COMMUNIQUE DE PRESSE

Paris, le 01/10/2020

Cybermoi/s 2020 : un mois pour se protéger du chantage numérique

La crise sanitaire et le confinement ont engendré une hausse fulgurante de l'utilisation des technologies dans nos vies personnelles et professionnelles. Les pirates du net en ont profité pour intensifier le chantage numérique à coups de rançongiciels et de chantage à la webcam. Pour y faire face, la campagne de sensibilisation du Cybermoi/s donne aux professionnels et aux particuliers les clés pour mieux comprendre et prévenir les menaces liées au chantage numérique.

Rançongiciels : une menace qui explose

Les rançongiciels sont des programmes malveillants permettant aux attaquants de prendre le contrôle à distance d'un ordinateur ou d'un système d'information. Ils rendent la consultation ou l'utilisation des données impossibles, sans le paiement d'une rançon.

Cette menace, qui existe depuis plusieurs années déjà, a augmenté ces derniers mois.

« Depuis le début de l'année 2020, plus de 1 100 victimes, dont 26 % de particuliers, ont demandé de l'assistance sur notre plateforme pour faire face à une attaque par rançongiciel. En recrudescence, ce type de chantage numérique a été la première cause de recherche d'assistance pour les collectivités et la deuxième pour les entreprises et les associations » explique Jérôme Notin, directeur général de Cybermalveillance.gouv.fr.

Certains secteurs d'activités sont particulièrement touchés par les rançongiciels.

« Entre janvier et septembre 2020, l'industrie, les collectivités territoriales et la santé ont été les secteurs d'activité les plus affectés par les attaques par rançongiciels traitées par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) » indique François Deruty, sous-directeur Opérations de l'ANSSI.

Les collectivités territoriales n'échappent pas non plus à la menace.

« L'étude MIPS 2020[1] menée par le Club de la sécurité de l'information français (CLUSIF) a révélé que 30 % des conseils territoriaux et des villes ont été affectés par des rançongiciels, qui représentent désormais la principale cause d'incidents identifiée pour les collectivités territoriales » déclare Cyril Bras, responsable de la partie Collectivités territoriales de l'étude MIPS 2020 et responsable de la sécurité des systèmes d'information de Grenoble-Alpes Métropole.

[1] Étude Menaces informatiques et pratiques de sécurité en France, CLUSIF, 2020 : https://clusif.fr/publications/mips-2020-menaces-informatiques-et-pratiques-de-securite-en-france-edition-2020-rapport-global/?visible=public

Avec le soutien du

GOUVERNEMENT
Liberté
Égalité
Fraternité

Chantage à la webcam : une recrudescence pendant le confinement

Autre forme de chantage numérique, le chantage à la webcam consiste en l'envoi de mails menaçant de publier des vidéos compromettantes, obtenues via la webcam de particuliers, à leurs contacts personnels et/ou professionnels.

Il s'agit en réalité d'un chantage à la webcam prétendument piratée. Les cybercriminels n'ont aucune preuve, souvent parce que la victime n'a jamais consulté les sites mentionnés, et envoient ces mails en masse en espérant qu'une – voire plusieurs – personnes mordent à l'hameçon.

« Pendant le confinement, nous avons constaté une forte recrudescence de chantage à la webcam prétendue piratée lors d'une consultation de site pornographique. Preuve de l'ampleur de ce phénomène, notre page dédiée à cette menace a fait l'objet de plus de 130 000 consultations. Le chantage à la webcam est la quatrième cause de recherche d'assistance sur notre plateforme », constate Jérôme Notin, directeur général de Cybermalveillance.gouv.fr.

Des recommandations indispensables face au chantage numérique

Face à la recrudescence des rançongiciels et du chantage à la webcam, le Cybermoi/s partage tout au long du mois d'octobre, les recommandations indispensables pour mieux se protéger dans son espace de vie numérique, et ce dès le plus jeune âge.

Chantage numérique : comment s'en prémunir ?

- Ne cliquez jamais sur les liens, ne téléchargez jamais de pièces jointes venant d'un expéditeur inconnu.
- Choisissez des mots de passe robustes.
- Pensez à faire des sauvegardes régulières sur un support externe déconnecté.
- Effectuez vos mises à jour.
- Sensibilisez votre entourage et vos collègues en vous appuyant sur les publications des experts.

Vous êtes victime d'un chantage à la webcam ou d'un rançongiciel : comment y faire face ?

- Ne payez jamais les rançons demandées.
- Obtenez de l'assistance auprès de Cybermalveillance.gouv.fr qui vous mettra en relation avec des professionnels à proximité.
- Déposez plainte auprès des autorités compétentes.

Pour plus d'informations, rendez-vous sur www.cybermois.fr

À PROPOS DU CYBERMOI/S

Coordonné en France par un groupe de travail national réuni autour de l'ANSSI, le Mois européen de la cybersécurité est un événement de sensibilisation organisé chaque année. En 2019, la France a lancé le « Cybermoi/ s», la déclinaison nationale du Mois européen de la cybersécurité consacrée à la protection des usages numériques.

Pendant le mois d'octobre, des activités de sensibilisation sont organisées en France et en Europe autour des enjeux de sécurité numérique (menaces, bonnes pratiques, formation en sécurité des systèmes d'information, etc.). Conférences, vidéos, campagnes de communication… De nombreux acteurs publics et associatifs se mobilisent en France pour proposer un programme de sensibilisation ambitieux et pédagogique à tous, dans la vie personnelle, comme professionnelle.

Cette mobilisation d'acteurs variés, en France et en Europe, poursuit un objectif : favoriser l'émergence d'une culture partagée de la sécurité du numérique !

CONTACTS PRESSE

ANSSI - Baptiste GRÉGOIRE / baptiste.gregoire@ssi.gouv.fr / 06 07 68 25 91 - Margaux VINCENT / margaux.vincent@ssi.gouv.fr / 06 49 21 63 80

Avec le soutien du

GOUVERNEMENT
Liberté
Égalité
Fraternité

Club des experts de la sécurité d'information et du numérique - Véronique LOQUET / vloquet@alx-communication.com

CLUSIF - Luména DULUC / lumena.duluc@clusif.fr / 06 21 04 86 02

Commission nationale de l'informatique et des libertés - Yohann BRUNET / ybrunet@cnil.fr / 01 53 73 22 13 / 06 80 71 51 25

Confédération des petites et moyennes entreprises - Anne-Victoire CHAUMET / avchaumet@cpme.fr / 01 47 62 73 31

Cybermalveillance.gouv.fr - Pôle communication / presse@cybermalveillance.gouv.fr

Fédération bancaire française - Benoit DANTON / bdanton@fbf.fr / 01 48 00 50 70 - Jenny SENSIAU / jsensiau@fbf.fr / 01 48 00 50 52

ISSA FRANCE - Laëtitia BERCHÉ / laetitia@securitytuesday.com / 06 14 48 02 95

Mouvement des entreprises de France - Anne-Charlotte GEOFFROY / ageoffroy@medef.fr / 01 53 59 18 08

Ministère de l'Éducation nationale, de la Jeunesse et des Sports - Agnès LONGUEVILLE / agnes.longueville@education.gouv.fr / 06 85 03 77 87 / 01 55 55 17 10

Ministère de l'Agriculture - Service de presse du ministère / ministere.presse@agriculture.gouv.fr / 01 49 55 60 11

Syntec Numérique - Hopscotch pour Syntec Numérique - Marlène Para / mpara@hopscotch.fr / 01 41 34 23 74 - Ghizlane Elyoussfi / gelyoussfi@hopscotch.fr / 01 41 34 21 14 - Caroline Fouquet / cfouquet@syntec-numerique.fr / 06 99 85 48 24

Avec le soutien du

GOUVERNEMENT
Liberté
Égalité
Fraternité