GOUVERNEMENT

*Liberté*
*Égalité*
*Fraternité*

## COMMUNIQUE DE PRESSE

Paris, le 04/09/2020

# RANCONGICIELS : FACE A L'AMPLEUR DE LA MENACE, L'ANSSI ET LE MINISTERE DE LA JUSTICE PUBLIENT UN GUIDE POUR SENSIBILISER LES ENTREPRISES ET LES COLLECTIVITES

Les attaques par rançongiciels connaissent une augmentation sans précédent. Depuis le début de l'année, l'ANSSI a traité 104 attaques par rançongiciels. Face à ce constat l'ANSSI, en partenariat avec la Direction des Affaires criminelles et des grâces (DACG) du ministère de la Justice, publie le guide de sensibilisation *Attaques par rançongiciels, tous concernés - Comment les anticiper et réagir en cas d'incident ?*. Le Groupe M6, le CHU de Rouen et Fleury Michon, tous trois victimes d'un rançongiciel en 2019, livrent un témoignage éclairant dans ce guide à destination des entreprises et des collectivités.

Les attaques par rançongiciels augmentent en nombre, en fréquence et en sophistication. **Depuis le 1er janvier 2020, l'ANSSI a traité 104[1] attaques par rançongiciels**. Leurs conséquences sont de plus en plus dévastatrices, sur la continuité d'activité, voire la survie de l'organisation victime.

« Les acteurs privés comme publics sont encore trop peu conscients du risque et de leur propre vulnérabilité » constate Guillaume Poupard, directeur général de l'ANSSI.

« Il est urgent pour les entreprises et les collectivités de mettre en œuvre des mesures pour prévenir les attaques par rançongiciels et d'apprendre à bien réagir lorsqu'il est trop tard » explique François Deruty, sous-directeur Opérations de l'ANSSI.

Pour faire face à cette situation inédite et dans le cadre d'une dynamique gouvernementale, l'ANSSI, en partenariat avec la DACG, publie le guide *Attaques par rançongiciels, tous concernés - Comment les anticiper et réagir en cas d'incident ?*

Ce guide de bonnes pratiques préventives et réactives face aux rançongiciels est enrichi des témoignages de trois organisations victimes : le Groupe M6, le CHU de Rouen et Fleury Michon. Très concret, il s'adresse en particulier aux dirigeantes et dirigeants, ainsi qu'aux responsables informatiques des entreprises et des collectivités.

Parmi ses recommandations, le guide présente l'importance du dépôt de plainte en cas d'attaque par rançongiciel. « Le dépôt de plainte auprès des services de police ou de gendarmerie permet l'ouverture d'une enquête qui sera supervisée par des magistrats spécialisés et à l'issue de laquelle il sera éventuellement possible de déchiffrer les données altérées. Déposer plainte peut surtout permettre

[1] Ces chiffres ne fournissent pas une vision exhaustive de l'actualité des rançongiciels affectant le territoire national. Cet état de la situation ne s'appuie que sur les faits portés à la connaissance de l'ANSSI (par ses bénéficiaires ou partenaires) et traités par elle.

d'identifier, interpeller et présenter les auteurs de l'attaque à la Justice, afin de mettre un terme au sentiment d'impunité des cyberdélinquants » explique Catherine Pignon, directrice de la DACG.

Plusieurs acteurs ont contribué à la réalisation de ce guide : le dispositif cybermalveillance.gouv.fr, la Brigade de lutte contre la cybercriminalité (BL2C), la Commission nationale de l'informatique et des libertés (CNIL) et la Direction centrale de la Police judiciaire (DCPJ).

**UNE MENACE QUI EXPLOSE ET SE REINVENTE**

Le guide s'ouvre sur un aperçu des dernières tendances observées en matière de rançongiciels. L'immense majorité des attaques est opportuniste et profite du faible niveau de maturité en sécurité numérique des organisations victimes. Depuis 2018 cependant, l'ANSSI observe une recrudescence des attaques par rançongiciels ciblant des organisations aux moyens financiers importants ou aux activités particulièrement critiques. L'importance de ces cibles fait entrer les rançongiciels dans la catégorie des attaques dites *« Big Game Hunting »*.

L'agence constate par ailleurs que certains groupes criminels associent désormais la menace de publication de données sensibles à l'utilisation de rançongiciels. Ils accentuent ainsi la pression exercée sur leurs victimes pour les amener à payer la rançon.

Alors que les montants habituels s'élèvent à plusieurs centaines ou milliers d'euros, les rançons demandées lors des attaques de type *« Big Game Hunting »* sont à la mesure des moyens financiers de la victime. Elles peuvent atteindre des sommes allant jusqu'à plusieurs millions d'euros.

Les récentes attaques par rançongiciels ciblant des entreprises clés d'un secteur et leurs sous-traitants, entraînent un risque de déstabilisation générale de l'ensemble d'un secteur.

**M6, LE CHU DE ROUEN ET FLEURY MICHON TEMOIGNENT**

Pour marquer les consciences et briser certains tabous, M6, le CHU de Rouen et Fleury Michon, tous trois victimes de rançongiciels, partagent leurs expériences et leurs conseils dans le guide. Ces différents témoignages confirment un point clé : peu importe le secteur d'activité, les cyberattaques n'épargnent personne !

« Aujourd'hui, il est important de rappeler aux organisations du secteur de la santé comme aux autres que l'on n'est pas tous seuls pour faire face à ce type de situations. Il ne faut pas hésiter à se faire assister et solliciter un avis extérieur » explique Cédric Hamelin, Responsable adjoint à la sécurité du système d'information du CHU de Rouen.

« Je n'ai pas un mais trois conseils à partager. 1) Gérer une crise cyber, c'est à la fois mettre en œuvre un plan et jouer une partition non écrite. Sur ces deux volets, rien ne se fait seuls ! 2) Rester calme (ne marche que si l'on n'est pas seuls). 3) D'un point de vue plus organisationnel enfin, cette expérience m'a conforté dans l'idée qu'un Responsable de la sécurité des systèmes d'information doit avoir un accès direct et facilité à tous les acteurs de la gestion de crise – directions et managers compris – pour préparer l'organisation à ces épreuves et y réagir le cas échéant » conseille Jérôme Lefébure, CFO, membre du directoire en charge des métiers de support du Groupe M6.

« Préparez-vous sera mon dernier conseil ! On ne peut pas s'en sortir tout seul » conclut Laurent Babin,

## Contacts presse

**ANSSI** : Margaux Vincent - margaux.vincent@ssi.gouv.fr - 06 49 21 63 80

**Cabinet du garde des Sceaux** : secretariat-presse.cab@justice.gouv.fr - 01 44 77 63 15

Responsable de la sécurité du système d'information de Fleury Michon.

**LES BONNES PRATIQUES DE SECURITE NUMERIQUE**

Le guide propose des mesures préventives issues du Guide d'hygiène informatique de l'ANSSI. Les appliquer permet d'éviter qu'un rançongiciel n'atteigne l'organisation ou, a minima, de réduire les pertes liées à une telle attaque.

**Les conseils de l'ANSSI pour réduire le risque d'attaque par rançongiciels**

- Sauvegarder les données
- Maintenir à jour les logiciels et systèmes
- Utiliser et maintenir à jour les logiciels antivirus
- Cloisonner le système d'information
- Limiter les droits des utilisateurs et autorisations des applications
- Maîtriser les accès Internet
- Mettre en œuvre une supervision des journaux
- Sensibiliser les collaborateurs
- Évaluer l'opportunité de souscrire à une assurance cyber
- Mettre en œuvre un plan de réponse aux cyberattaques
- Penser sa stratégie de communication de crise cyber

Le guide présente également les mesures à adopter pour bien réagir face à une attaque par rançongiciel. Les premières actions techniques proposées, quand elles sont mises en œuvre rapidement, permettent de réduire les pertes liées à une telle attaque.

**Les conseils de l'ANSSI pour bien réagir en cas d'attaque**

- Adopter les bons réflexes
- Piloter la gestion de la crise cyber
- Trouver de l'assistance technique
- Communiquer au juste niveau
- Ne pas payer la rançon
- Déposer plainte
- Restaurer les systèmes depuis des sources saines

En réunissant témoignages de victimes et bonnes pratiques de sécurité numérique, ce guide donne un coup de projecteur sur les rançongiciels et invite les organisations – du comité exécutif aux collaborateurs – à se saisir de ces questions.

Le guide *Attaques par rançongiciels, tous concernés - Comment les anticiper et réagir en cas d'incident?* est disponible sur le site de l'ANSSI : https://www.ssi.gouv.fr/publication/rancongiciels-face-a-lampleur-de-la-menace-lanssi-et-le-ministere-de-la-justice-publient-un-guide-pour-sensibiliser-les-entreprises-et-les-collectivites/

## Contacts presse

**ANSSI** : Margaux Vincent - margaux.vincent@ssi.gouv.fr - 06 49 21 63 80

**Cabinet du garde des Sceaux** : secretariat-presse.cab@justice.gouv.fr - 01 44 77 63 15

**À PROPOS DE L'ANSSI**
L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a été créée par le décret n°2009-834 du 7 juillet 2009 sous la forme d'un service à compétence nationale.
L'agence assure la mission d'autorité nationale en matière de défense et sécurité des systèmes d'information. Elle est rattachée au secrétaire général de la défense et de la sécurité nationale, sous l'autorité du Premier ministre.

www.ssi.gouv.fr - communication@ssi.gouv.fr

**À PROPOS DE LA DACG**
La direction des affaires criminelles et des grâces constitue la direction de la norme et de la justice pénales du ministère de la Justice. La DACG travaille à tous les projets législatifs ou réglementaires en matière répressive portés par le ministère de la Justice ou d'autres ministères.

## Contacts presse

**ANSSI** : Margaux Vincent - margaux.vincent@ssi.gouv.fr - 06 49 21 63 80

**Cabinet du garde des Sceaux** : secretariat-presse.cab@justice.gouv.fr - 01 44 77 63 15