Wanna Cry fue un ataque cibernético mundial que se llevó a cabo el 12 de mayo de 2017, logrando afectar a más de 200 mil sistemas en 150 países. Kaspersky Lab informó que México se encuentra en el lugar número 11 de los países más afectados por el ransomware.

La compañía informó en un comunicado que la nación más afectada fue Rusia, con 33.64% de empresas atacadas, seguida por Vietnam, con 12.45%, India con 6.95%. Mientras que en América Latina, Brasil ocupa el sexto lugar con 4.06% y México la undécima con 1.59%.

Kaspersky afirma que la principal característica del ataque fue la forma de propagación, por medio del exploit Eternal Blue, que instalaba por Internet la puerta trasera DoublePulsar, que se utiliza para inyectar código malicioso sin requerir interacción con el usuario.

Cuando los equipos se infectan, WannaCry cifra la información y extorsiona a las víctimas, pidiendo un pago para rescatar su información.

La compañía de seguridad afirma que WannaCry mostró lo fácil que era explotar una vulnerabilidad conocida para el sistema operativo Windows, y aunque el parche ya estaba disponible, muchos administradores de sistemas se percataron que su red estaba expuesta cuando ya era demasiado tarde.

> *«La lección de Wanna Cry es que un virus puede causar daños reales, hasta pérdidas de millones de dólares. Estas ya no son consecuencias aisladas de ataques dirigidos de alto perfil, sino de ataques simples que afectan al mayor número de víctimas posible»,* dijo Dmitry Bestuzhev, director del Equipo de Investigación y Análisis para Kaspersky Lab América Latina.

Explicó también que las empresas deben tener presente que todos están en peligro y por lo mismo, sus negocios y activos corren gran riesto. Según estadísticas de Kaspersky Lab, el 65% de las empresas afectadas por ransomware en 2017 perdió acceso a una gran cantidad de datos o incluso todos sus datos, además de que una de cada seis de las que pagaron el rescate nunca recuperó su información.

Ante la problemática, Kaspersky Lab recomienda a las compañías verificar que se ha instalado el parche de Microsoft que corrige la vulnerabilidad específica, y asegurarse de instalar las actualizaciones de seguridad que resuelven vulnerabilidades en el futuro.