

# ATTAQUE « OLYMPIC DESTROYER » CONTRE LES JEUX OLYMPIQUES D'HIVER DE PYEONGCHANG

Le 9 février 2018, le logiciel malveillant Olympic Destroyer a attaqué les systèmes informatiques des Jeux olympiques d'hiver de PyeongChang pendant la cérémonie d'ouverture. Un acte d'accusation américain met en cause des officiers de l'unité 74455 du GRU (Sandworm) pour cette attaque. Le même acte d'accusation porte sur des opérations de piratage et de divulgation visant l'élection présidentielle française de 2017 et sur des attaques en Géorgie.

UKRAINE EVIDENCE HUB  
AU-DELÀ DE L'UKRAINE  
AU 15 OCT. 2026

## DEGRÉ DE PREUVE

### ATTRIBUTION OFFICIELLE

Un gouvernement, un procureur, l'UE, l'OTAN ou un organe de l'ONU a formellement désigné la Russie, ses services ou ses forces soutenues par l'État. Il s'agit d'une position de cette autorité, non d'un jugement.

## QUI L'A ÉTABLI

Acte d'accusation d'un grand jury fédéral américain contre six officiers de l'unité 74455 du GRU (rendu le 15 oct. 2020, annoncé le 19 oct. 2020). Le NCSC britannique a publié une attribution parallèle le même jour.

## DERNIÈRES NOUVELLES

L'acte d'accusation reste pendant et aucun accusé n'est détenu.

## LIEN AVEC LA GUERRE CONTRE L'UKRAINE

La même unité du GRU est mise en cause pour des attaques contre le réseau électrique ukrainien et pour NotPetya.

## SOURCES

**B** Département de la Justice des États-Unis – Six officiers du GRU russe inculpés · 2020-10-19

<https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and>

**B** GOV.UK : Le Royaume-Uni dévoile une série de cyberattaques russes contre les Jeux olympiques et paralympiques · 2020-10-19

<https://www.gov.uk/government/news/uk-exposes-series-of-russian-cyber-attacks-against-olympic-and-paralympic-games>

## CE QUE NOUS DEMANDONS DES ÉTATS MEMBRES

- Attribuer conjointement et porter la question devant le Groupe de travail à composition non limitée des Nations Unies sur la sécurité du numérique.
- Appliquer le régime de sanctions cyber de l'UE aux unités responsables.
- Partager les indicateurs et renforcer la résilience des infrastructures critiques.

Le statut suit quatre degrés de preuve : décision de justice · attribution officielle · mis en accusation · soupçonné (les cas soupçonnés ne figurent que sur la page en ligne). Niveau A = juridictions, organes de l'ONU, organisations internationales · B = gouvernements, parquets · C = médias et enquêteurs. Rectificatifs : [evidence@ukraine-evidence.org](mailto:evidence@ukraine-evidence.org)



page en ligne ·  
rectificatifs