

# Ransomwares : les USA structurent leur réponse

Dix millions de dollars. C'est la somme que Washington est [prêt](#) à donner en échange d'informations sur certains actes de cybermalveillance. En l'occurrence, ceux qui cibleraient des infrastructures critiques, en violation du Computer Fraud and Abuse Act. En première ligne, les *ransomwares*. Qui font d'ailleurs l'objet d'[autres mesures](#) annoncées en parallèle de cette dotation financière.

*Rewards Up To \$10 Million!*

*For information on foreign malicious [#cyber](#) operations targeting U.S. critical infrastructure.*

*Submit info on these illegal activities via Tor at <https://t.co/Wvkl416g4W>*

*You may be eligible for a reward. [pic.twitter.com/BjftNvC5bc](https://pic.twitter.com/BjftNvC5bc)*

*— Rewards for Justice (@RFJ\_USA) [July 15, 2021](#)*

Parmi ces autres mesures, il y a la mise en ligne d'un [site](#) « Stop Ransomware ». Y sont centralisées des ressources issues de diverses agences gouvernementales. En tête desquelles la CISA, homologue de notre ANSSI. Il y a aussi une réunion « spéciale *ransomwares* » – à venir [en août](#) – du FinCEN (Financial Crimes Enforcement Network). Ce sera la deuxième sur cette thématique pour le groupe de lutte contre le blanchiment.

Pour ce qui est de la transmission d'informations, elle se fait au travers d'un SecureDrop hébergé sur un [site Tor](#). Les éventuelles primes seront accordées dans le cadre du programme « Rewards for Justice », déjà mis à contribution pour la lutte contre le trafic de drogue et le terrorisme.



## First submission

First time submitting to our SecureDrop? Start here.

GET STARTED

## Return visit

Already have a codename? Check for replies or submit something new.

LOG IN

Ces initiatives, on les doit essentiellement à l'[attaque](#) contre Colonial Pipeline. L'incident, survenu en mai, a en tout cas joué un rôle de déclencheur pour les démarches « anti-ransomwares » de l'administration U.S. Il a notamment donné lieu à la création d'un groupe de travail interagences (Trésor, DHS, renseignement). Ou encore à l'élaboration – en cours – d'un [guide de référence](#) fondé sur le *framework* cybersécurité du NIST.

Photo d'illustration © Rawpixel.com – Adobe Stock