

[Home](#) / [Sécurité](#) / Sécurité en ligne

Sécurité en ligne

Recherche sur Internet

914



dossiers

En matière d'appui, les enquêteurs "Internet" de la cellule i2-IRU de la Police Fédérale ont apporté leur aide dans 914 dossiers en 2018, ce qui représente une moyenne de 75 missions par mois.

L'appui le plus régulièrement fourni concerne le terrorisme. Par exemple, sous la coordination du Parquet fédéral, i2-IRU a collaboré avec des services d'enquête (inter)nationaux à la saisie de serveurs utilisés par l'État Islamique. La cellule est également active dans le signalement, en vue d'un retrait, de contenus ayant trait à la propagande, au terrorisme, au radicalisme, à l'extrémisme violent et au discours de haine. En 2018, 1 621 contenus à caractère terroriste ont ainsi été signalés. 1 193 ont fait l'objet d'un retrait. 129 contenus en matière de discours de haine ont par ailleurs été référencés et 77 ont pu être effacés. Les autres n'ont pu être retirés par les plateformes.

Un autre phénomène faisant l'objet de nombreuses demandes d'appui est la criminalité en matière d'abus sexuels sur mineurs. L'an dernier, la cellule a réceptionné 494 profils, dont 163 sont toujours en cours de recherche d'identification. 191 identifications ont été effectuées et ont fait l'objet d'un procès-verbal. La différence, soit 140 profils, correspond à des non identifiés ou non identifiables (par exemple, des profils qui n'existent plus ou qui ont été clôturés).

Précisons que les signalements aux plateformes, en vue de solliciter le retrait d'un contenu, ne sont pas des réquisitions judiciaires. Les plateformes sont donc libres de retirer ou non les contenus signalés.

Enfin, en matière de blocage de sites et/ou de contenus, la cellule i2-IRU a réceptionné 33 réquisitoires visant 67 adresses. La large majorité des demandes sont à mettre en lien avec la vente illégale de tickets événementiels en ligne.

Cybercriminalité

La Police Fédérale surveille le cyberspace pour détecter de nouvelles formes d'arnaques. Dans le cadre de la prévention, des alertes ont été lancées dans les médias, notamment par le biais de l'émission "Surfons tranquille" (RTBF). Ces alertes ont suscité beaucoup d'intérêt public. Une alerte concernant une campagne de *phishing* visant une banque belge a, par exemple, été lue par 180 125 personnes en 24 heures et partagée maintes fois.

Phishing* et ransomware** en 2018

1478



sites supprimés du web pour cause de phishing***

171



procès-verbaux pour ransomwares****

* **Phishing** : les criminels qui ont recours à cette forme d'escroquerie extorquent de l'argent à des personnes qui ne se doutent de rien, par le biais d'e-mails ou de sites web frauduleux imitant des sites réels, comme par exemple celui d'une institution bancaire.

** **Ransomware** : virus qui est installé sur un appareil sans que le propriétaire n'en ait donné l'autorisation. Le virus tient l'appareil en otage et les fichiers sont cryptés jusqu'à l'obtention d'une rançon.

*** Contre 648 522 déclarations via le site Safeonweb.be du Centre de cybersécurité Belgique (CCB).

**** Contre 437 déclarations au point de contact du Service public fédéral (SPF) Économie.

Les chiffres de la cybercriminalité sont très relatifs, car la population a tendance à peu déclarer les faits. Les victimes de cybercriminalité ne se tournent pas souvent vers la police pour déposer plainte. En 2018, les services de police ont enregistré 24 582 faits. Lors de l'enquête pour le Moniteur de sécurité, 8 % de la population ont indiqué avoir été victimes d'« escroquerie sur Internet »

au moins une fois sur l'année écoulée. Seule une personne concernée sur cinq a déclaré les faits. Il existe donc un important *dark number*.



Police Fédérale

✉ federal.contactcenter@police.belgium.eu

🌐 www.policefederale.be

Archives

[Rapport annuel 2017](#)

[Rapport annuel 2016](#)

Choix des langues

[Nederlands](#)

[Français](#)

Copyright ©2019 | Designed by [Police Fédérale](#)

