les publications sur les réseaux sociaux qui ont le plus marqué l'année 2019

TOP 5 DES PUBLICATIONS

1. Alerte à l'arnaque au faux bon d'achat Carrefour
2. Alerte à l'arnaque au chantage à la webcam prétendue piratée
3. Alerte à l'escroquerie au logo Cybermalveillance.gouv.fr
4. Lancement de la version complète du kit de sensibilisation
5. Alerte à l'escroquerie aux dons pour Notre-Dame de Paris

De nombreuses publications, et notamment les alertes, ont fait l'objet de relais importants de la part des internautes et ont été reprises largement par la presse écrite et télévisée.

2. LES MISSIONS ET ORGANISATION DU GIP

1 PRÉSENTATION DU DISPOSITIF

Piloté par le Groupement d'intérêt public (GIP) ACYMA, le dispositif Cybermalveillance.gouv.fr s'adresse aux **particuliers** et à toutes les **entreprises** et **collectivités territoriales** (hors OIV et OSE*).
Ses missions sont :

1

L'ASSISTANCE AUX VICTIMES D'ACTES DE CYBERMALVEILLANCE avec, notamment, la mise en relation avec des prestataires de proximité susceptibles de les assister ;

2

LA SENSIBILISATION DES PUBLICS AUX RISQUES NUMÉRIQUES

au travers de contenus et de campagnes de prévention à la sécurité du numérique ;

3

L'OBSERVATION DU RISQUE NUMÉRIQUE

pour mieux l'anticiper et y réagir.

* Opérateurs d'importance vitale (OIV) et opérateurs de services essentiels (OSE)

2 LA CRÉATION DU GIP EN DATES CLÉS

Lancement national de la plateforme Cybermalveillance.gouv.fr le 17 octobre 2017

16 octobre 2015

Annonce dans la **Stratégie nationale pour la sécurité du numérique** par le Premier ministre de la création d'un dispositif répondant au besoin des populations : « *Le dispositif adoptera une forme juridique et une organisation lui permettant de bénéficier de l'apport des acteurs économiques du secteur de la cybersécurité (éditeurs de logiciels, plates-formes numériques, fournisseurs de solutions). Grâce aux technologies mises en œuvre, le dispositif devra proposer aux victimes des solutions techniques s'appuyant sur des acteurs de proximité et faciliter les démarches administratives, notamment afin de favoriser le dépôt de plainte.* »

2016-2017

Incubation par l'ANSSI en copilotage avec le ministère de l'Intérieur, et le soutien des ministères de la Justice, de l'Économie et des Finances et du secrétariat d'État chargé du Numérique

3 mars 2017

Création du Groupement d'Intérêt Public pour le dispositif national d'assistance aux victimes d'actes de cybermalveillance (GIP ACYMA – Actions contre la cybermalveillance - NOR: PRMD1704935A).

17 octobre 2017

Lancement national de la plateforme Cybermalveillance.gouv.fr en présence de Guillaume Poupard, Président du conseil d'administration du GIP ACYMA ; Thierry Delville, DMISC* ; Bernard Spitz, Président de la FFA** ; Mounir Mahjoubi, Secrétaire d'État chargé du numérique ; Louis Gautier, SGDSN*** ; Jérôme Notin, Directeur général du GIP ACYMA.

Extrait de l'arrêté du 3 mars 2017 portant approbation de la convention constitutive du groupement d'intérêt public pour le dispositif national d'assistance aux victimes d'actes de cybermalveillance

La dénomination du Groupement est : « Groupement d'intérêt public pour le dispositif national d'assistance aux victimes d'actes de cybermalveillance ». Son sigle est « GIP ACYMA ».
Le Groupement a pour objet d'assurer :

- une mission d'intérêt général portant sur l'assistance aux particuliers, aux entreprises et aux administrations victimes d'actes de cybermalveillance par la mise en place d'un « guichet unique ». Plus particulièrement, le groupement s'attachera d'une part, à permettre la mise en relation avec des acteurs de proximité capables de procéder à la reprise d'activité d'équipement(s) informatique(s) des victimes et d'autre part, à fournir l'aide aux démarches administratives requises pour le dépôt de plainte ;
- la sensibilisation du public sur les enjeux de la sécurité et de la protection de la vie privée numérique en lien avec les autorités compétentes et le développement de campagnes de prévention en la matière ;
- la fourniture d'éléments statistiques offrant une vue réelle et consolidée de la menace cyber afin de mieux l'anticiper à travers la création d'un observatoire dédié.

* Délégué Ministériel aux Industries de Sécurité et à la lutte contre les Cybermenaces
** Fédération Française des Assurances
*** Secrétaire Général de la Défense et de la Sécurité Nationale

3 GOUVERNANCE ET ORGANISATION DU GIP

Gouvernance

Le GIP ACYMA est composé de 40 membres, d'un président du Conseil d'administration et d'un directeur général. Les membres sont répartis en quatre collèges représentant l'ensemble de l'écosystème :

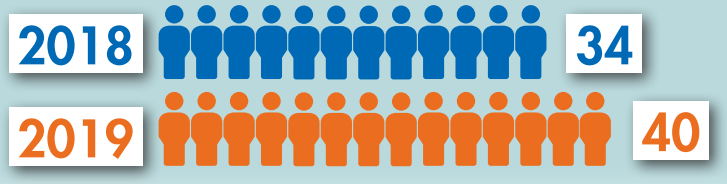
- **Les étatiques :** ministères et secrétariat d'État ;
- **Les utilisateurs :** associations de consommateurs, d'aide aux victimes, clubs d'utilisateurs et organisations professionnelles ;
- **Les prestataires :** syndicats et fédérations professionnelles ;
- **Les offreurs de solutions et de services :** constructeurs, éditeurs, opérateurs, sociétés de services…

Le GIP est organisé autour d'une Assemblée générale et d'un Conseil d'administration qui déterminent les orientations du Groupement.

Organisation fonctionnelle du GIP

LES MEMBRES DU GIP

Les membres de Cybermalveillance.gouv.fr sont des organismes privés et publics qui ont souhaité s'engager dans l'action du dispositif et contribuer à l'accomplissement de ses missions. En participant aux travaux du dispositif, ces membres témoignent de leur implication sur le sujet de la sécurité numérique auprès du public.



Les membres en 2019

Les nouveaux membres en 2019 : CESIN, CrowdStrike, HP France, MAIF, Palo Alto Networks, Publicis Consultants

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

avec

- MINISTÈRE DE LA JUSTICE
- MINISTÈRE DE L'ÉCONOMIE ET DES FINANCES
- MINISTÈRE DE L'INTÉRIEUR
- SECRÉTARIAT D'ÉTAT CHARGÉ DU NUMÉRIQUE

Paroles de membres

CÉDRIC O
Secrétaire d'Etat chargé du Numérique
Ministère de l'Économie, des Finances, de l'Action et des Comptes publics

Cybermalveillance.gouv.fr est un dispositif essentiel pour renforcer la confiance des usagers dans le numérique. Accompagner les victimes de cybermalveillance est la condition d'une transformation numérique sereine et sûre, tant pour nos entreprises que pour nos concitoyens.

MICHEL
VAN DEN BERGHE
Président Directeur Général
Orange Cyberdefense

Les usages numériques doivent bénéficier au plus grand nombre. Il est primordial que les internautes puissent trouver une assistance de proximité en cas de piratage informatique. C'est la raison pour laquelle Orange Cyberdefense est fier d'être membre du dispositif Cybermalveillance.gouv.fr.

JUSTINE
ATLAN
Directrice Générale
Association e-Enfance

L'association e-Enfance, avec sa plateforme de signalements Net Ecoute.fr, a tout naturellement rejoint Cybermalveillance.gouv.fr comme membre fondateur. Nous partageons, en effet, le même objectif d'accompagnement des victimes et de sensibilisation des internautes de tous âges aux risques numériques.

GODEFROY
DE BENTZMANN
Président
Syntec Numérique

L'assistance aux victimes et la sensibilisation des publics sont des enjeux clés auxquels répond Cybermalveillance.gouv.fr. Syntec Numérique est fier de contribuer à ces missions en tant que membre fondateur, avec l'ensemble des acteurs investis sur ce sujet. Il reste encore tant à faire !

3. UN PARTENARIAT PUBLIC / PRIVÉ AU SERVICE D'UNE MISSION D'INTÉRÊT GÉNÉRAL

Original et efficace, le partenariat public / privé du GIP regroupe des acteurs de l'État, tels que l'ANSSI et différents ministères, ainsi que des membres privés. Le dispositif noue également des partenariats plus spécifiques sur des opérations ponctuelles afin de développer des actions ciblées auprès des populations.

Exemples de collaborations en 2019

LES ARNAQUES À L'EMPLOI, AVEC PÔLE EMPLOI

En collaboration avec Pôle emploi, Cybermalveillance.gouv.fr a produit trois nouvelles fiches pour adopter les bons réflexes face aux principaux types d'arnaque à l'emploi pouvant être rencontrés par les particuliers, les entreprises et les recruteurs. Également intégrées dans les parcours de prévention et d'assistance aux victimes de la plateforme www.cybermalveillance.gouv.fr, ces fiches concernent les propositions d'emploi frauduleuses que peuvent recevoir des particuliers, les fausses offres d'emploi sur Internet et le piratage de l'espace personnel d'un recruteur sur un site d'emploi. Ces contenus sont relayés sur le site Internet et les différents supports de Pôle emploi, et mis à disposition des 34 600 conseillers.

« Les services en lignes destinés aux professionnels et au grand public sont attaqués par les cybercriminels. Les sites de recrutement ne sont pas épargnés par ce fléau. Pôle emploi, en sa qualité de service public pour l'emploi, se devait de mettre à disposition des candidats et recruteurs les bonnes pratiques pour éviter de devenir victime. Cybermalveillance.gouv.fr est le partenaire incontournable pour faire connaître aux internautes les bonnes pratiques et les risques spécifiques liés aux arnaques aux faux recrutements. »

LAURENT SIMEONI
CHARGÉ DE MISSION, PÔLE EMPLOI

LA SÉCURITÉ POUR LES ACHATS EN LIGNE, AVEC LA FEVAD

Tous les deux ans, la Fevad publie avec l'INC un guide pratique pour accompagner les consommateurs lors de leurs achats en ligne. *Achats en ligne, Suivez le Guide* répond aux questions que peuvent se poser les cyberacheteurs avant, pendant ou après leurs achats sur Internet. Avec Cybermalveillance.gouv.fr, la Fevad et l'INC mettent également en garde dans ce guide contre l'hameçonnage ou phishing, une technique utilisée par le fraudeur pour obtenir les données personnelles des particuliers.

« Cette année, en partenariat avec Cybermalveillance.gouv.fr, une page a été consacrée à l'hameçonnage afin de mettre en garde les internautes mais également de leur indiquer comment réagir s'ils en sont victimes. La Fevad et Cybermalveillance.gouv.fr partagent la volonté commune de protéger les consommateurs des actes de malveillance sur la toile. »

NATHALIE LAINE
DIRECTRICE DE LA COMMUNICATION, LA FEVAD

LES ÉCHANGES OPÉRATIONNELS AVEC LA SECTION F1 CYBERCRIMINALITÉ (JIRS*) DU PARQUET DE PARIS ET LES SERVICES D'ENQUÊTE DE POLICE JUDICIAIRE

Le début d'année 2019 voit l'amplification des campagnes de « crypto-porno » (chantage à la webcam prétendue piratée) et, par conséquent, du nombre de victimes. Ce phénomène est rapidement identifié par les magistrats spécialisés du pôle cybercriminalité, qui rédigent aussitôt un modèle de lettre plainte en collaboration avec la SDLC**.

Cybermalveillance.gouv.fr a mis à disposition le document sur sa plateforme, permettant aux victimes de **formaliser leur plainte** et de partager des données techniques avec les enquêteurs. 28 000 concitoyens transmettent alors les éléments sur 140 000 visiteurs de la page dédiée. Grâce aux informations collectées, les services d'enquête identifient deux personnes. Elles sont interpellées en septembre, puis en décembre 2019.

« Fort des informations recueillies auprès des internautes, victimes de ces actes de chantages numériques, Cybermalveillance.gouv.fr constitue un réceptacle exceptionnel des infractions de cybercriminalité dont sont victimes notamment les particuliers, qui le plus souvent font le choix de ne pas déposer plainte, pour diverses raisons. »

ALICE CHÉRIF
VICE-PROCUREUR, CHEF DE SECTION PÔLE CYBERCRIMINALITÉ F1 – PARQUET DE PARIS

* JIRS: Juridiction Interrégionale Spécialisée
**SDLC : Sous-direction de Lutte contre la Cybercriminalité

FRANCK **GICQUEL**
Responsable des partenariats
Dispositif Cybermalveillance.gouv.fr

Les membres du GIP constituent l'une de ses grandes forces : quarante entités d'horizons très divers, issues des sphères publique et privée, partageant des valeurs communes (sensibilisation, hygiène numérique) et fédérées autour du même enjeu de sécurité numérique. Les membres participent activement à la vie du dispositif à la fois sur le plan stratégique, notamment lors des Assemblées générales et Conseils d'administration, et sur le plan opérationnel en participant au rayonnement du dispositif et en prenant part aux différents groupes de travail. Ces groupes constituent de véritables communautés de compétences. Les échanges y sont riches, fructueux et tendent à décloisonner le sujet de la sécurité numérique afin que ces travaux puissent profiter au plus grand nombre.

Zoom sur...

LES GROUPES DE TRAVAIL : UN MODE DE COLLABORATION AVEC LES MEMBRES DU GIP

Les groupes de travail sont constitués essentiellement des membres du GIP. Ils se réunissent à plusieurs reprises tout au long de l'année pour travailler sur des sujets et projets majeurs pour le dispositif. Au nombre de trois pour l'année 2019, ils ont porté sur la production d'un kit sensibilisation, l'élaboration d'un référentiel d'expertise pour les prestataires et l'étude préalable à la création de l'observatoire du risque numérique.

4. LA SENSIBILISATION, PREMIÈRE ARME CONTRE LES CYBERMALVEILLANCES

Prévenir les populations des risques liés à la cybermalveillance et favoriser les bonnes pratiques à mettre en œuvre constituent l'une des principales missions du dispositif Cybermalveillance.gouv.fr. Outre la production de contenus de sensibilisation et la contribution aux contenus produits par des tiers, Cybermalveillance.gouv.fr a participé ou lancé en 2019 des actions destinées à tous les publics, dans une volonté de développer sa visibilité auprès du grand public et de renforcer sa présence dans son écosystème.

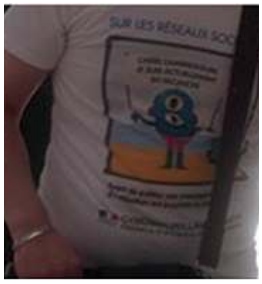
1 ORGANISER ET PARTICIPER À DES ÉVÉNEMENTS

GRAND PUBLIC

Le 26 juillet 2019, Cybermalveillance.gouv.fr est allé à la rencontre du public à la gare de Lyon. Soucieux de toucher tous les âges, il s'est associé à ISSA France et la SNCF pour la distribution de 3 000 exemplaires d'une pochette contenant un kit « mémos » de sensibilisation et le cahier de vacances *Les As du Web* destiné aux enfants.

Cette rencontre sur le terrain a permis de sensibiliser les publics aux risques numériques en incitant les usagers à faire preuve de vigilance à l'occasion des départs en vacances.

20 000 exemplaires de ce kit « mémos » furent également remis aux personnes ayant assisté à la tournée nationale « Sécurité en famille » organisée par Google dans 20 villes de France entre octobre et décembre 2019. Les participants ont pu tester leurs connaissances en sécurité numérique grâce à un quiz élaboré par Cybermalveillance.gouv.fr.



« Avec l'enthousiasme qu'on lui connaît, l'équipe cybermalveillance.gouv.fr a choisi de distribuer ses contenus de sensibilisation au format grand public, accompagnés d'une partie des livrets « Les As du Web » d'ISSA France produits par la SNCF, et ainsi rencontrer les citoyens numériques que nous sommes. En cybersécurité comme en bien d'autres domaines, l'union fait la force, et provoque aussi de belles rencontres. Merci à Cybermalveillance.gouv.fr. Merci à ISSA France »

FABRICE NERACOULIS
PILOTAGE DU PROGRAMME DE SENSIBILISATION À LA PROTECTION DE L'INFORMATION, SNCF

Par ailleurs, le dispositif s'est appuyé sur ses membres pour démultiplier ses actions de sensibilisation. À l'occasion du Mois Européen de la Cybersécurité « Cybermoi/s » consacré à la protection des usages numériques et piloté par l'ANSSI en octobre 2019, Cybermalveillance.gouv.fr a apporté sa contribution active :

- **Une campagne d'information tout au long du mois d'octobre** sur les réseaux sociaux et le site Internet www.cybermalveillance.gouv.fr avec la publication de bonnes pratiques et fiches réflexes sur les clés d'une bonne hygiène numérique ;

- **La mise à disposition de nombreuses ressources** à destination des professionnels et du grand public sur le site dédié à l'événement « Cybermoi/s » ;

- **Une campagne médias auprès des consommateurs**, en partenariat avec l'INC sur les chaînes du groupe France Télévisions et de nombreux médias en ligne, du 22 octobre au 29 novembre (lire l'encart page 21) ;

- **La conception, avec l'ANSSI, d'une étude sur la perception des enjeux autour de la sécurité numérique des citoyens**, pour faire évoluer les comportements. Lancée en novembre 2019, avec une restitution début 2020, ses résultats ont, notamment, pour but d'adapter les outils de sensibilisation des prochaines éditions de la campagne « Cybermoi/s » ;

- **Une campagne de sensibilisation en partenariat avec la Gendarmerie nationale** avec la diffusion de bonnes pratiques sur des supports du quotidien. 800 000 fourreaux à pain ont été distribués dans huit départements de France (dispositif R-Mess, Prix de la Prévention 2019 de la Gendarmerie nationale).

Mois européen de la cybersécurité « Cybermoi/s » 2019.

PROFESSIONNELS

Cybermalveillance.gouv.fr a participé à divers événements et salons en lien avec son écosystème professionnel.

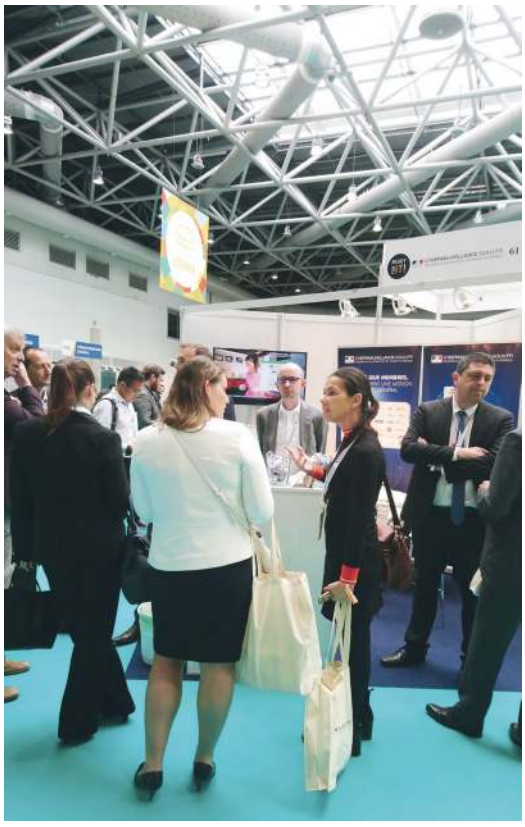
Présence sur cinq salons incontournables dans les domaines de l'informatique et de la cybersécurité :

- **Le Forum International de la Cybersécurité** (FIC) à Lille (10 000 visiteurs) ;
- **IT Partners** à Marne-La-Vallée (8 500 participants) ;
- **GS Days** à Paris (500 participants) ;
- **Ready for IT** à Monaco (plus de 700 visiteurs) ;
- **Les Assises de la sécurité** à Monaco (plus de 3 000 visiteurs).

Lors de ces salons, plus de 2000 kits de sensibilisation ont été distribués, outil nécessaire pour sensibiliser les collaborateurs d'entreprise aux risques numériques.

« Depuis 2017, Cybermalveillance.gouv.fr et IT Partners ont engagé un partenariat stratégique qui enrichi l'événement d'une expertise fondamentale pour les prestataires IT. Les prestataires IT, communauté pour laquelle IT Partners est organisé, sont la pierre angulaire du déploiement des solutions de sécurité informatique au sein des organisations professionnelles. Ils trouvent dans la présence de Cybermalveillance.gouv.fr un soutien essentiel pour leur montée en compétences sur ce sujet critique. »

LAURENT EYDIEU,
DIRECTEUR DE DIVISION
SALON IT PARTNERS



Salon Ready For IT, édition 2019 à Monaco.

Interventions (colloques, conférences…) et co-organisation d'événements, à Paris et en régions.

Tour de France Cyber

Cybermalveillance.gouv.fr était partenaire du Tour de France de la Cybersécurité (TDFCyber) 2019 organisé par le CyberCercle. A travers ses étapes en région, le TDFCyber a pour vocation de porter les sujets de sécurité et de confiance numériques au plus près des acteurs présents sur les territoires (secteurs public et privé, élus, spécialistes de la cybersécurité nationaux, européens et locaux, associations, collectivités…).

> *« La présence du dispositif sur l'ensemble des étapes a représenté un lien privilégié entre local et national. À chaque étape, les équipes de Cybermalveillance.gouv.fr ont présenté leurs missions et animé un atelier « sensibilisation interne ». Lors de ces étapes, s'est exprimé de manière très forte le besoin des acteurs présents en région d'avoir des informations fiables sur la sécurité numérique et d'être accompagnés dans leurs démarches par des acteurs de confiance. Deux axes de travail majeurs de Cybermalveillance.gouv.fr. »*
>
> **BÉNÉDICTE PILLET, PRÉSIDENTE DU CYBERCERCLE**

Le TDFCyber a réuni en 2019 plus de 1300 participants dans six régions (Centre-Val de Loire, Nouvelle-Aquitaine, Sud, Bretagne, Auvergne-Rhône-Alpes et Pays de la Loire).

Les SecNum Eco

En 2019, Cybermalveillance.gouv.fr est intervenu lors de la plupart des événements SecNum Eco co-organisés par l'ANSSI et le Service de l'Information Stratégique et de la Sécurité Économique (SISSE), en partenariat avec un acteur majeur du territoire concerné (CCI, Conseil départemental…). Les SecNum Eco ont pour vocation de faire partager les bonnes pratiques et les expériences en matière de sécurité numérique et de sécurité économique.

Du fait de ses réponses adaptées, le dispositif Cybermalveillance.gouv.fr a, chaque fois, suscité l'intérêt des acteurs économiques, notamment des TPE/PME.

Conférence sur les cyberattaques

Le 12 décembre 2019 s'est tenue une conférence sur les cyberattaques coorganisée par Syntec Numérique et Cybermalveillance.gouv.fr. Une table ronde centrée sur les bons réflexes à adopter autour d'une cyberattaque, à partir du témoignage du président-directeur général de la société Altran a permis aux experts présents d'expliquer le contexte global des cyberattaques, les enjeux et la gestion de tels incidents, ainsi que les enseignements à en tirer pour renforcer sa sécurité numérique.

Conférence du 12 décembre 2019 sur les cyberattaques.

2 CONCEVOIR DES CONTENUS DE SENSIBILISATION

Avec l'augmentation des cyberattaques envers les particuliers et les professionnels, Cybermalveillance.gouv.fr produit régulièrement de nouveaux contenus et diversifie ses supports pour une prévention plus efficace.

Publication d'articles sur le site Internet Cybermalveillance.gouv.fr :

Qu'ils soient de fond ou d'actualité, 12 articles ont été publiés sur le site Internet en 2019.

Quelques-uns des sujets traités :

- *Les 10 règles de base pour la sécurité numérique ;*
- *Comment protéger vos données en sensibilisant vos collaborateurs ? ;*
- *Black Friday et fêtes de fin d'année – Attention aux cyberarnaques ! ;*
- *Les bonnes pratiques pour naviguer sur Internet*
- *…*

Les chiffres de 2019

15 alertes publiées sur les réseaux sociaux (4 en 2018) :
8 sur des campagnes d'arnaques et 7 sur des failles de sécurité critiques.

46 contenus publiés (26 en 2018) :
5 fiches réflexes, 4 fiches pratiques, 2 infographies, 9 mémos, 14 vidéos, 12 articles.

37 660 kits complets de sensibilisation téléchargés

Mise à jour et création de fiches conseils « pratiques » et « réflexes »

Dans la continuité de 2018, Cybermalveillance.gouv.fr a mis à jour ses contenus et conçu des supports de sensibilisation sur de nouvelles thématiques d'actualité (les réseaux sociaux, les sauvegardes, les mises à jour, les rançongiciels…).

Scindés en deux catégories pour une meilleure appropriation par les publics, ceux-ci prennent la forme :

- **de conseils pour adopter les bonnes pratiques en matière de sécurité numérique :** généralement présentés en 10 points, les conseils donnés offrent au lecteur les règles de base de sécurité numérique sur le thème abordé,
- **de fiches « réflexes » pour mieux comprendre les menaces et agir :** les sujets de ces fiches sont essentiellement issus des remontées de la plateforme d'assistance Cybermalveillance.gouv.fr et sont traités sous l'angle infractionnel.

Déclinés en différents formats (vidéos, mémos, etc.), ces fiches et conseils ont été, pour la plupart, intégrés au **kit de sensibilisation aux risques numériques** qui s'est enrichi en 2019 de nouveaux thèmes et supports (lire p. 20).

Zoom sur...
LA SENSIBILISATION DES PLUS JEUNES EN 2019

Les bonnes pratiques en matière de sécurité numérique doivent s'acquérir dès le plus jeune âge. Dans cette volonté de sensibiliser les publics non avertis, Cybermalveillance.gouv.fr a, dans un premier temps, rendu accessible l'ensemble de ses contenus en déclinant les conseils de sécurité numérique sur des supports variés et ludiques : une bande dessinée sur les réseaux sociaux, un quiz pour tester ses connaissances ou encore des vidéos en « motion design ». Le dispositif a noué, en parallèle, des partenariats avec des acteurs engagés auprès des jeunes tels qu'ISSA France, en distribuant son cahier de vacances « Les As du Web » destiné aux 7-11 ans, ou encore en participant à l'élaboration du kit de jeu « 1,2,3 CYBER ! » lancé par l'association « Centre de la Cybersécurité pour les Jeunes » pour sensibiliser les 11-14 ans aux dangers d'Internet.

YAMINA **KERZALE**
Responsable de la communication et du marketing
Dispositif Cybermalveillance.gouv.fr

« Quotidiennement exposés aux outils numériques, mais bien souvent peu conscients des risques encourus dans leurs pratiques, les jeunes sont eux aussi des cibles potentielles : cyberharcèlement, vol de données personnelles, piratage de comptes en ligne… En tant qu'organisation gouvernementale, nous avons un rôle à jouer dans la prévention de ces publics plus vulnérables, en développant plus encore notre action de sensibilisation avec des outils et de messages adaptés à ces publics. Nous pouvons compter sur nos membres et nos partenaires pour nous appuyer dans cette démarche en 2020 ! »

LES ACTIONS DE SENSIBILISATION MARQUANTES DE L'ANNÉE 2019

LANCEMENT DU KIT DE SENSIBILISATION COMPLET

Cybermalveillance.gouv.fr a publié le 13 juin 2019 **la version complète de son kit de sensibilisation aux risques numériques**. Un an après la sortie du 1er volet, le kit de sensibilisation s'est enrichi de cinq nouveaux thèmes et de quatre nouveaux formats, **dans un graphisme totalement repensé et des contenus accessibles à tous**. Fruit d'une collaboration menée depuis plusieurs mois entre institutions publiques, organismes privés et associations membres du GIP, et avec la contribution d'utilisateurs pour déterminer les sujets et types de contenus à développer, **cet outil s'adresse à tous les publics, que ce soit dans leurs usages professionnels ou personnels et quelles que soient leurs connaissances en sécurité du numérique.**

« En complément des outils techniques nécessaires pour se protéger, la sensibilisation de chacun est indispensable afin d'évoluer de manière sécurisée dans notre monde de plus en plus connecté. Nous avons donc identifié, avec l'aide de nos membres publics et privés, les menaces que nos concitoyens rencontrent au quotidien afin d'expliquer les bonnes pratiques pour s'en protéger, et ce de manière pragmatique et ludique. Le choix fort de la licence ouverte permet par ailleurs à chacun d'adapter le contenu à son environnement spécifique. »

JÉRÔME NOTIN
DIRECTEUR GÉNÉRAL DU GIP ACYMA
CYBERMALVEILLANCE.GOUV.FR

La version complète du kit de sensibilisation aux risques numériques est téléchargeable à l'adresse : **www.cybermalveillance.gouv.fr**

Diffusé principalement sous une licence ouverte (Etalab 2.0) **pour en permettre la plus large diffusion, adaptation et réutilisation**, le kit de sensibilisation aborde neuf thèmes (les mots de passe, la sécurité sur les réseaux sociaux, la sécurité des appareils mobiles, les sauvegardes, les mises à jour, la sécurité des usages pro-perso, l'hameçonnage, les rançongiciels et l'arnaque au faux support technique), déclinés en différents supports : fiches pratiques, vidéos, mémos, mais aussi – et c'est l'une des nouveautés – des formats interactifs et ludiques : une bande dessinée, un poster, un quiz et, pour la version papier, des autocollants.

FOCUS SUR LA CAMPAGNE NATIONALE D'INFORMATION ET DE SENSIBILISATION « CONNECTÉ ET PROTÉGÉ »

Afin d'améliorer la sécurité numérique des consommateurs et dans le cadre du Mois Européen de la Cybersécurité, Cybermalveillance.gouv.fr a réalisé en partenariat avec l'INC une campagne intitulée « Connecté et protégé », composée d'une série de quatre émissions Consomag, de six clips vidéos thématiques au format questions-réponses d'experts et d'un spot de sensibilisation de 25 secondes.

Cette campagne a été diffusée sur les chaînes du groupe France Télévisions du 21 octobre au 9 novembre 2019, auprès de médias nationaux et régionaux, généralistes ou spécialisés jusqu'au 29 novembre. Le spot de sensibilisation de 25 secondes a, quant à lui, été diffusé sur les chaînes BFM Business TV, BFM Paris, RMC Sport News, ainsi que les chaînes du groupe Canal+ et la Chaîne Météo.

Spots « connecté et protégé »
6 550 diffusions
(114 heures d'antenne)
Consomag
2,7 millions
de téléspectateurs

« L'audience moyenne cumulée recueillie pour une émission sur France Télévisions s'est élevée à 2,7 millions de téléspectateurs. Quant aux six vidéos et au spot, ils ont été regroupés dans un vidéo Press-kit. 150 médias, 59 télévisions, 22 web TV, 69 sites et/ou réseaux sociaux les ont relayés. »

ANNE-JULIETTE REISSIER, RESPONSABLE COMMUNICATION MEDIA, INC

Sujets des Consomags :

- Comment sécuriser ses achats sur Internet : les bonnes pratiques !
- Comment utiliser les réseaux sociaux en toute sécurité ?
- Sauvegarder ses données numériques : un impératif !
- Pourquoi faut-il faire des mises à jour sur ses appareils numériques ?

Sujets des spots « La minute info : connecté et protégé » :

- Comment réagir face un mail de phishing ?
- L'accès à mes fichiers informatiques a été bloqué et on me demande une rançon. Que faire ?
- WiFi public : comment empêcher le vol de mes données ?
- Comment fonctionne un gestionnaire de mots de passe ?
- Applications, faut-il accepter toutes les autorisations pour pouvoir les utiliser ?
- Comment sécuriser mes appareils pour qu'ils ne soient pas attaqués par des virus ?

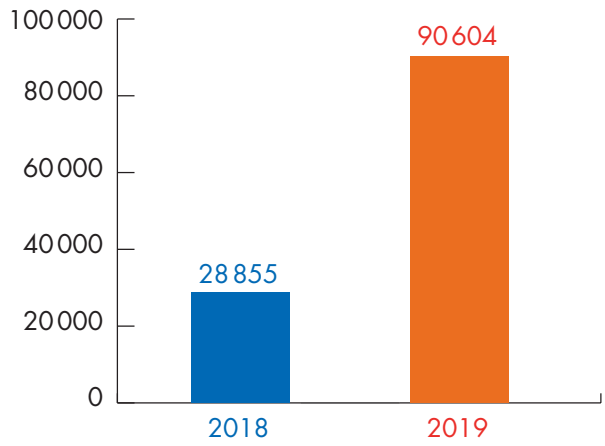
Retrouvez l'ensemble de ces vidéos sur www.cybermalveillance.gouv.fr.

5. L'ASSISTANCE AUX VICTIMES : UN BESOIN, UNE NÉCESSITÉ

Si la prévention est indispensable, l'assistance aux victimes reste l'objectif premier du dispositif Cybermalveillance.gouv.fr. La plateforme permet aux victimes de décrire leur problème en répondant à quelques questions et leur propose un diagnostic de l'incident qu'elles rencontrent. Avec ce diagnostic, **des conseils sont fournis aux victimes** pour les aider à remettre en service leur système ou pour les orienter vers des services compétents. Si l'incident le justifie, les victimes se voient également proposer de recourir à des **prestataires spécialisés de proximité**, référencés sur la plateforme et susceptibles de leur apporter une assistance technique pour résoudre leur problème.

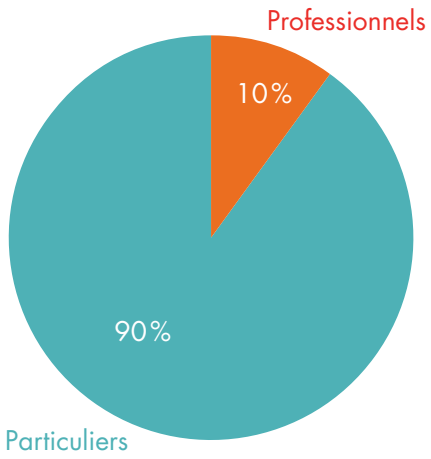
1 LA RÉPONSE À UN BESOIN DES POPULATIONS : L'ASSISTANCE EN CHIFFRES

Nombre de parcours victimes sur la plateforme Cybermalveillance.gouv.fr 2018-2019 :



Plus de 28 000 victimes étaient venues chercher de l'assistance en 2018 sur la plateforme. En 2019, ce sont plus de 90 000 victimes. Cette augmentation de plus de 200 % montre que les efforts entrepris pour développer la notoriété du dispositif portent leurs fruits et qu'il existe un réel besoin d'assistance face aux différentes formes de cybermalveillance.

Répartition des publics en recherche d'assistance



Les particuliers représentent 90 % des victimes en recherche d'assistance sur la plateforme. Cette catégorie de public est bien souvent désarmée face aux incidents de sécurité qui la frappent et dispose de peu de recours et d'appui pour y faire face.

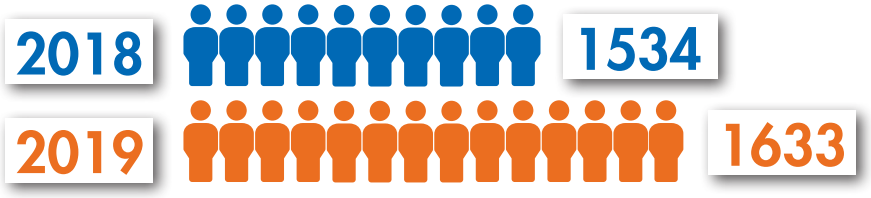
Bien que souvent mieux soutenus, les professionnels (entreprises, collectivités…) ont également recours régulièrement à la plateforme notamment pour accéder aux conseils de première urgence ou être mis en relation avec un prestataire de proximité en mesure de leur apporter l'assistance nécessaire à la reprise de leur activité suite à une attaque.

2 UN RÉSEAU DE PRESTATAIRES D'ASSISTANCE AUX VICTIMES

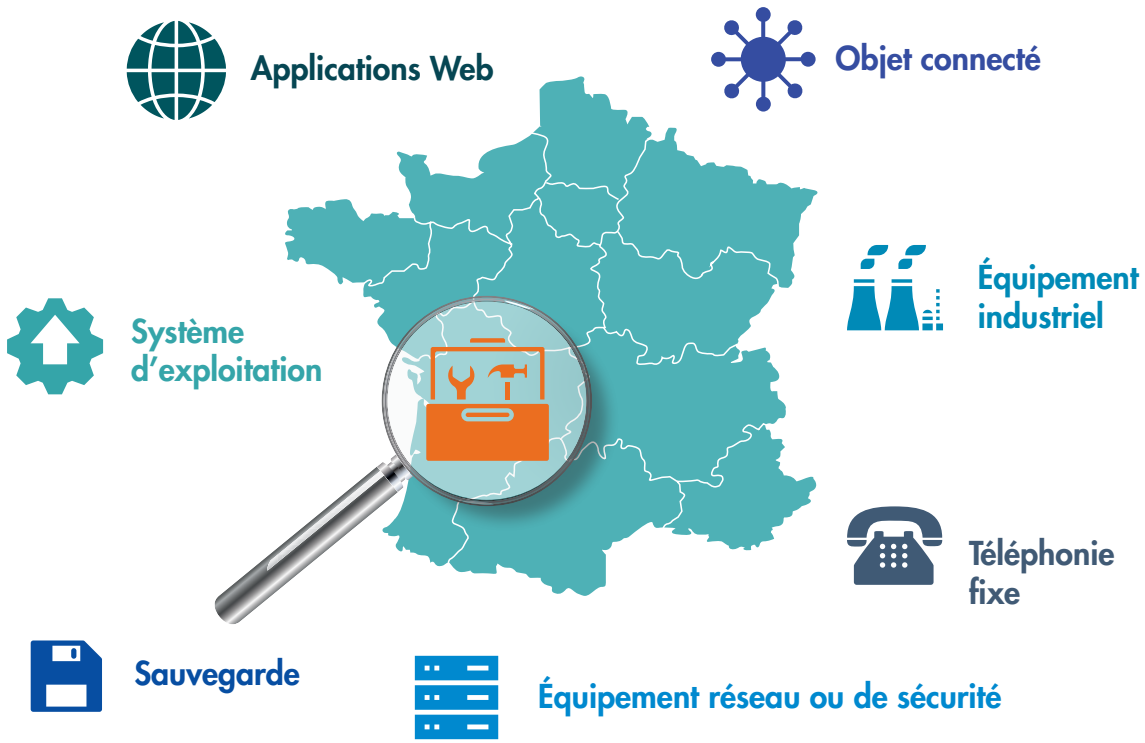
Dans le cadre de sa mission d'assistance, la plateforme référence plus de 1 600 prestataires spécialisés sur le territoire national. Ces prestataires, qui se sont engagés à respecter une charte de bonnes pratiques, peuvent intervenir tant auprès des particuliers que des professionnels, suivant leurs champs d'action et de compétences.

Ils informent, par ailleurs, le dispositif quasiment en temps réel de la menace et de ses évolutions qui pèsent sur la population. **Ils sont donc un atout clé pour le GIP dans la détection de nouveaux phénomènes et dans la collecte d'éléments techniques.**

Le réseau de prestataires spécialisés référencés sur Cybermalveillance.gouv.fr



Les domaines de compétences couverts par les prestataires



3 DES CONSEILS & CONTENUS ACTUALISÉS DÈS QU'UNE NOUVELLE CATÉGORIE DE MENACE EST IDENTIFIÉE

Les parcours d'assistance et fiches « réflexes » sont régulièrement complétés pour prendre en compte de nouvelles menaces et demandes de conseils.

En 2019, les nouveaux contenus d'assistance ont concerné :

- **le piratage de compte en ligne ;**
- **le chantage à la webcam prétendue piratée ;**
- **les différents types d'arnaque à l'emploi (fausses annonces, piratage d'espace recruteur…).**

Un outil de déchiffrement du rançongiciel PyLocky réalisé par les services du ministère de l'Intérieur, membre fondateur du dispositif, en collaboration avec la BEFTI* de la Préfecture de Police, du ST(SI)²**, de la Gendarmerie nationale et de la Police nationale, a été mis à la disposition des victimes sur la plateforme Cybermalveillance.gouv.fr.

* Brigade d'Enquêtes sur les Fraudes aux Technologies de l'Information
** Service des Technologies et des Systèmes d'Information de la Sécurité Intérieure

Zoom sur...

LE LABEL EXPERTCYBER : QUALITÉ EXPERTISE NUMÉRIQUE

EXPERT CYBER

LABEL SÉCURITÉ NUMÉRIQUE Cybermalveillance.gouv.fr

Cybermalveillance.gouv.fr a annoncé le 12 décembre 2019 le lancement d'un nouveau label début 2020 à l'occasion d'une conférence organisée avec Syntec Numérique. Le label a été pensé pour apporter aux victimes d'actes de cybermalveillance une meilleure lisibilité sur l'expertise des prestataires d'accompagnement et d'assistance en sécurité numérique. Élaboré depuis un an avec la participation des principaux syndicats et fédérations de la profession, il va permettre d'évaluer les prestataires candidats sur de nombreux points, allant de leurs engagements en matière de respect des données personnelles de leurs clients, à leurs compétences techniques, avec un accent mis sur la transparence, la sensibilisation des clients et la préservation de la preuve numérique.

Le label ExpertCyber est développé par Cybermalveillance.gouv.fr, en partenariat avec les principaux syndicats professionnels du secteur (Fédération EBEN, Cinov Numérique, Syntec Numérique), la Fédération Française de l'Assurance et le soutien de l'AFNOR.

ADRIENNE **CHARMET**

Chargée de mission partenariats institutionnels
Dispositif Cybermalveillance.gouv.fr

« *Nous nous sommes faits accompagner par l'AFNOR, spécialiste de la certification, pour créer ce label afin qu'il réponde parfaitement aux besoins identifiés : accompagner, vérifier, valoriser les compétences. C'est pour nous une évolution essentielle dans notre mission d'assistance aux victimes d'actes de cybermalveillance, qui viennent chercher de l'aide sur la plateforme.* »

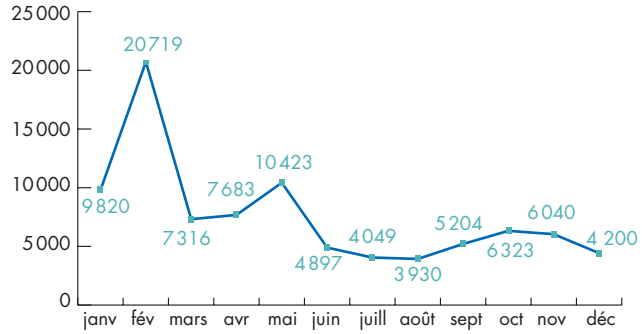
6. OBSERVER LA MENACE POUR MIEUX L'ANTICIPER ET ADAPTER L'OFFRE D'ASSISTANCE

L'assistance aux victimes apportée par Cybermalveillance.gouv.fr est un capteur unique d'informations sur la réalité de la cybermalveillance. Cette observation de la menace permet au dispositif d'adapter rapidement son offre d'assistance et de sensibilisation pour répondre aux préoccupations des victimes frappées par les nouveaux phénomènes cybercriminels. Elle permet également de détecter des phénomènes de masse émergents, comme l'exploitation d'une nouvelle faille de sécurité ou de nouveaux modes opératoires cybercriminels, et ainsi d'alerter non seulement les populations, mais également les pouvoirs publics.

1 LES CHIFFRES DE CYBERMALVEILLANCE.GOUV.FR EN 2019

Les chiffres et tendances sont issus des données de la plateforme Cybermalveillance.gouv.fr.

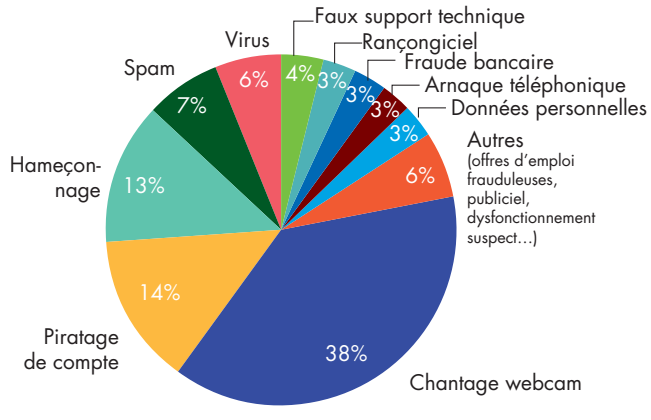
Évolution du nombre de recherches d'assistance sur l'année 2019



Les pics de recherches d'assistance constatés au premier semestre, et en particulier en février et mai correspondent à différentes vagues massives de chantage à la webcam prétendue piratée.

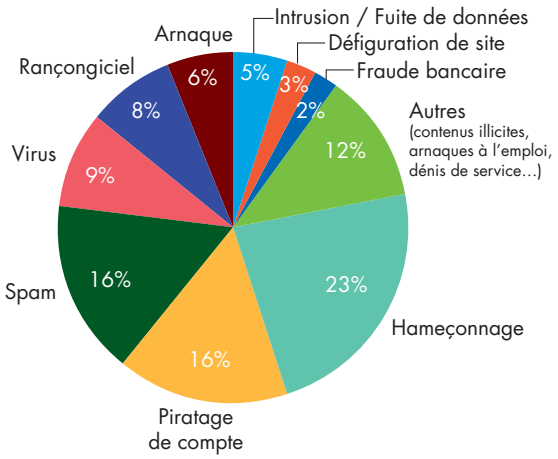
Répartition des menaces par types de publics

Recherches d'assistance / particuliers



En 2019 les principales recherches d'assistance des particuliers sur la plateforme ont principalement porté sur le phénomène du chantage à la webcam pour 38 %, suivi du piratage de compte en ligne avec 14 %, l'hameçonnage avec 13 % devant les spams 7 %, les virus 6 % et les arnaques au faux support technique 4 %.

Recherches d'assistance / professionnels*



Chez les professionnels (entreprises, collectivités, associations), les recherches d'assistance en 2019 ont principalement porté sur l'hameçonnage (23 %), le piratage de compte en ligne tels que messagerie, réseaux sociaux, commerce en ligne… (16 %), le spam (16 %), les virus (9 %), les rançongiciels (8 %).

* Entreprises, collectivités

2 LES GRANDES TENDANCES DE LA MENACE OBSERVÉES EN 2019

Ces principales tendances sont tirées des remontées d'information des victimes et des comptes-rendus d'intervention adressés au dispositif par les prestataires référencés sur la plateforme.

L'HAMEÇONNAGE (*PHISHING*) RESTE LA MENACE PRÉDOMINANTE ET SE DIVERSIFIE

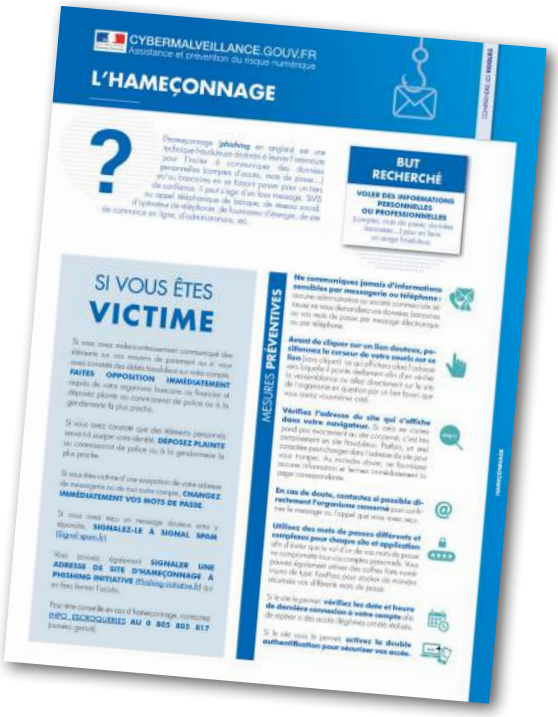
Le principe mis en œuvre par les cybercriminels dans leurs attaques par hameçonnage consiste à demander à une victime de fournir des informations personnelles voire confidentielles (mots de passe…) ou encore bancaires (numéros de CB) en échange d'un gain (un remboursement par exemple), ou au risque d'une sanction (fermeture d'un accès par exemple) en se faisant passer pour un acteur officiel.

Ces attaques touchent aussi bien les particuliers que les professionnels. Autrefois facilement identifiables, **elles apparaissent de mieux en mieux réalisées et même les internautes les plus avertis peuvent parfois s'y faire prendre**. Les faux remboursements de la sécurité sociale ou des impôts, ou les fausses confirmations de commandes sur Internet restent dans le peloton de tête des vagues régulières qui ciblent les particuliers.

Du côté des professionnels, ce sont les arnaques à la mise en conformité RGPD* ou à la fermeture d'un nom de domaine qui font des victimes notamment sur les plus petites structures.

L'hameçonnage sur les réseaux sociaux tend aussi à se développer, car il permet souvent de contourner la protection mise en place par les opérateurs de messagerie. On voit ainsi fleurir de faux bons d'achats pour des grandes surfaces, ou des places gratuites dans des parcs d'attractions ou des billets gratuits de compagnies aériennes… **Sur les réseaux sociaux, ce sont généralement les victimes elles-mêmes qui vont propager l'escroquerie à leurs contacts en la leur partageant.**

Durant l'année 2019, Cybermalveillance.gouv.fr a émis plusieurs alertes sur ces vagues d'attaques. Leur caractère de plus en plus massif réside certainement dans la facilité qu'ont aujourd'hui les cybercriminels pour se procurer sur les marchés noirs des bases d'adresses conséquentes issues de fuites de données qui ont frappé certaines grandes plateformes Internet ces dernières années. **L'hameçonnage représente la première menace pour les entreprises** avec 23 % des recherches d'assistance et **la troisième menace pour les particuliers** avec 13 % des recherches d'assistance.



* Règlement général sur la protection des données

LES ARNAQUES AU FAUX SUPPORT TECHNIQUE CONTINUENT DE FAIRE DES RAVAGES

L'arnaque au faux support technique consiste principalement en l'apparition, durant une navigation ou après avoir cliqué sur un lien malveillant, d'une fenêtre qui bloque l'écran de l'utilisateur et lui demande de rappeler d'urgence un numéro de support technique au risque de perdre ses informations ou l'usage de son matériel. Après lui avoir demandé d'accéder à distance à son équipement, le prétendu support technique va alors faire payer à la victime un pseudo-dépannage de son matériel et lui faire acheter des logiciels inutiles voire nuisibles.

Identifiée par le dispositif fin 2017 et étendue en 2018, **cette catégorie d'attaque ne cesse de gagner en sophistication**. Elle vise les personnes les moins aguerries et en particulier les personnes âgées qui n'ont souvent même pas l'impression de s'être faites escroquer **tant le discours des cybercriminels semble crédible et étayé de documents d'apparence officielle** (factures, contrats). Ceux-ci peuvent donner confiance aux victimes sur la légitimité du dépannage et du contrat auquel elles ont souscrit. Malgré les nombreuses arrestations dans ces réseaux cybercriminels dans le monde, y compris en France en janvier 2019 par la Gendarmerie nationale, ce type d'arnaque représente encore une part très importante des interventions réalisées par les prestataires référencés par le dispositif sur les publics particuliers. **Une évolution observée en 2019 des modes opératoires est le blocage suite à un clic sur un lien contenu dans un message envoyé par un proche, après le piratage de son compte de messagerie. Cette évolution démontre le caractère aujourd'hui imbriqué et protéiforme des cybermalveillances.**

LES RANÇONGICIELS (*RANSOMWARE*) GAGNENT EN SOPHISTICATION ET CIBLENT LES PROFESSIONNELS

Les rançongiciels sont des programmes malveillants qui chiffrent les fichiers de la victime et lui demandent une rançon pour leur en délivrer la clé. Si, à son origine, cette catégorie d'attaque visait massivement tout un chacun, **on constate aujourd'hui qu'elles sont beaucoup plus ciblées sur des victimes professionnelles pressenties pour pouvoir payer des montants de rançon beaucoup plus importants** au regard des préjudices que ce type d'attaque peut faire subir à leur activité. En 2019, la presse a régulièrement fait écho à ces attaques qui ont touché tant de grands acteurs industriels, que de petites entreprises, des collectivités de toutes tailles, des hôpitaux…

D'après les observations, les groupes de cybercriminels qui commettent aujourd'hui ces attaques commencent par rechercher un point d'accès vulnérable dans le réseau de l'entité. Il s'agira souvent d'un accès à distance ou de télémaintenance insuffisamment sécurisé. Une fois le réseau pénétré, les cybercriminels vont alors le parcourir, parfois durant plusieurs jours voire semaines, pour rechercher les informations et bases de données les plus critiques pour l'entreprise, ainsi que pour identifier ses systèmes de sécurité et de sauvegarde afin de les neutraliser avant de lancer leur attaque.

Ce type d'attaque peut avoir des conséquences économiques très importantes voire désastreuses pour les entreprises qui en sont victimes. Dans les structures victimes qui ne disposent que de sauvegardes en ligne qui ont été détruites par les cybercri-

minels, c'est la survie même de l'activité de l'entité qui peut se jouer. La tentation peut alors paraître forte de payer la rançon. Mais payer, au-delà de l'incertitude d'obtenir les éléments permettant le déchiffrement des données, engendre également le risque de subir de nouvelles attaques du même type, surtout si la manière dont les cybercriminels ont pu pénétrer le réseau n'a pas pu être identifiée et corrigée entre-temps. En 2019, les rançongiciels ont représenté 8 % des recherches d'assistance par les entreprises et collectivités sur la plateforme.

LE CHANTAGE À LA WEBCAM : UN PHÉNOMÈNE QUI EXPLOSE EN 2019

Dans ce type d'attaque, la victime est contactée par un message d'un pseudo-pirate qui prétend avoir pris le contrôle de son ordinateur et l'a filmée alors qu'elle visitait des sites pornographiques. Il la menace alors de divulguer à ses proches des images compromettantes si elle ne paie pas une rançon.

Même s'il n'y a eu aucun cas rapporté de piratage réel et qu'il ne s'agit que d'une simple arnaque, de nombreuses personnes se sont interrogées ou ont été effrayées par la réception de ces messages. **Le dispositif a identifié le phénomène et lancé une première alerte à l'été 2018. Suite à une nouvelle vague d'attaque très massive fin janvier 2019, le dispositif a alors consacré un article entier sur le sujet et modifié ses parcours d'assistance pour intégrer cette menace devenue d'ampleur.**

Durant toute l'année 2019 et par vagues successives, cette catégorie d'attaque a fait l'objet d'une part importante des recherches d'information et d'assistance sur la plateforme, et d'interventions des prestataires qui y sont référencés.

Les vagues d'attaques qui ont suivi, ont démontré qu'elles étaient mises en œuvre par différents cybercriminels, s'exprimant dans diverses langues et allant parfois jusqu'à écrire aux victimes avec leur propre adresse de messagerie et/ou en leur envoyant l'un de leurs mots de passe pour appuyer leurs menaces. Ces informations étaient, là aussi, souvent facilement accessibles pour les cybercriminels sur les marchés noirs et issues de fuites de données de différentes grandes plateformes. Ils ont alors pu jouer sur le fait que nombre de personnes ne changent malheureusement que très rarement voire jamais leur mot de passe, ignorant qu'il a été compromis et qu'il est entre les mains de cybercriminels.

Suite à la mise en place sur la plateforme d'une lettre plainte permettant de signaler ce type d'arnaque aux autorités judiciaires, deux arrestations ont pu avoir lieu en France en septembre et décembre 2019.

Focus sur les chiffres du chantage à la webcam

« Cybermalveillance.gouv.fr est devenu un partenaire de premier rang dans la lutte contre la cybercriminalité envers les particuliers grâce à sa capacité à observer et à détecter les phénomènes rapidement, et de les prévenir par la diffusion d'information au public, également via les réseaux sociaux. »

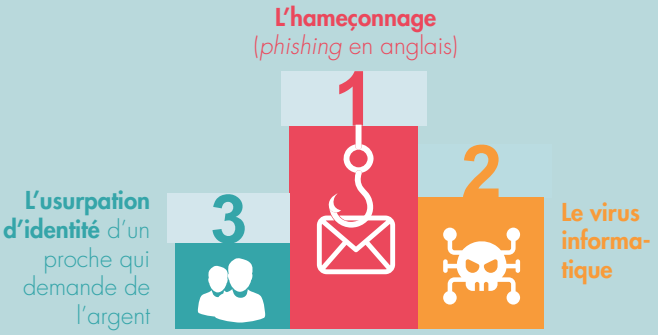
ALICE CHÉRIF
VICE-PROCUREUR, CHEF DE SECTION PÔLE CYBERCRIMINALITÉ F1 – PARQUET DE PARIS

MESURER

ENQUÊTE SUR LA PERCEPTION DU RISQUE NUMÉRIQUE ET LA NOTORIÉTÉ DU DISPOSITIF CYBERMALVEILLANCE.GOUV.FR

En partenariat avec l'INC, Cybermalveillance.gouv.fr a lancé en juin 2019 une étude dont l'objectif était de mesurer son niveau de notoriété auprès des publics, mais aussi de connaître leur connaissance en matière de sécurité numérique, pour mieux adapter ses outils et messages de prévention.

Menée sur un panel représentatif de 4 507 personnes, l'étude a montré que plus de **9 Français sur 10 avaient déjà été confrontés à un acte de malveillance sur Internet.** 8 % disaient connaître le dispositif Cybermalveillance.gouv.fr. Sur l'échelle des actes de cybermalveillance les plus fréquents pour les personnes sondées, on trouve dans l'ordre :



S'agissant de l'hameçonnage, l'étude nous apprend que **54 % des personnes interrogées ne font rien de particulier** et ne signalent donc pas aux autorités les actes de cybermalveillance qu'ils ont subis. Quant aux personnes qui ont vu leur identité usurpée, elles se sont débrouillées seules ou avec un proche pour 37 %.

Les enseignements généraux tirés de ces résultats sont de deux ordres :

1. **La nécessité de poursuivre les actions de prévention auprès des citoyens.**
2. **Le besoin de faire connaître le plus largement possible le dispositif Cybermalveillance.gouv.fr afin de permettre aux citoyens de mieux comprendre les risques pour s'en prémunir et d'agir efficacement quand ils sont victimes.**

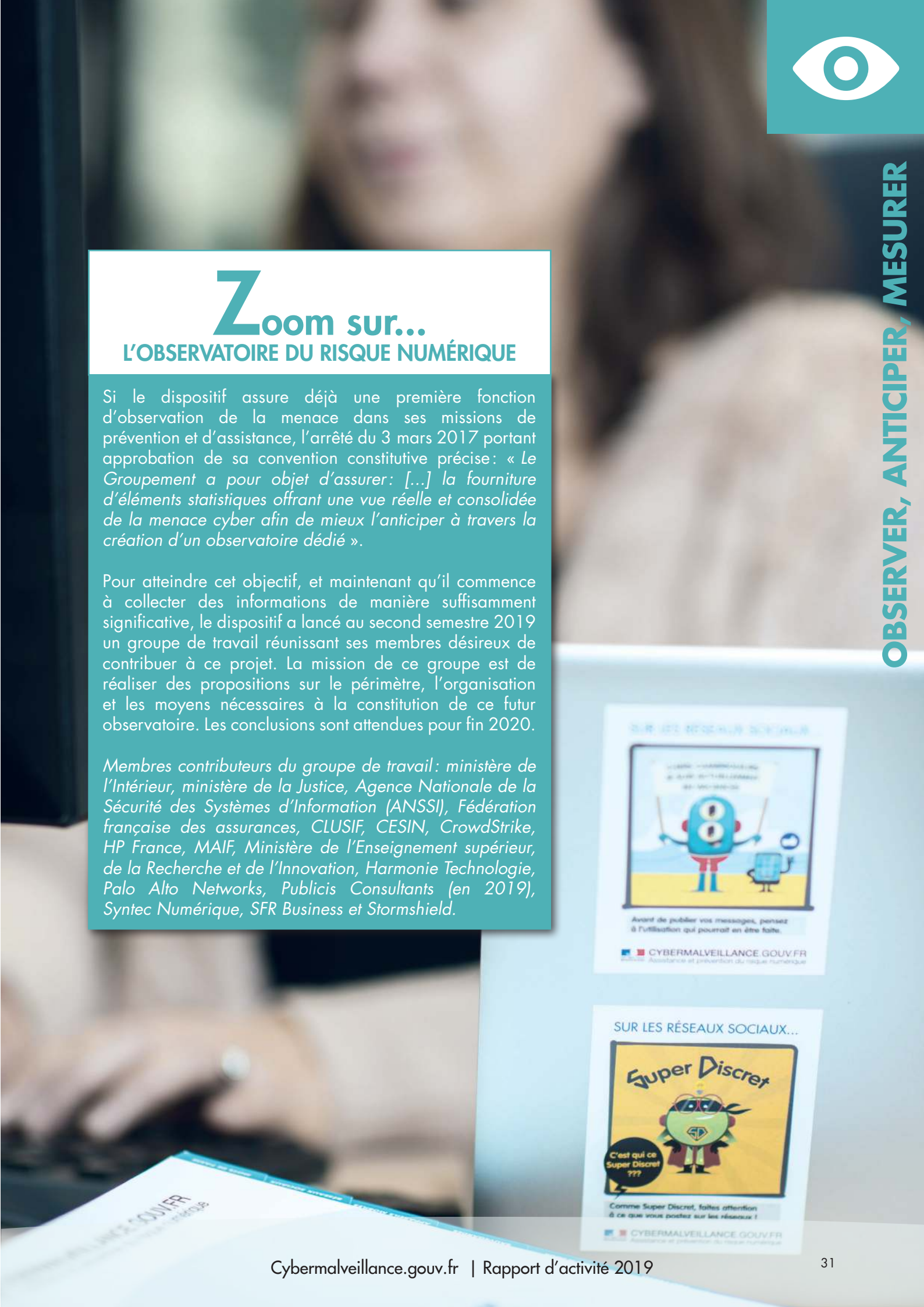
Le dispositif souhaite pérenniser cette approche, en relançant chaque année, une étude de notoriété.

Zoom sur...
L'OBSERVATOIRE DU RISQUE NUMÉRIQUE

Si le dispositif assure déjà une première fonction d'observation de la menace dans ses missions de prévention et d'assistance, l'arrêté du 3 mars 2017 portant approbation de sa convention constitutive précise : « *Le Groupement a pour objet d'assurer : [...] la fourniture d'éléments statistiques offrant une vue réelle et consolidée de la menace cyber afin de mieux l'anticiper à travers la création d'un observatoire dédié* ».

Pour atteindre cet objectif, et maintenant qu'il commence à collecter des informations de manière suffisamment significative, le dispositif a lancé au second semestre 2019 un groupe de travail réunissant ses membres désireux de contribuer à ce projet. La mission de ce groupe est de réaliser des propositions sur le périmètre, l'organisation et les moyens nécessaires à la constitution de ce futur observatoire. Les conclusions sont attendues pour fin 2020.

Membres contributeurs du groupe de travail : ministère de l'Intérieur, ministère de la Justice, Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), Fédération française des assurances, CLUSIF, CESIN, CrowdStrike, HP France, MAIF, Ministère de l'Enseignement supérieur, de la Recherche et de l'Innovation, Harmonie Technologie, Palo Alto Networks, Publicis Consultants (en 2019), Syntec Numérique, SFR Business et Stormshield.



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

CYBERMALVEILLANCE.GOUV.FR

Assistance et prévention du risque numérique

GIP ACYMA
6 rue Bouchardon, 75010 Paris
www.cybermalveillance.gouv.fr

Suivez-nous sur :