Investigadores de seguridad cibernética lanzaron una versión actualizada de la herramienta de descifrado del ransomware GrandCrab, que permitiría a millones de usuarios afectados desbloquear sus archivos cifrados de forma gratuita sin pagar un rescate a los piratas informáticos.

GrandCrab es una de las familias de ransomware más prolíficas hasta la fecha, que ha infectado a más de 1.5 millones de computadoras desde que apareció pro primera vez en enero de 2018.

Creada por BitDefender, la nueva herramienta de descifrado de GrandCrab, ahora puede desbloquear archivos encriptados por las últimas versiones del ransomware, de 5.0 a 5.2, así como para las versiones anteriores del ransomware.

Como parte del proyecto *«No más ransom»,* BitDefender trabaja en asociación con el FBI, Europol, la Policía de Londres y otras agencias de aplicación de la ley en todo el mundo para ayudar a los usuarios afectados por el ransomware.

La compañía de seguridad cibernética lanzó en los últimos dos meses herramientas de eliminación de ransomware para algunas versiones anteriores de GrandCrab que ayudaron a casi 30,000 víctimas a recuperar sus datos de forma gratuita, ahorrando aproximadamente 50 millones de dólares en rescates.

Los creadores de GrandCrab anunciaron recientemente el retiro de sus operaciones de Ransomware-as-a-service (RaaS), que permitieron a los piratas informáticos criminales afiliados al crimen organizado, extorsionar más de 2 mil millones de dólares a las víctimas.

> *«Mientras que el número es muy exagerado, la operación de GrandCrab fue lo suficientemente prolífica como para obtener suficientes ingresos para permitir que sus maestros se retiren. El cierre será seguido por la eliminación de todas las claves, dejando a las víctimas incapaces de recuperar los datos rescatados incluso pagando un rescate»,* dijeron los investigadores.

> *«Lanzado en enero de 2018, GrandCrab se convirtió rápidamente en la herramienta para piratas informáticos para el ransomware basado en afiliados, con una participación del 50% de todo el mercado de ransomware a mediados de 2018»,* explicó la Europol.
>
> *«Establecidos como un modelo de licencia de ransomware-as-a-service, los distribuidores podrían comprar el ransomware en los mercados web oscuros y distribuirlo entre sus víctimas. A cambio, pagarían el 40% de sus ganancias a los desarrolladores de GrandCrab y se quedarían con el 60% para ellos mismos»,* agregó.

La mayoría de los virus informáticos infectan los sistemas debido a la falta de prácticas simples de seguridad. Estos son algunos consejos para seguir con el fin de proteger las computadoras contra ataques de ransomware:

- Tener cuidado con los correos electrónicos de suplantación de identidad (phishing), siempre es necesario sospechar de los documentos solicitados que se envían por correo electrónico y nunca hacer clic en los enlaces que se encuentran dentro de los documentos, a menos que se verifique la fuente.
- Realizar copias de seguridad regularmente.
- Mantener el software y sistema antivirus actualizados.