

LE LOGICIEL MALVEILLANT DESTRUCTEUR NOTPETYA SE PROPAGE DANS LE MONDE ENTIER

Le logiciel malveillant effaceur NotPetya a été lancé le 27 juin 2017 par l'intermédiaire d'un logiciel de comptabilité ukrainien et s'est propagé dans le monde entier. Des entreprises en Europe, aux États-Unis et ailleurs ont subi de lourdes pertes. Le point sur la carte indique Copenhague, siège de Maersk, l'une des entreprises les plus touchées, et n'a qu'une valeur illustrative.

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

Attribution à l'armée russe par le Foreign Office britannique (15 févr. 2018), avec des déclarations des États-Unis et des alliés. Les sanctions du Conseil de l'UE du 30 juillet 2020 (règlement d'exécution (UE) 2020/1125) ont visé le Centre principal des technologies spéciales du GRU (GTsST, « Sandworm »). Acte d'accusation américain contre six officiers de l'unité 74455 du GRU (15 oct. 2020).

DERNIÈRES NOUVELLES

Les inscriptions au titre des sanctions cyber de l'UE restent en vigueur. L'acte d'accusation américain reste pendant et aucun accusé n'est détenu.

LIEN AVEC LA GUERRE CONTRE L'UKRAINE

L'attaque a commencé en Ukraine et visait principalement l'Ukraine avant de se propager dans le monde entier.

SOURCES

A EUR-Lex – Règlement d'exécution (UE) 2020/1125 du Conseil du 30 juillet 2020 (sanctions relatives aux cyberattaques) · 2020-07-30

https://eur-lex.europa.eu/eli/reg_impl/2020/1125/oj/eng

B Département de la Justice des États-Unis – Six officiers du GRU russe inculpés pour le déploiement mondial de logiciels malveillants destructeurs · 2020-10-19

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

C MIT Technology Review – Le Royaume-Uni affirme que la Russie est à l'origine de la vaste attaque par rançongiciel NotPetya · 2018-02-15

<https://www.technologyreview.com/2018/02/15/241258/the-uk-says-russia-was-behind-the-huge-notpetya-ransomware-attack/>

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



page en ligne ·
rectificatifs