

EL PROGRAMA MALIGNO DESTRUCTIVO NOTPETYA SE PROPAGA POR TODO EL MUNDO

El programa maligno de borrado NotPetya se lanzó el 27 de junio de 2017 a través de un programa informático de contabilidad ucraniano y se propagó por todo el mundo. Empresas de toda Europa, los Estados Unidos y otros lugares sufrieron grandes pérdidas. El punto del mapa señala Copenhague, sede de Maersk, una de las empresas más afectadas, y tiene carácter meramente ilustrativo.

UKRAINE EVIDENCE HUB
MÁS ALLÁ DE UCRANIA
A 15 OCT 2026

GRADO DE PRUEBA

ATRIBUCIÓN OFICIAL

Un Gobierno, una fiscalía, la UE, la OTAN o un órgano de las Naciones Unidas ha señalado formalmente a Rusia, a sus servicios o a sus fuerzas respaldadas por el Estado. Se trata de una posición de esa autoridad, no de una sentencia.

QUIÉN LO ESTABLECIÓ

Atribución del Ministerio de Relaciones Exteriores del Reino Unido al ejército ruso (15 feb 2018), con declaraciones de los Estados Unidos y de aliados. Las sanciones del Consejo de la UE de 30 de julio de 2020 (Reglamento de Ejecución (UE) 2020/1125) incluyeron al Centro Principal de Tecnologías Especiales del GRU (GTsST, «Sandworm»). Escrito de acusación de los Estados Unidos contra seis oficiales de la Unidad 74455 del GRU (15 oct 2020).

LO MÁS RECIENTE

Las inclusiones en las sanciones cibernéticas de la UE siguen en vigor. El escrito de acusación de los Estados Unidos sigue pendiente y ninguno de los acusados está detenido.

VÍNCULO CON LA GUERRA CONTRA UCRANIA

El ataque comenzó en Ucrania y estaba dirigido principalmente contra Ucrania antes de propagarse por todo el mundo.

FUENTES

A EUR-Lex – Reglamento de Ejecución (UE) 2020/1125 del Consejo, de 30 de julio de 2020 (sanciones por ciberataques) · 2020-07-30

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

B Departamento de Justicia de EE. UU. – Imputados seis oficiales del GRU ruso en relación con el despliegue mundial de malware destructivo · 2020-10-19

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

C MIT Technology Review – El Reino Unido afirma que Rusia estuvo detrás del enorme ataque de ransomware NotPetya · 2018-02-15

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

QUÉ PEDIMOS

A LOS ESTADOS MIEMBROS

- Atribuir conjuntamente y plantearlo en el Grupo de Trabajo de Composición Abierta de las Naciones Unidas sobre seguridad de las TIC.
- Aplicar el régimen de sanciones cibernéticas de la UE a las unidades responsables.
- Compartir indicadores y apoyar la resiliencia de las infraestructuras críticas.

El estado sigue cuatro grados de prueba: decisión judicial · atribución oficial · imputados · sospecha (los casos sospechosos solo figuran en la página en línea). Nivel A = tribunales, órganos de la ONU, organizaciones internacionales · B = gobiernos, fiscalías · C = medios e investigadores. Correcciones: evidence@ukraine-evidence.org



página en línea ·
correcciones