Le Monde.fr

URL :http://www.lemonde.fr/
PAYS : France
TYPE : Web Grand Public

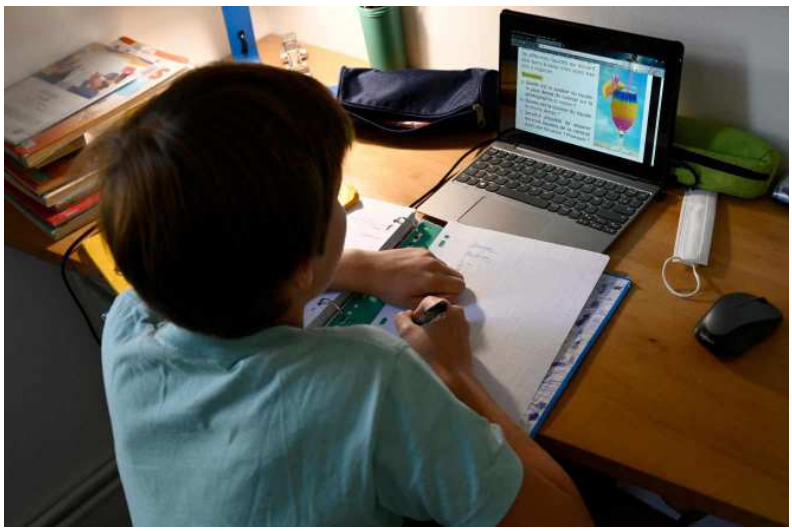
► **8 avril 2021 - 10:14**

> Version en ligne

Ecole à la maison : le CNED a-t-il été victime d'une attaque informatique « venue de l'étranger » ?

- Pixels
- Sécurité informatique

Une enquête judiciaire a été confiée à la police nationale et une information judiciaire ouverte par le parquet de Paris, alors que le CNED a dénoncé des attaques par déni de service contre ses systèmes.



Ecole à distance, à Marseille, le 6 avril 2021. Il y a un an, une enquête avait également été ouverte, dans des circonstances similaires, après les perturbations qui avaient entaché la mise en place de l'enseignement à distance. NICOLAS TUCAT / AFP

La reprise des cours à la maison, mardi 6 avril, à la suite des nouvelles mesures sanitaires prises contre la Covid-19, s'est faite avec difficulté, en raison de nombreuses défaillances techniques. Dans la foulée, le ministère de l'éducation a dénoncé des cyberattaques contre les services du Centre national d'enseignement à distance (CNED), rendant l'accès à certains outils difficile, voire impossible.

• Est-ce bien une attaque ?

A ce stade, le CNED a dénoncé des *« actes délibérés de malveillance »* et la justice s'est saisie du dossier. La section « cyber » du parquet de Paris a annoncé, mercredi 7 avril, l'ouverture d'une information judiciaire des chefs *« d'accès frauduleux à un système de traitement automatisé »* et *« d'entrave au fonctionnement »* de ce système. Il s'agit des dénominations classiques utilisées dans le cadre d'une enquête sur une intrusion informatique ou une attaque par déni de service. Cette enquête a été confiée à l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLTIC), une cellule de la police nationale. Les investigations devront pouvoir démontrer si une attaque a bien touché les services du CNED et donner une estimation de son ampleur.

Il y a un an, une enquête avait également été ouverte, dans des circonstances similaires, après les perturbations qui avaient entaché la mise en place de

Le Monde.fr
URL :http://www.lemonde.fr/
PAYS : France
TYPE : Web Grand Public

► **8 avril 2021 - 10:14** **> Version en ligne**

l'enseignement à distance et que le ministère avait, en partie, attribuées à une attaque informatique.
Lire aussi Ecole à la maison : ouverture d'une enquête après des « actes délibérés de malveillance » contre la plate-forme du CNED

- **De quel type d'attaque s'agit-il ? Est-ce compliqué à mettre en œuvre ?**

Le CNED a estimé mardi que ses services avaient été victimes d'une attaque par déni de service (Ddos, pour Distributed Denial of Service Attack). Il s'agit, en gros, de bombarder un ou plusieurs sites de connexions, souvent à l'aide d'un grand nombre de machines, pour saturer les serveurs et les mettre à genoux. Les Ddos sont vieux comme l'informatique en réseau, et il existe une myriade de logiciels plus ou moins évolués, mais aussi de services payants, permettant d'organiser de telles attaques, parfois même sans avoir de compétences techniques particulières.

- **Une attaque peut-elle expliquer l'ensemble des perturbations rencontrées ce mardi par les services d'enseignement à distance ?**

Seul le CNED a, d'après le ministère de l'éducation nationale, été visé par ces *« actes de malveillance »* –, les autres services (environnements numériques de travail…) perturbés en ce début de semaine ont surtout été victimes de l'afflux d'utilisateurs. Les syndicats d'enseignants ont largement dénoncé une *« impréparation »* face à une arrivée massive d'utilisateurs pourtant très prévisible.
Lire les témoignages : « On a beau vouloir s'adapter, les outils ne fonctionnent pas » : débuts chaotiques pour la reprise des cours à distance

Par ailleurs, une attaque de déni de service est d'autant plus efficace que sa cible est déjà soumise à une forte sollicitation, comme c'était le cas, ce mardi, pour les services en ligne du CNED.

- **Peut-on faire la différence entre une attaque qui vient de l'étranger et une attaque depuis la France ?**

Oui et non. Il est relativement facile de voir d'où proviennent les connexions qui saturent un service ou un site, mais ces connexions *« parasites »* ne proviennent en général pas directement de l'assaillant. Schématiquement, un commanditaire situé en France peut très facilement avoir recours à un service ou à un logiciel *« clés en main »* qui utilisera des machines situées en Russie, aux Etats-Unis ou dans tout autre pays. L'attaque peut donc très bien *« venir de l'étranger »* , comme l'a affirmé ce mercredi Jean-Michel Blanquer, mais n'avoir rien à voir avec une attaque étatique et même avoir un commanditaire français.

Il est très possible qu'on ne sache jamais précisément d'où provenait l'attaque. Dans la plupart des cas, les commanditaires d'attaques par déni de service ont recours à des services tiers, payés en cryptomonnaies, et leur trace est très difficile à remonter.

Parfois, le démantèlement de groupes cybercriminels spécialisés, ou la coupure de réseaux de machines utilisées pour des opérations de ce type, permet de découvrir, longtemps après, l'identité probable des commanditaires d'attaques, mais c'est rare.
Lire aussi L'école à la maison reprend, mais « des dysfonctionnements et des défaillances » empêchent élèves et professeurs de travailler

Le Monde
Contribuer

Le Monde.fr

URL :http://www.lemonde.fr/
PAYS : France
TYPE : Web Grand Public

► **8 avril 2021 - 10:14**

> Version en ligne

Services

téléphone ou tablette).

- Comment ne plus voir ce message ?

  Si vous utilisez ce compte à plusieurs, passez à une offre multicomptes pour faire profiter vos proches de votre abonnement avec leur propre compte. Sinon, cliquez sur « » et assurez-vous que vous êtes la seule personne à consulter Le Monde avec ce compte.

- Vous ignorez qui d'autre utilise ce compte ?

  Nous vous conseillons de modifier votre mot de passe .

- Que se passera-t-il si vous continuez à lire ici ?

  Ce message s'affichera sur l'autre appareil. Ce dernier restera connecté avec ce compte.

- Y a-t-il d'autres limites ?

  Non. Vous pouvez vous connecter avec votre compte sur autant d'appareils que vous le souhaitez, mais en les utilisant à des moments différents.