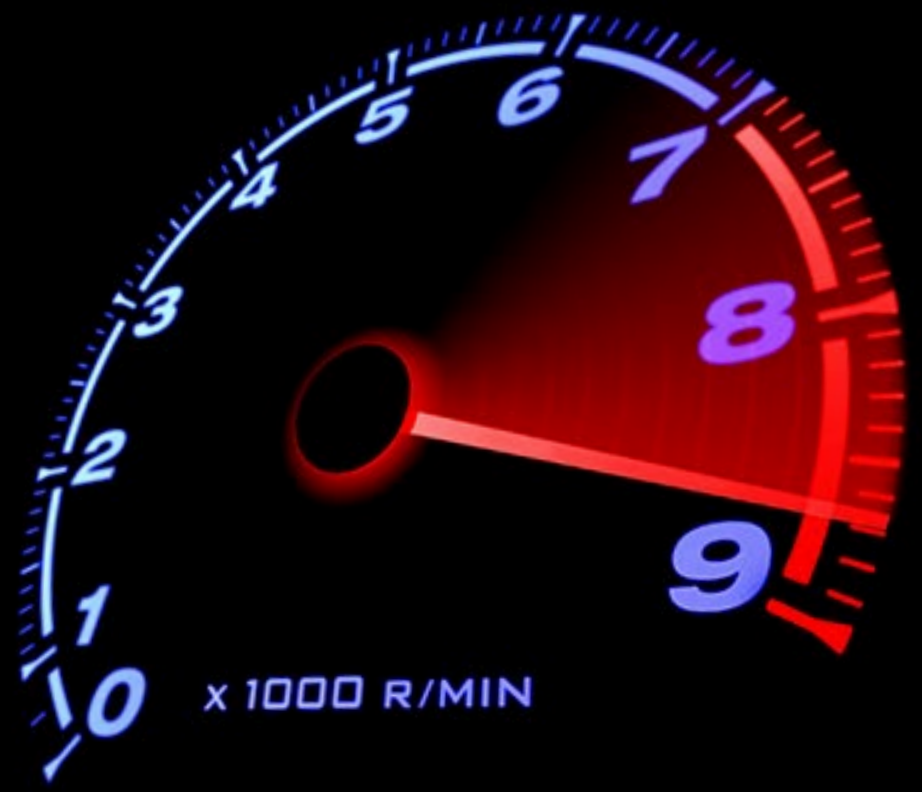
Marsh

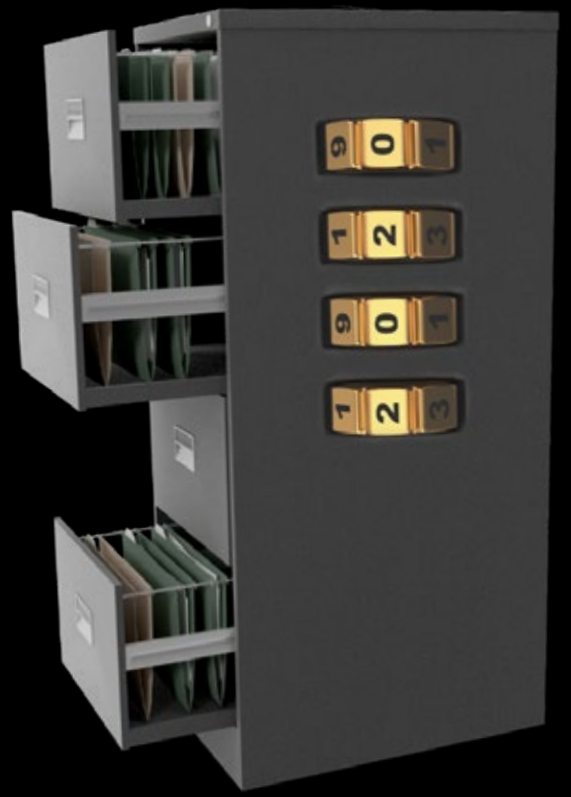
Principales tipos de Ransomware y su velocidad



Lockbit

1

Activo desde 2019



Principales caractéristicas

- Habilitado con capacidades de evasión de herramientas de seguridad.
- Velocidad de cifrado extremadamente rápida.
- Algunos benchmarks refieren que este Ransomware es capaz de cifrar 100GB de información en tan solo 4 minutos.

Modelo de Extorsión

A la víctima le pueden pedir que compre su información sensible

Además de pagar el rescate exigido para descifrar los sistemas

Versión 3.0

Reglas de los afiliados

- Prohíben el cifrado de archivos de ciertas industrias consideradas como críticas
- Sí se permite la extorsión por el robo de información a través de su portal.

¿Por qué se destaca?

- Integrar mejoras continuas en su plataforma de ataque.
- En Junio de 2022 se presentó LockBit 3.0, que guarda algunas similitudes con el Ransomware BlackMatter.
- La última versión incorpora funciones avanzadas de anti-análisis.
- Es una amenaza tanto para sistemas Windows, Linux y Mac.

BlackCat / ALPHV

2

Observado por primera vez a finales de 2021

Principales caractéristicas

- Emplea una plataforma Ransomware as a Service.
- Es capaz de desactivar las herramientas de seguridad.
- Eludir los análisis.

Se cree que es el primer grupo de Ransomware

Utiliza RUST, un lenguaje de programación seguro que ofrece un rendimiento excepcional para el procesamiento concurrente.

El Ransomware también utiliza secuencias de comandos de Windows para desplegar la carga útil y comprometer otros hosts.

50GB

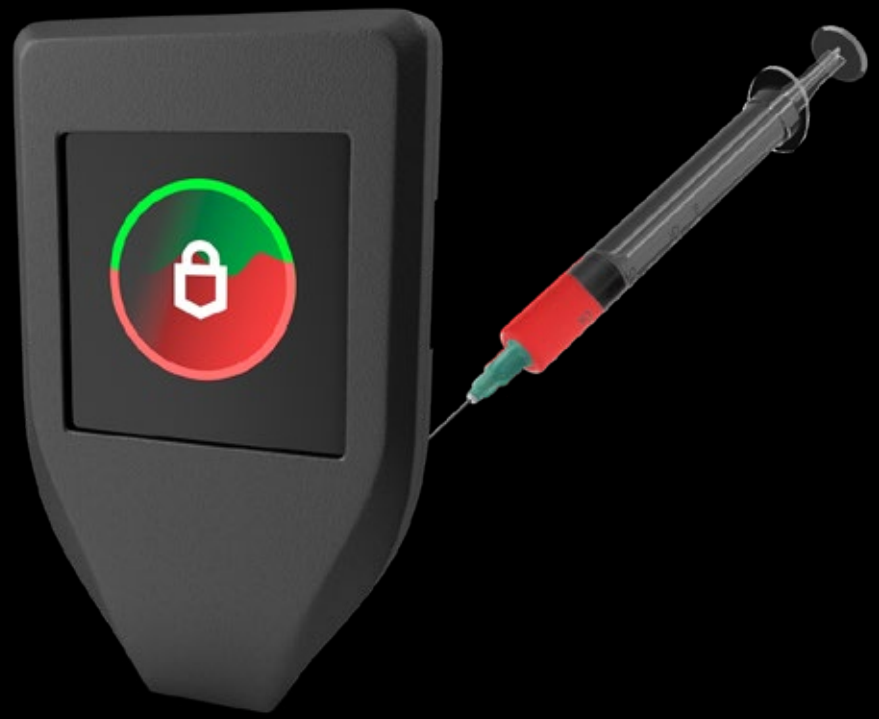
Según algunos benchmarks

Este Malware podría cifrar en menos de 2 minutos.

Black Basta

3

Surgió a principios de 2022



Principales caractéristicas

- Es un actor de Ransomware as a Service.
- Se considerá por algunos investigadores un resurgimiento de los grupos de ataque Conti y REvil.

Puede infectar sistemas

Windows | Linux

Aprovechando vulnerabilidades en **VMware ESXi** que se ejecuta en servidores empresariales

Utiliza

- ChaCha20
- RSA-4096

Para cifrar rápidamente la red

En algunos casos

- Aprovecha cepas de Malware como **Qakbot y Exploits** como **PrintNightmare** durante el proceso de infección.