

NOTPETYA DESTRUCTIVE MALWARE SPREADS WORLDWIDE

NotPetya wiper malware was launched on 27 June 2017 through Ukrainian accounting software and spread worldwide. Companies across Europe, the US and elsewhere suffered heavy losses. The map point marks Copenhagen, home of Maersk, one of the most affected firms, and is illustrative only.

UKRAINE EVIDENCE HUB
BEYOND UKRAINE
AS OF 15 OCT 2026

DEGREE OF PROOF

OFFICIAL ATTRIBUTION

A government, a prosecutor, the EU, NATO or a UN body has formally named Russia, its services or its state-backed forces. This is a position of that authority, not a verdict.

WHO ESTABLISHED IT

UK Foreign Office attribution to the Russian military (15 Feb 2018), with US and allied statements. EU Council sanctions of 30 July 2020 (Implementing Regulation (EU) 2020/1125) listed GRU's Main Centre for Special Technologies (GTsST, 'Sandworm'). US indictment of six GRU Unit 74455 officers (15 Oct 2020).

LATEST

EU cyber sanctions listings remain in force. The US indictment is outstanding, and no defendant is in custody.

LINK TO THE WAR AGAINST UKRAINE

The attack started in Ukraine and was aimed mainly at Ukraine before spreading worldwide.

SOURCES

A EUR-Lex – Council Implementing Regulation (EU) 2020/1125 of 30 July 2020 (cyber-attacks sanctions) · 2020-07-30

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

B US Department of Justice – Six Russian GRU officers charged in connection with worldwide deployment of destructive malware · 2020-10-19

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

C MIT Technology Review – The UK says Russia was behind the huge NotPetya ransomware attack · 2018-02-15

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

WHAT WE ASK OF MEMBER STATES

- Attribute jointly and raise it in the UN Open-ended Working Group on ICT security.
- Use the EU cyber sanctions regime against the units responsible.
- Share indicators and support the resilience of critical infrastructure.

Status follows four degrees of proof: court finding · official attribution · charged · suspected (suspected cases are listed only on the live page). Tier A = courts, UN bodies, international organisations · B = governments, prosecutors · C = media and investigators. Corrections: evidence@ukraine-evidence.org



live page · corrections