Partager les outils de lutte contre la cybermalveillance

Entretien avec Jérôme Notin, Directeur général du dispositif d'assistance aux victimes de cybermalveillance

Jérôme Notin

Pourriez-vous nous présenter le dispositif national d'assistance aux victimes de cybermalveillance ?

Au regard du nombre croissant d'attaques, le gouvernement a décidé dans sa stratégie numérique présentée en juin 2015 d'offrir, à travers la création d'un dispositif d'assistance aux victimes de cybermalveillance, un meilleur soutien à l'ensemble de nos concitoyens qu'ils soient particuliers, entreprises ou collectivités face à la cybermalveillance. Ce dispositif s'articule autour de 3 axes : la prévention, l'assistance aux victimes et la prospective. Ces missions sont réalisées en synergie avec les autres services de l'État impliqués dans la lutte contre la cybermalveillance.

Pour porter ces missions d'intérêt général, le gouvernement a souhaité la création d'une entité juridique spécifique. L'Agence nationale de sécurité des systèmes d'information (ANSSI) et le ministère de l'Intérieur, qui ont co-pilotés ce projet, ont retenu la forme d'un groupement d'intérêt public (GIP) qui permet de réunir les forces des acteurs publics et privés, de disposer d'une autonomie de gestion sur le plan opérationnel, tout en restant sous le contrôle de l'État. C'est ainsi qu'est né le GIP ACYMA (actions contre la cybermalveillance) le 3 mars 2017.

C'est ce GIP ACYMA qui a créé la plateforme Cybermalveillance.gouv.fr. Après une expérimentation à partir de mai 2017 dans la région des Hauts-de France, la plateforme a généralisé l'accès à ses services sur l'ensemble du territoire national en octobre 2017. Ce lancement national a été réalisé en présence du Secrétaire d'État chargé du numérique, Mounir Mahjoubi, du Secrétaire général de la défense et de la sécurité nationale, du directeur général de l'ANSSI, du président de la Fédération française de l'assurance, ainsi que de nombreux représentants du ministère de l'Intérieur, dont le Délégué ministériel aux industries de sécurité et à la lutte contre les cybermenaces.

Quels sont ses missions précises ?

La première mission du dispositif Cybermalveillance.gouv.fr est d'apporter une assistance aux victimes de cybermalveillance. Au travers de la plateforme Cybermalveillance.gouv.fr, les victimes décrivent leur problème en répondant à des questions types qui permettent d'établir un diagnostic. A l'issue, il leur sont donnés les premiers conseils puis elles sont orientées au besoin vers les structures existantes pour les assister (par ex. internet-signalement.gouv.fr). A ce titre, Cybermalveillance.gouv.fr a vocation à être le point d'entrée unique vers les différents services de l'État pour tous les citoyens victimes de cybermalveillance.

La plateforme Cybermalveillance.gouv.fr propose également aux victimes des prestataires privés de proximité susceptibles de les accompagner pour remédier au problème qu'elles rencontrent si une intervention technique s'avère nécessaire. A ce jour, plus de 1 500 prestataires sont référencés et couvrent l'ensemble du territoire national.

Enfin, toujours dans l'esprit d'assister les victimes, la plateforme les accompagne dans leur démarche juridique. Dans ce cadre, elle propose pour certains types de cybermalveillance des fiches réflexes qui, entre autres éléments sur les bonnes pratiques à adopter pour s'en prémunir et les actions à mener lorsque l'on en est victime, indique les incriminations pénales susceptibles de pouvoir être retenues lors du dépôt de plainte.

La seconde mission du dispositif Cybermalveillance.gouv.fr est la sensibilisation du public aux bonnes pratiques en matière de sécurité et de protection de la vie privée numériques. Des contenus de sensibilisation réalisés par le dispositif avec le soutien de ses membres sont disponibles sur son site Internet. Il met également en valeur des guides et supports pédagogiques réalisés par les tiers sélectionnés pour leur complétude et la qualité du

message délivré. Le dispositif réalise de surcroît des actions ponctuelles de sensibilisation dans différents cercles professionnels de son coeur de cible. Ces actions et contenus sont relayés sur les réseaux sociaux (Twitter, Facebook et LinkedIn) afin de toucher le plus grand nombre de nos concitoyens. Le dispositif également a pour mission à terme de réaliser des campagnes de prévention nationales sur les sujets liés à la sécurité du numérique.

La troisième mission du dispositif Cybermalveillance.gouv.fr est la mise en place d'un observatoire de la menace numérique, qui sera mis en place lorsque les remontées des prestataires seront en nombre suffisant. Celui-ci visera à apporter une vue sur la réalité de la cybermenace au-delà des statistiques des infractions relevées qui ne représente parfois qu'une partie infime des phénomènes pas ou peu signalés aux forces de l'ordre. Cette vision offrira au pouvoir politique, aux services de sécurité et aux acteurs de la société civile une cartographie des risques et une analyse des tendances leur permettant une meilleure prise de décisions sur les axes d'effort nécessaires.

Quels sont ses liens avec l'Agence nationale de sécurité des systèmes d'information (ANSSI) ?

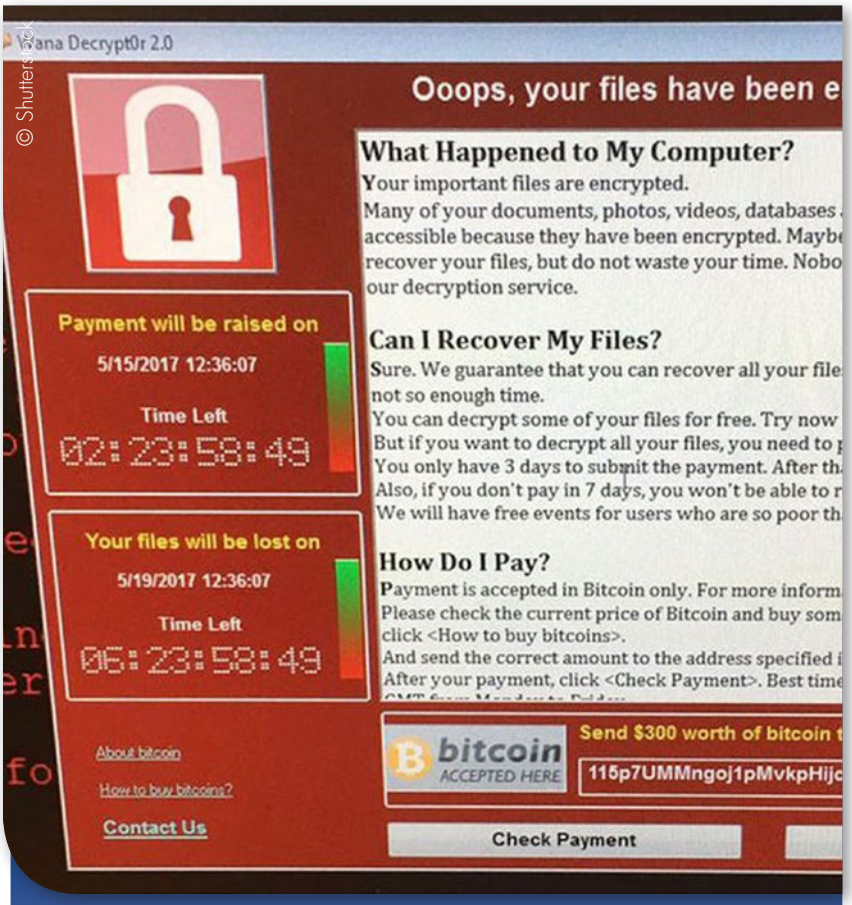
L'ANSSI a incubé le dispositif et nous sommes depuis le lancement au quotidien en relation avec elle, que cela soit sur des aspects opérationnels et organisationnels. Le président du GIP est d'ailleurs l'actuel directeur général de l'ANSSI, Guillaume Poupard.

Comment sont réparties les missions entre l'ANSSI et le dispositif Cybermalveillance ?

L'ANSSI s'adresse principalement aux administrations étatiques et aux critiques (OIV, OSE ...). Notre public étant les particuliers, TPE, PME et collectivités, nous sommes donc très complémentaires, et nous œuvrons en très étroite coordination vis à vis de nos publics respectifs.

Pourriez-vous rappeler ce qu'est un opérateur d'importance vitale (OIV) ?

Un OIV est un opérateur public ou privé dont l'activité est indispensable au bon fonctionnement de la nation. Si la liste des entités est classifiée, les secteurs sont publics et concernent par exemple la gestion de l'eau, de l'alimentation ou des transports. Si un OIV n'est plus en capacité de rendre le service attendu, cela pose un problème de sécurité nationale.



Simulation d'attaque par rançongiciel, plus spécifiquement dédiée aux PME. Les fichiers de la victime sont cryptés jusqu'à paiement d'une rançon à très courte échéance.

Existe-t-il des dispositifs équivalents dans les autres pays ? Dans ce cas, avez-vous des contacts, des échanges de pratiques ?

A ma connaissance seul le Luxembourg propose une assistance à ses concitoyens par une liste statique de prestataires sur le site de l'autorité nationale. Nous allons plus loin et cela intéresse d'ailleurs beaucoup de gouvernements européens avec lesquels nous partageons notre retour d'expérience. Certains mettront d'ailleurs en place dès 2019 une démarche identique à la nôtre, avec potentiellement certains outils que nous leur fournirons au titre de la coopération européenne.

Sensibiliser les particuliers au risque numérique et leur offrir un meilleur soutien dans la lutte contre la cybermalveillance.

Quels sont les relations avec les différents ministères ?

Certains ministères font partie du dispositif et nous travaillons au quotidien avec eux. Le GIP a comme membre fondateur les services du Premier ministre (SGDSN-ANSSI), le ministère de l'Intérieur, le ministère de la Justice, le ministère de l'Économie et des Finances et le Secrétariat d'État au Numérique. Ils sont majoritaires au conseil d'administration et à l'assemblée générale en termes de voix. Il est également composé de représentants du secteur privé avec des associations de consommateurs, des fédérations d'entreprises des secteurs du numérique ou de l'assurance, des représentants des chambres de commerce et d'industrie, des entreprises, des services d'assistance aux victimes et des entreprises du secteurs du numériques tels des opérateurs de télécommunications, des éditeurs de logiciels, des sociétés spécialisées dans la cybersécurité.

Nous avons également des échanges avec d'autres ministères qui ne font pas (encore ?) partie du GIP afin qu'ils nous appuient dans nos missions, au titre de leurs prérogatives ou du public auquel ils s'adressent.

Et avec le monde de l'entreprise ?

Le GIP est par nature ouvert sur le monde de l'entreprise, à laquelle il s'adresse par ailleurs à travers ses missions. Nous sommes donc au contact permanent des entreprises et des collectivités pour leur porter assistance ou produire du *contenu de sensibilisation* avec eux.

Comment ce dispositif est-il financé ?

Nous bénéficions d'une subvention de l'ANSSI qui représente 70 % de notre budget, complétée par la participation des membres privés. A terme l'objectif est que la part des membres privés augmente afin que le GIP dispose de plus de moyens, en particulier pour communiquer encore plus largement auprès de ses publics.

Pouvez-vous nous donner quelques chiffres dans le domaine de la cybermalveillance en France ?

S'il est un peu tôt pour avoir une vision complète de la menace sur nos populations, nous savons que nous avons déjà plus de 11 000 victimes depuis notre lancement, ce qui démontre l'intérêt de notre dispositif. De même, les premiers mois de fonctionnement ont déjà permis de confirmer certaines tendances et d'identifier l'émergence ou la recrudescence de certaines menaces. A titre d'exemple, l'arnaque au faux support technique (Tech Support Scam, en anglais) apparaît comme une menace ascendante. Les victimes se font piéger durant une navigation sur Internet par des messages alarmistes leur demandant de rappeler sans délai un faux support technique pour « décontaminer » ou « réparer » leur ordinateur, au prix de plusieurs centaines d'euros pour cette prestation réglée par carte de crédit. Les cybercriminels imposent souvent à la victime d'installer sur sa machine des logiciels de prise de contrôle à distance. Parfois, elle est également menacée de destruction de ses fichiers ou de la divulgation de ses données personnelles si elle refuse de payer une nouvelle fois. Cette menace touche à ce jour plus de victimes que les rançongiciels en nombre de cas référencés par Cybermalveillance.gouv.fr et apparaît donc devoir être assortie d'une forte priorité dans la démarche visant à la circonscrire.

Qu'est-ce que le kit de *sensibilisation* proposé par Cybermalveillance ?

Le GIP réalise, avec ses membres publics et privés, un kit de sensibilisation diffusé sous licence ouverte pour toutes les entreprises et collectivités qui en font la demande. Les collaborateurs, sensibilisés via le canal professionnel, pourront ainsi

apprendre et mettre en place les bonnes pratiques de sécurité du numérique tant pour leurs usages personnels que professionnels.

Les organisations qui participeront à cette opération de sensibilisation contribueront ainsi à améliorer l'hygiène informatique et la résilience de leurs collaborateurs, et par conséquence de l'organisation elle-même.

Cybermalveillance propose au public un service d'information en ligne permettant d'accéder à une liste de prestataires susceptibles d'apporter leur assistance. Comment ceux-ci sont-ils sélectionnés ? Un contrôle de confiance est-il effectué ?

Après plusieurs vérifications, les candidats prestataires sont référencés sur la plateforme Cybermalveillance.gouv.fr. Ceux-ci se sont engagés au travers d'une charte qui encadre leur pratique. Ils peuvent faire l'objet d'une notation de leur intervention par les victimes. Nous travaillons en parallèle à la création d'un label qualité pour certains de ces prestataires.

Comment les prestataires assurent-ils la remontée d'informations (échantillon de virus informatique, modes opératoires) auprès du dispositif Cybermalveillance ?

Les prestataires disposent directement sur notre site d'un espace dédié pour nous faire parvenir du code malveillant ainsi que des informations techniques et opérationnelles sur les incidents qu'ils traitent. Ces informations sont très importantes pour percevoir la réalité de la menace.

Avez-vous un exemple emblématique au sein du monde de l'entreprise et des collectivités ?

Un rapport prestataire qui m'a marqué concerne une association importante. Elle a été victime d'un rançongiciel qui a chiffré une grande partie de ses données. Malheureusement, les sauvegardes n'étaient pas complètes. L'association a donc dû faire appel à des intérimaires pour ressaisir les données qui existaient en version papier. Le reste a été définitivement perdu, ce qui impacte encore aujourd'hui son activité. Cela nous rappelle donc la nécessité d'effectuer des sauvegardes complètes, et de s'assurer de leur bon fonctionnement.

Cybermalveillance.gouv.fr propose un kit de sensibilisation destiné aux entreprises, collectivités et associations pour lutter contre les attaques numériques, susceptibles de coûter beaucoup d'argent et beaucoup de temps.

Quels sont les prochains grands dossiers à venir ?

Nous devons dans les prochains mois, voire les prochaines années, travailler à développer notre notoriété afin que l'ensemble de notre public nous connaisse. C'est un vaste chantier que nous avons déjà entrepris, en particulier grâce aux différents ministères, au service d'information du gouvernement (SIG) et à nos membres. Nous travaillons également d'ores et déjà à la version 2 de notre plateforme qui accompagnera de manière encore plus complète les victimes. Enfin, nous pensons lancer un second kit de sensibilisation dès début 2019.

Entretien réalisé par Patrice Lefort-Lavauzelle

Pour en savoir plus :

https://www.cybermalveillance.gouv.fr/

Pour recevoir le kit de sensibilisation destiné aux entreprises, collectivités et associations :
https://www.cybermalveillance.gouv.fr/inscription-sensibilisation/