Entelgy Innotec
SECURITY

DRIDEX

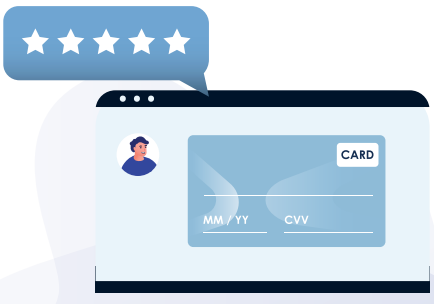
El troyano que roba claves de acceso y distribuye otras familias de malware.

¿Qué es Dridex?

Dridex es un troyano que apareció en 2014 como resultado de la evolución de Cridex, otro malware que se basa en el código fuente de la familia Zeus.

Desde entonces, debido a su constante desarrollo y complejidad, ha estado activo. Se calcula que este troyano ha afectado al 4 % de las empresas españolas.

¿Cómo funciona?



Su principal funcionalidad es robar claves de acceso a aplicaciones de banca online, aprovechando el momento en que accede un usuario, mediante técnicas como la inyección de scripts maliciosos.

Sin embargo, su alcance no se queda ahí, pues incluye otros módulos para realizar actividades fraudulentas, como *keylogger*, VNC o proxy SOCKS, además de servir para la distribución de otras familias de *malware*.

¿Qué sistema infecta?

Principalmente afecta a sistemas Windows a través de ataques de phishing.

¿Quién está detrás?

Su desarrollo se atribuye al grupo cibercriminal ruso autodenominado como "*Evil Corp*", el cual se estima que ha podido generar más de 100 millones de dólares con sus actividades.

¿Cómo protegerse?

La principal medida es la prevención y disponer de un antivirus y, aún mejor, de una solución EDR (Endpoint Protection Platform). Dado que se trata de campañas de spam, para evitar ser infectado es imprescindible no interactuar con el correo en caso de sospecha. En ningún caso se deberá abrir los enlaces que incluye ni descargar o abrir los archivos adjuntos.