Crece Ransomware en 2016 al 16,700%: SonicWall

La compañía de seguridad informática SonicWall presentó su Informe Anual de Amenazas 2017, que recoge los datos de más de un millón de sensores que componen su Red de Respuesta Global de Inteligencia de Defensa contra Amenazas (GRID), según el cual el número de ataques de modalidad Ransomware fue 167 veces mayor en 2016 con respecto al año anterior, pasando de los 3.8 a 638 millones.

El informe relaciona está explosión con la disponibilidad del Ransomware como Servicio (RaaS) que lo hace mucho más fácil de implementar, y que se puede obtener como un kit por una tarifa de alrededor de $100 dólares, aunque en otros casos también contempla un porcentaje sobre la ganancia mal habida.

Este aumento desmedido, relata el estudio, inició en marzo pasado cuando pasó de un promedio de 282 mil ataques por mes a casi 30 millones, para finalizar el año con más 266 millones de ataques de este tipo tan sólo en el último trimestre.

Entre las ramas de la industria más atacadas dentro de la modalidad se encontraron ingeniería mecánica e industrial con 15% de los incidentes, farmacéuticas y entidades financieras, cada una con 13%; y las bienes raíces con 12%.

Mientras que muchas empresas y entidades deciden no hacer público que han sido vulneradas, hubo casos que en 2016 cobraron notoriedad como el sufrido por la Agencia de Transporte Municipal de la ciudad de San Francisco, California, cuando más de 200 computadoras fueron bloqueadas exigiendo un rescate de 100 Bitcoins (73 mil dólares en esa fecha), que tuvo como consecuencia que los pasajeros viajarán sin cobro en el sistema de transportación por rieles. La autoridad negó haber pagado el rescate, caso contrario al del Hollywood Presbyterian Medical Center de Los Ángeles donde se admitió haber entregado una suma equivalente a 17 mil dólares a los cibercriminales.

El informe también menciona que habiendo pagado o no el rescate, sólo 42% de las empresas atacadas fueron capaces de recuperar totalmente sus datos, y que el impacto económico de un ataque de estas características podría llegar a ser hasta 99 veces el monto exigido como rescate.

Entre las predicciones sobre el tema, el informe estima que los delincuentes empezarán a secuestrar dispositivos conectados al Internet de las Cosas (IoT), y que potencialmente podrían parar las líneas de producción en una instalación industrial, redes de energía en centros urbanos, flotillas de vehículos de entregas e incluso conectarse a dispositivos de médicos como marcapasos y exigir rescate para no interrumpir su función.