Riesgos Cibernéticos

FUENTE: http://www.netmedia.mx/b-secure/ransomware-cortina-de-humo-para-atacar-infraestructura-critica/

Ransomware: cortina de humo para atacar infraestructura crítica

Desde hace algún tiempo las firmas de seguridad informática vienen alertando sobre un repunte en los ataques de ransomware a nivel mundial. A mediados de año, el ESET Security Report apuntaba que los ataques de ransomware ocupaban la segunda posición de incidentes en la región (16%) e, inclusive, habían desplazado al phishing al tercer lugar de las amenazas.

No obstante, conforme ha avanzado el año, las características de este tipo de ataques han motivado a los especialistas a hacerse una pregunta: ¿sólo se trata de ataques de ransomware o estamos frente a ataques con fines distintos?

Según los analistas de S21sec, así lo es. Aseguran que el ransomware ha sido utilizado por los cibercriminales como una cortina de humo para encubrir ataques dirigidos a corporativos e infraestructuras críticas. Basta pensar en Wanna Cry, Not Petya y Bad Rabbit para caer en la cuenta.

❖ El caso de Japón

Un ejemplo reciente es la persistencia de este tipo de ataques contra la industria japonesa. Antonio Ruiz, team leader ACS & MSS de S21Sec para México y Latinoamérica, destaca que la constatación de ataques persistentes contra dicha industria en un marco temporal comprendido entre tres y nueve meses (entre cuyos fines se encontraba el de codificar cientos de máquinas a la vez) ha disparado las alarmas acerca de su verdadero objetivo.

El analista asegura que, en el proceso de análisis de los actores implicados en este ataque, los ransomware utilizados responden al apelativo ONI y MBR-ONI, es decir, cada uno de ellos juega un papel diferenciado que no está dirigido al carácter expropiatorio y lucrativo, sino al robo de información confidencial.

Así las cosas, las nuevas funcionalidades detectadas han suscitado inquietud en buena parte de analistas en todo el mundo, por la potencial proyección y consecuencias de su extensión a otros continentes. Para Ruíz, lo anterior se fundamenta, en buena medida, en el análisis del crecimiento del ransomware como amenaza global que puede generalizarse en el corto o mediano plazo. Según él, esto podría poner en serio peligro las infraestructuras de muchos países.