Entelgy Innotec
SECURITY

GULOADER

Un malware precavido.

¿Qué es GuLoader?

GuLoader es un protector de ejecutables usado por muchas familias de malware para su distribución y ofuscación.

Fue detectado por primera vez en 2019 y nació con el nombre de DarkEye, empezándose a comercializar en la DarkNet. Actualmente se puede adquirir a través del sitio web https://www.securitycode.eu/ comprando el producto con nombre CloudEye Protector.

¿Cómo funciona?

GuLoader suele ser distribuido a través de campañas de Phishing con el propósito de descargar y ejecutar otras familias tipo Stealer o RAT (herramientas de acceso remoto), como pueden ser FormBook, Remcos o AgentTesla, entre otros.

El objetivo final es robar información confidencial y llevar a cabo otras acciones que generen ingresos a los ciberdelincuentes.

¿Qué sistemas infecta?

Afecta a sistemas Windows a través de ataques de Phishing.

¿Cómo protegerse?

La principal medida es la prevención y disponer de una solución de seguridad para el endpoint, como puede ser un antivirus o un EDR (Endpoint Detection and Response).