

Se Conoce Nueva Versión Del Ransomware Cryptowall

Ultimamente se ha conocido una gran **variedad de ransomware**  o **virus policía**, además de actualizaciones que han ido evolucionando para evitar o mejorar la forma de estafa. Como ya antes habíamos hablado, [CryptoLocker es uno de los potentes malware](#) que han evolucionado para engañar de una forma tan sutil a los usuarios, aun así, existen otros [programas maliciosos](#) que han surgido para reemplazarlo, estamos hablando del ransomware **CryptoWall**.

El despiadado ransomware Cryptowall está de regreso, con una reciente y mejorada versión del **malware que cifra archivos**. La nueva versión, llamada **Cryptowall 3.0** (o Crowti), usa las redes anónimas de Tor e [I2P](#) para llevar a cabo la comunicación entre las víctimas, además de mantener lejos a los investigadores y funcionarios encargados de hacer cumplir la ley.

El uso más notable de la poco conocida [red anónima I2P es la nueva Silk Road Reloaded](#), la nueva versión del conocido mercado negro en línea que operaba en un servicio oculto de Tor antes de ser disuelto por la policía. El Investigador francés [Kafeine](#) confirmó el uso de I2P para el mando y control de la comunicación, mientras que Microsoft informó que los enlaces a la página de instrucciones de descifrado todavía se realizan en la red Tor. Horgh (Horgh_RCE) han publicado un [análisis técnico](#) sobre el **malware identificado por Microsoft** a finales del año pasado.

«Parece que la comunicación con el C & C (comando y control) es codificado con [Rc4](#), y al parecer la clave parece ser alfanumérica y enviada usando el metodo POST» Kafeine escribió en un blog.

❌ Como ya se sabe, **CryptoWall cifra los archivos de las víctimas** con un fuerte cifrado RSA 2048, hasta que la víctima paga una cuota de rescate para conseguir que se descifren los archivos. A las víctimas se les pide pagar el equivalente a \$ 500 USD en Bitcoin para recibir la clave de descifrado que les permita recuperar sus archivos.

El programa ransomware proporciona a los usuarios enlaces a varios sitios que actúan como puertas de acceso Tor, los cuales se conectan automáticamente al navegador del usuario y al servicio de descifrado CryptoWall alojado en la red Tor. Sin embargo, con **CryptoWall 3.0**, el tráfico del usuario también pasa a través de I2P, la otra red de anonimato.