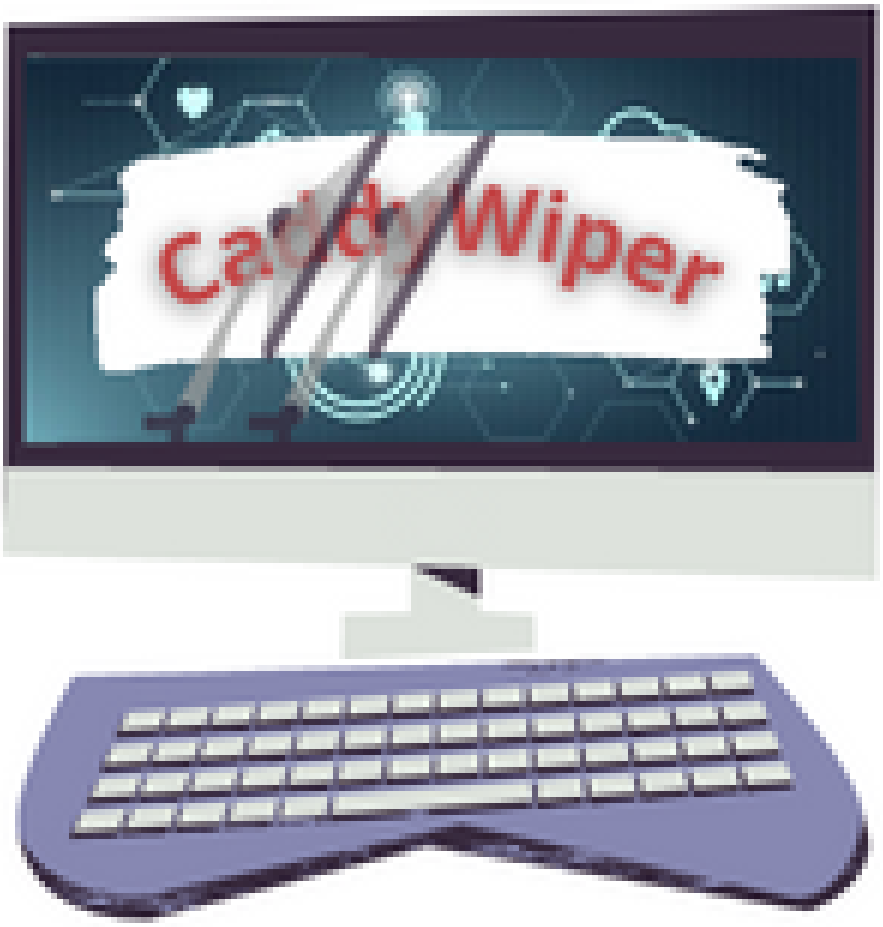


¿QUÈ ES CADDYWIPER?

¿Qué es CADDYWIPER?

La herramienta borra no solo los datos del usuario, sino también la información de partición de cualquier unidad que haya tenido la mala suerte de estar conectada a una máquina afectada.

- Funciona al corromper archivos en una máquina y sobrescribirlos con caracteres de bytes nulos, perdiendo los datos del usuario para siempre en el proceso.
- A diferencia de un malware Ransomware, un malware de limpieza se usa para eliminar permanentemente los datos de una PC afectada.
- Es un enfoque más directamente destructivo y no tiene nada que ver con extraer dinero de las víctimas.
- No presenta similitudes en el código importantes en comparación con HermeticWiper o IsaacWiper, los otros dos nuevos Wipers de datos que han afectado a organizaciones en Ucrania desde el 23 de febrero.

HermeticWiper

Funciona corrompiendo primero el Registro de arranque maestro (**MBR**) de cada unidad física.

El **MBR** es un sector de arranque al principio del almacenamiento de disco duro particionado que contiene información sobre cómo se organizan el sistema de archivos y las particiones en el disco en particular.

HermeticWizard

Un gusano personalizado utilizado para propagar HermeticWiper dentro de las redes locales.

HermeticRansom

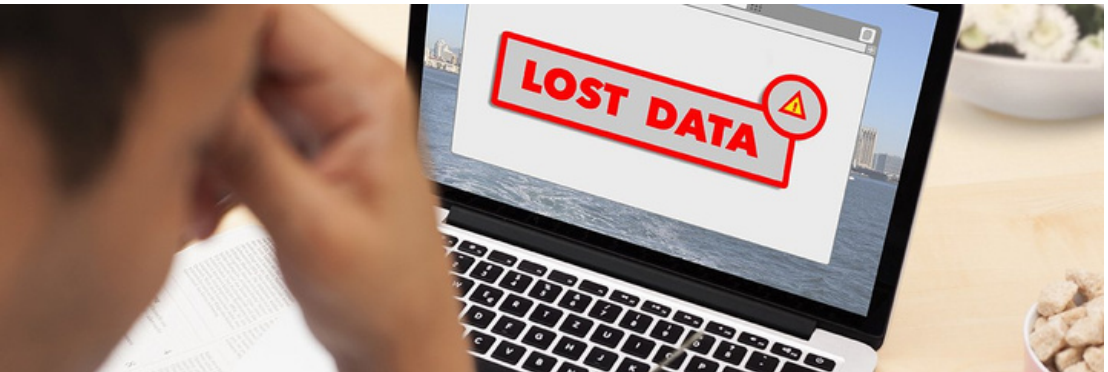
Un ransomware utilizado como señuelo.

WhisperGate

Se detectó el 13 de enero de 2022.

Este malware se lanzó explícitamente contra varias organizaciones ucranianas en ataques con motivos geopolíticos.

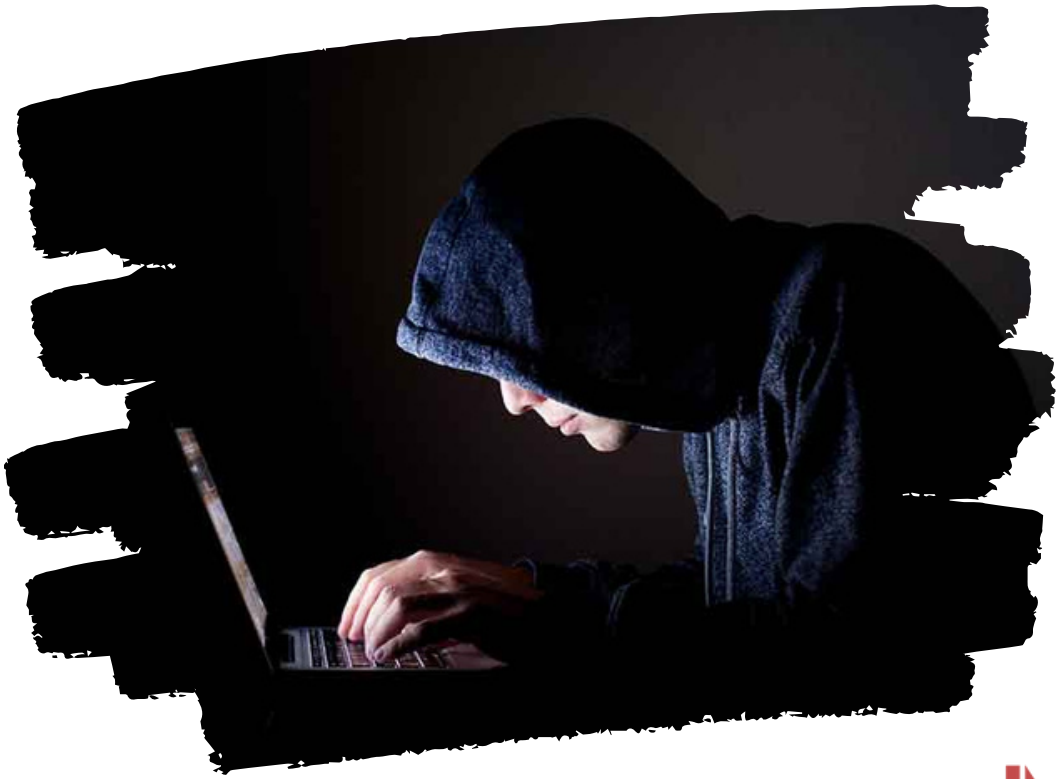
Es un malware diseñado para parecer un Ransomware, pero cuya intención es realmente provocar daños irreparables.



IMG

ACID RAIN

- El jueves 24 de febrero de 2022, un ciberataque dejó inoperables los módems Viasat KASAT en Ucrania.
- Los efectos secundarios de este ataque hicieron que 5.800 aerogeneradores de Enercon en Alemania no pudieran comunicarse para monitoreo o control remoto.
- La declaración de Viasat del miércoles 30 de marzo de 2022 proporciona una descripción algo plausible pero incompleta del ataque.
- Los investigadores de SentinelLabs descubrieron un nuevo malware que llamamos 'Acid Rain'.
- **Acid Rain es un malware ELF MIPS diseñado para borrar módems y enrutadores.**
- Acid Rain es el **séptimo malware de limpieza asociado con la invasión rusa de Ucrania.**



DOUBLEZERO

- Es un malware tipo Wiper de limpieza de datos que destruye archivos, claves de registro y árboles en la máquina Victima.
- El 17 de marzo de 2022, el equipo de respuesta a emergencias informáticas de Ucrania descubrió un malware denominado "DoubleZero" dirigido a empresas ucranianas durante la invasión rusa de Ucrania.
- Este malware fue escrito en lenguaje de programación .net.

PARA MÁS INFORMACIÓN CONTÁCTANOS EN NUESTRAS REDES SOCIALES

IMAGENTI

info@imagenti.mx

Tel. 55 55 12 73 37