TERRITOIRES ET DÉMARCHE COLLABORATIVE

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

UNE DÉMARCHE COLLABORATIVE AU PROFIT DES VICTIMES

Le dispositif national d'assistance aux victimes : Cybermalveillance.gouv.fr reflète une démarche collaborative fédérant des acteurs publics et privés : particuliers, entreprises, collectivités et associations.
Le dispositif a une capacité à accompagner la victime dans sa démarche judiciaire et à l'orienter vers des experts pour gérer une crise. Le dispositif a lancé un label, élaboré en partenariat avec l'AFNOR et les associations professionnelles, qui signale la fiabilité et les compétences de prestataires spécialisés en matière de cybersécurité.
Une de ses spécificités est de savoir identifier des phénomènes à partir d'événements discrets et épars et de les assembler pour mettre en évidence une stratégie d'attaque sérielle et d'un volume important.
Sa force est également d'être un outil de prévention en donnant l'accès aux documents recensant les bonnes pratiques. Il joue un rôle majeur en concentrant des expertises, en assistant les structures en difficultés, répondant ainsi à la mission d'intérêt public que lui a assigné L'État.

Cybermalveillance.gouv.fr : au cœur de la cybersécurité collective et collaborative

Par Jérôme Notin

Lancé en octobre 2017, le dispositif national d'assistance aux victimes cybermalveillance.gouv.fr, piloté par le Groupement d'Intérêt Public ACYMA, est par essence une démarche collective et collaborative qui fédère des acteurs publics et privés pour une meilleure cybersécurité.

La stratégie nationale pour la sécurité du numérique, qui appelait à la création du dispositif d'assistance aux victimes d'actes de cybermalveillance, indiquait dès 2015 : « 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, plateformes numériques, fournisseurs de solutions ».

JÉRÔME NOTIN

Directeur général du GIP ACYMA
Chef d'escadron de la réserve citoyenne cyberdéfense de la gendarmerie

Notre collectif était né.

Rappel sur l'organisation

Cybermalveillance.gouv.fr a trois missions :

- la sensibilisation et la prévention par la diffusion de bonnes pratiques en cybersécurité et la diffusion d'alertes contextualisées ;
- l'assistance aux victimes par une aide au diagnostic du problème, des conseils simples et adaptés, une orientation vers les services compétents, voire vers des prestataires spécialisés de proximité en capacité de les assister ;
- l'observation de la menace afin de détecter les phénomènes émergents pour pouvoir les anticiper et y répondre.

Les publics du dispositif sont les particuliers, les entreprises, les collectivités et les associations, hors opérateurs d'importance vitale et de services essentiels.

Le choix du vecteur administratif retenu a été de créer un groupement d'intérêt public (GIP), le GIP ACYMA. Ce partenariat public-privé rassemble les acteurs de l'État et de la société civile engagés dans sa mission d'intérêt public de lutte contre la cybermalveillance, qui travaillent de manière collaborative au quotidien.

Parmi les membres du GIP, on peut ainsi citer l'ANSSI, qui relève des services du Premier ministre et le ministère de l'Intérieur qui ont co-piloté sa conception, ainsi que le ministère de la Justice, le ministère de l'Économie et des Finances et le secrétariat d'État en charge du numérique.
À leurs côtés travaillent de nombreux acteurs de la société civile comme des associations de consommateurs et d'aide aux victimes, des représentations professionnelles de type fédérations ou syndicats, des assureurs, des opérateurs, des constructeurs, des éditeurs…
Fin 2020, le groupement d'intérêt public est fort de 47 membres. Outre leur soutien financier, ces membres renforcent et démultiplient les actions du dispositif en participant à des groupes de travail pilotés par les agents du GIP.

Un capteur en temps réel de la cybermalveillance

Une originalité du dispositif est qu'il intervient généralement en amont des autres services de l'État lorsque la victime rencontre un incident. Il est en cela un capteur très intéressant pour les pouvoirs publics de la cybermalveillance pour des victimes qui n'envisagent pas toujours en première intention de déposer plainte parce qu'elles n'ont pas conscience que leur incident pourrait faire l'objet de poursuites, qu'elles pensent que les poursuites dans la sphère cyber ont peu de chance d'aboutir ou enfin qu'elles ont honte et craignent pour leur image. Le dispositif intervient notamment en incitant systématiquement la victime au dépôt de plainte chaque fois qu'une infraction peut être retenue, mais aussi en l'aidant dans sa démarche au travers des conseils élaborés en collaboration étroite avec le ministère de l'Intérieur.

Une des forces du dispositif est donc sa capacité à identifier des phénomènes à partir d'événements qui, parfois pris séparément, peuvent être considérés comme marginaux mais dont le rassemblement met en évidence leur caractère sériel voire massif. C'est ainsi que le dispositif a pu contribuer dès ses premiers mois de fonctionnement à l'identification du phénomène cybercriminel de masse qu'est « l'arnaque au faux support technique ». L'identification de l'ampleur de cette catégorie d'escroquerie a pu être réalisée en grande partie grâce aux rapports techniques d'intervention sur le terrain qui lui sont remontés par ses prestataires référencés. Dans la grande majorité des cas, si les victimes avaient bien eu l'impression à un moment ou un autre de s'être faites arnaquer,

elles n'envisageaient généralement pas pour autant de déposer plainte, pour les raisons évoquées précédemment.

L'identification de ce phénomène cybercriminel et les échanges opérationnels qui ont pu être conduits avec les services des ministères de l'Intérieur et de la Justice ont conduit à l'ouverture d'une enquête par la section de lutte contre la cybercriminalité du parquet de Paris, en mars 2018. Cette enquête, confiée au centre de lutte contre les criminalités numériques (C3N) du pôle judiciaire de la Gendarmerie nationale, a conduit à l'interpellation et la mise en examen de trois individus ayant fait près de 8 000 victimes et la saisie de près de 2 millions d'euros début 2019. D'autres enquêtes sur ce phénomène, qui perdure et fait encore quotidiennement de nombreuses victimes, sont aujourd'hui toujours en cours.

Le début 2019 a également vu 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 le dispositif et les magistrats spécialisés du pôle cybercriminalité. Ces magistrats élaborent aussitôt un modèle de lettre plainte électronique 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. Grâce aux informations collectées, les services d'enquête identifient deux personnes. Elles sont interpellées en septembre, puis en décembre 2019.

Cette possibilité d'identification des menaces au plus près de leur apparition permet également au dispositif d'alerter les populations sur son site Internet et/ou ses réseaux sociaux (Twitter, Facebook, LinkedIn). Grâce à l'appui de ses membres, plusieurs alertes émises par le dispositif ont été largement reprises par les médias grands publics (Presse, émissions et journaux télévisés de grand audience comme des 20h00), démultipliant ainsi les capacités d'atteindre le plus grand nombre de victimes potentielles.

Un outil de sensibilisation

La sensibilisation reste la meilleure arme pour éviter les cyberattaques. Cette sensibilisation aux cybermenaces et aux bonnes pratiques à adopter pour les détecter et les éviter est donc primordiale. En effet, ce sont les utilisateurs qui par leurs pratiques et leur vigilance pourront être les premiers remparts de la cybersécurité. Ils doivent être considérés comme des acteurs à part entière. Or, cela reste souvent un exercice difficile, car les sujets de sécurité numérique sont généralement ressentis comme rébarbatifs et sources de contraintes pour les utilisateurs.

© ACYMA

C'est en partant de ce constat, issu des travaux conduits avec ses membres, que le dispositif a réalisé en 2018 le premier volet de son kit de sensibilisation, le plus facile d'accès possible.

© Acyma – Gendarmerie

Au titre de la prévention et de la sensibilisation, on peut également citer la campagne partenariale avec la Gendarmerie nationale, sur une initiative du GGD88, avec la diffusion de bonnes pratiques sur des supports du quotidien : 800 000 fourreaux à pain ont été distribués par huit groupements : dispositif R-Mess, Prix de la Prévention 2019 de la Gendarmerie nationale.

(1) Etalab est un département de la direction interministérielle du numérique (DINUM), dont les missions et l'organisation sont fixées par le décret du 30 Octobre 2019. Il coordonne notamment la conception et la mise en œuvre de la stratégie de l'État dans le domaine de la donnée. Il coordonne les actions des administrations de l'Etat et leur apporte son appui pour faciliter la diffusion et la réutilisation de leurs informations publiques.

Le kit complet a été finalisé en juin 2019. Il peut être téléchargé gratuitement. Il comprend différents types de supports (courtes vidéos, infographies, fiches pratiques, mémo...). Il vise les usages personnels de manière pédagogique et illustrée, sur des sujets qui peuvent également intéresser l'entreprise dans ses pratiques professionnels. Par exemple, si une personne sait détecter et réagir à un message d'hameçonnage (*phishing*) dans ses usages personnels, elle saura également le faire dans ses usages professionnels. Un choix fort a été de le publier sous licence *Etalab 2.0*[1], qui permet à toute entité de le modifier, et donc d'ajouter ou supprimer du contenu. Beaucoup de structures ont par exemple simplement ajouté le logo de leur entité afin que l'adhésion des collaborateurs soit encore plus forte.

La période Covid-19

Comme lors de toute crise, les cybercriminels savent très vite s'adapter pour en tirer profit. Le GIP a donc rapidement proposé un contenu de prévention spécifique. Dès la veille du confinement, nous avons publié sur notre site un appel au renforcement de la vigilance en termes de sécurité en présageant d'un certain nombre de menaces que la situation pourrait engendrer, tant pour les particuliers que pour les professionnels. Force a été malheureusement de constater que nos prévisions se sont avérées exactes. Cet article a d'ailleurs battu un record de consultation sur notre site en quelques semaines.

Dans les premiers jours du confinement, une autre production majeure a été diffusée sur le télétravail en situation de crise proposant des recommandations de cybersécurité pour répondre au besoin tant des employeurs que de leurs collaborateurs.

La plate-forme a ainsi fonctionné à plein régime avec un taux de fréquentation qui a augmenté de 400 % durant les premières semaines du confinement. Elle a dans le même temps continué à recevoir des mises à jour régulières de fonctionnalités et de contenus. Côté assistance aux victimes et relations avec les professionnels référencés, la réactivité a été assurée.

A noter que le dispositif a finalisé trois projets structurants durant cette période. Le premier est le lancement de son label ExpertCyber auprès des prestataires, initié en 2019. Ce label, élaboré en partenariat avec l'AFNOR et les associations professionnelles vise à apporter un niveau de reconnaissance des compétences des prestataires spécialisées en cybersécurité.

© ACYMA

Le GIP a également conçu une campagne télévisée de spots de sensibilisation grand public, réalisée en partenariat avec France Télévisions et diffusée en mai et juin sur ses chaînes ainsi que sur celles des groupes TF1 et Canal+. Les quatre clips de 30 secondes ont été réalisés en moins de trois semaines.

Enfin, au regard du besoin lié au confinement, une intégration d'un lien vers la brigade numérique de la Gendarmerie nationale a été réalisée dans les espaces privés des professionnels et depuis l'apparition de certaines cybermalveillances les concernant. Les victimes peuvent désormais avoir directement une l'assistance pour déposer une plainte lorsqu'une cybermalveillance

cible leur entité. Projet initié en janvier 2020 avec la Gendarmerie, il a été jugé utile de le rendre accessible au plus vite du fait des contraintes du confinement et de l'augmentation de la menace.

Tout ceci en parallèle du travail de fond réalisé par le dispositif.

Et demain ?

L'avenir du GIP s'annonce toujours plus collectif et productif, du fait du renforcement de son équipe avec l'arrivée de 3 nouveaux agents mis à disposition par le ministère de l'Intérieur et par l'intégration de nouveaux membres au sein du GIP, comme le ministère des Armées.

L'année 2021 sera également marquée par le lancement au FIC du label ExpertCyber. Ce label a vocation à apporter une reconnaissance des compétences des professionnels de la cybersécurité et garantir un accompagnement de qualité ainsi qu'une meilleure lisibilité des prestations et services aux publics professionnels (entreprises, associations, collectivités).

Plusieurs nouveaux supports de sensibilisation aux bonnes pratiques de la cybersécurité et d'assistance face aux cybermenaces en cours de finalisation seront également publiés dans les prochains mois.

Enfin, de nombreux projets sont en gestation avec nos membres en bilatéral ou réunis au sein de groupes de travail.

Pour faire face à la problématique de la cybermalveillance, une démarche collaborative et collective avec tous les acteurs impliqués est indispensable, car il serait évidemment illusoire de penser que l'on puisse vaincre seul ce fléau. Qu'il s'agisse des pouvoirs publics, des acteurs de la société civile ou même du simple citoyen, chacun peut avoir un rôle à jouer et une contribution à apporter en fonction de ses prérogatives et moyens dans la prévention et l'assistance aux victimes de la cybermalveillance. A ce titre, le dispositif Cybermalveillance.gouv.fr joue un rôle majeur en concentrant et fédérant les énergies et bonnes volontés pour en amplifier les effets au service de la mission d'intérêt public qui lui a été assignée par L'État.

À propos de Cybermalveillance.gouv.fr

Lancé en octobre 2017, Cybermalveillance.gouv.fr est le dispositif national d'assistance aux victimes de cybermalveillance. Ce dispositif a été incubé par l'Agence nationale de sécurité des systèmes d'information (ANSSI) en copilotage avec le ministère de l'Intérieur et avec le soutien des ministères de l'Économie et des Finances, de la Justice et du secrétariat d'État chargé du Numérique. Il est désormais piloté par le Groupement d'intérêt Public (GIP) ACYMA.

SES PUBLICS SONT :

- **les particuliers**
- **les entreprises** (hors opérateurs critiques – OIV)
- **les collectivités** (hors opérateurs critiques – OIV)

SES MISSIONS SONT :

- **l'assistance** aux victimes d'actes de cybermalveillance
- **l'information et la sensibilisation** au niveau national sur la sécurité numérique
- **l'observation** du risque numérique pour pouvoir l'anticiper

SES MEMBRES SONT :

L'AUTEUR

Impliqué dans la sécurité numérique depuis de nombreuses années, Jérôme Notin dispose d'expériences dans la création et la direction d'entreprises. Il a rejoint l'ANSSI en mai 2016 en qualité de préfigurateur du dispositif et a été nommé, en mars 2017, directeur général du GIP ACYMA lors de sa création. Il est par ailleurs ancien gendarme auxiliaire (94/10 PSIG de Blois) et réserviste citoyen de défense et de sécurité de la Gendarmerie nationale.