



15ème législature

Question N° : 895	De M. Fabien Gouttefarde (La République en Marche - Eure)	Question écrite
Ministère interrogé > Intérieur		Ministère attributaire > Intérieur
Rubrique >numérique	Tête d'analyse >Cybermalveillance	Analyse > Cybermalveillance.
Question publiée au JO le : 05/09/2017 Réponse publiée au JO le : 20/02/2018 page : 1454 Date de signalement : 23/01/2018		

Texte de la question

M. Fabien Gouttefarde attire l'attention de M. le ministre d'État, ministre de l'intérieur, sur l'expérimentation de la plateforme d'assistance aux victimes d'actes de cybermalveillance « ACYMA ». En janvier 2017, au Forum international de la cybersécurité, Mme Axelle Lemaire, secrétaire d'État aux numériques, avait annoncé le lancement d'une plateforme d'assistance aux victimes d'actes de cybermalveillance (ACYMA). Chaque année, le nombre de signalements traités par l'Agence nationale de la sécurité des systèmes d'information augmente de façon exponentielle et 2017 a été marqué par des incidents publics de plus en plus nombreux et des cyberattaques mondiales sans précédent : attaques coordonnées et simultanées à des fins de déstabilisation, rançongiciel (Wannacry, Pétaya), espionnage informatique ciblant le secteur industriel, exfiltration massive de données client, attaques en déni de service exploitant des objets connectés, hacktivisme en soutien à l'État islamique et défaçage de sites de collectivités territoriales. Face à cette menace croissante, il est primordial de sensibiliser le grand public mais également de se mobiliser afin d'accompagner techniquement et juridiquement les victimes d'actes de cybermalveillance. Le 30 mai 2017, l'expérimentation de la plateforme « cybermalveillance.gouv.fr » a été lancée sur la région Haut-de-France et il a été évoqué une généralisation possible en octobre 2017. À ce jour, aucun retour n'a été fait sur cette expérimentation. Il souhaiterait connaître le bilan de cette expérimentation et savoir si une telle plateforme va bientôt être étendue à tout le territoire.

Texte de la réponse

Le groupement d'intérêt public (GIP) « ACYMA » (actions contre la cybermalveillance) a pour objet d'assurer trois missions. 1) Une mission d'intérêt général portant sur l'assistance aux particuliers, aux entreprises et aux collectivités territoriales, victimes d'actes de cybermalveillance par la mise en place d'un « guichet unique ». La première mission est essentiellement portée par la plateforme d'assistance aux victimes d'actes de cybermalveillance : www.cybermalveillance.gouv.fr. La plateforme assure la mise en relation des victimes après autodiagnostic (sur la base d'un parcours d'orientation) avec une assistance de proximité composée d'intervenants susceptibles d'assister techniquement les victimes (réparateurs informatiques, associations d'entraide, sociétés spécialisées dans la réponse à incident informatique) et des services de l'Etat. La plateforme donne également les premiers conseils aux victimes lorsque l'intervention technique n'est pas forcément nécessaire. L'expérimentation de la plateforme d'assistance a eu lieu de fin mai à mi-octobre 2017 sur la région des Hauts-de-France. Les résultats durant cette période sont : - 724 mises en relation victimes/prestataires au total dans la phase d'expérimentation de 4 mois ; - 83 % des incidents de cybermalveillance déclarés comme des virus et 44% du total des incidents déclarés « virus » correspondent à des attaques de type ransomware. Au cours de l'expérimentation en région Hauts-de-France, 1 123 prestataires locaux ont été référencés par le GIP en préparation du lancement national. Le lancement

national du dispositif a eu lieu le 17 octobre 2017. L'ensemble du territoire national est couvert par des prestataires référencés, sauf au niveau de la Nouvelle-Calédonie où le dispositif n'est pas opérationnel en raison d'une difficulté liée à la base de données de data.gouv.fr (résolution à l'étude). Au 31 janvier 2018, le nombre de prestataires référencés s'est établi à 1 419 et il y a eu au total 4 904 mises en relation victimes/prestataires. 2) Une mission de sensibilisation du public sur les enjeux de la sécurité et de la protection de la vie privée numérique en lien avec les autorités de l'État et le développement de campagnes de prévention en la matière. La plateforme numérique délivre un premier niveau d'information aux utilisateurs et participants au dispositif sous forme de fiches, guides et vidéos de sensibilisation. Cinq films de sensibilisation ont été réalisés par le GIP et sont en ligne sur la plateforme. De nombreuses fiches correspondant à des typologies d'attaques y figurent et sont complétées régulièrement sur de nouveaux phénomènes (comme par exemple l'arnaque au faux support technique en novembre 2017). Depuis octobre 2017, le GIP dispose également d'un compte référencé « @cybervictimes » sur les réseaux sociaux Twitter et Facebook. Le GIP réalise également des actions de communication dans les médias, comme à l'occasion du dernier « Black Friday », le vendredi 24 novembre 2017, en appelant à la vigilance sur les cyber-arnaques. L'effort principal du GIP « ACYMA » portera en 2018 sur la communication afin de faire connaître le dispositif auprès des citoyens, des entreprises et des collectivités territoriales, dans l'objectif d'augmenter la visibilité de la plateforme et son utilisation en terme de parcours victimes, mais aussi pour impliquer un plus grand nombre de partenaires privés ou publics dans la sensibilisation du public. Par ailleurs, un kit de sensibilisation est en cours de réalisation. L'objectif est de s'adresser au particulier à travers le canal professionnel. Ayant la possibilité de réserver en ligne ce kit, différentes entités (entreprises, collectivités, organismes, etc.) se sont signalées : 780 inscriptions représentant potentiellement 3,5 millions de collaborateurs ont été comptabilisées au 31 janvier 2018, soit une semaine après l'annonce. 3) Une mission de 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. Plus la plateforme est connue et utilisée, plus elle permettra d'apporter des éléments d'information dans un temps court, sur les incidents de sécurité informatiques rencontrés par les victimes participant au dispositif. Les informations techniques ainsi recueillies pourront être analysées notamment pour informer et alerter les autorités et le public sur l'état de la menace au travers de la mise en place future d'un observatoire du risque numérique. Cependant, sans attendre l'établissement de cet observatoire, des primo-analyses sont déjà conduites comme celle portant sur l'arnaque au faux support technique, qui a permis aux forces de sécurité intérieure d'accélérer les enquêtes en cours.