ágoraSIC Centro de Conocimiento en Ciberseguridad

Ciberataques en 2019: la imaginación al poder

Los golpes de la delincuencia (más o menos organizada) de marcada especialización en el robo de dinero directa o indirectamente, las escaramuzas entre estados enfrentados en una guerra político-comercial con las empresas estratégicas como campo de batalla, los grupos activistas de distinto alcance y orientación, las actividades terroristas y todo lo que media entre estas realidades, no van a frenar su escalada en el actual ciberespacio. El negocio es rentable para los ladrones, tiene interés para los estados rivales y la elaboración de campañas de agitación masivas todavía prende en muchas capas de la población.

Esta es la conclusión general a la que se llega tras leer con detenimiento las respuestas de 161 entidades públicas y privadas vinculadas con la ciberseguridad a las que SIC ha formulado la siguiente pregunta: ¿Qué técnicas novedosas se espera que pongan en práctica los ciberdelincuentes durante 2019?

SUMARIO

* Es posible obtener una versión en pdf de este especial rellenando el formulario disponible en www.revistasic.com

INNOTEC AN ENTELGY COMPANY

Félix Muñoz
CEO

"En este 2019 es de esperar que se sigan explotando los eslabones más vulnerables de la ciberseguridad: las personas y la cadena de suministro (proveedores y terceros en general). Asimismo el incremento constante del número de dispositivos conectados (IoT) aumentará en gran medida el nivel de exposición tanto de las empresas, como de los usuarios finales. En cuanto a las técnicas empleadas, muchas se repetirán (*ransomware* dirigido, APT, DDoS...), pero también irán apareciendo algunas novedosas. Así, vamos a ver un número cada vez mayor de *malware* sin fichero, así como las primeras muestras públicas de este software dañino incrustado en el *firmware* de algún dispositivo. No obstante, el *malware* más habitual seguirán siendo los *criptominer*, en la medida de que siga siendo una fuente de ingresos fácil y de bajo riesgo para los ciberdelincuentes.

Por otro lado, desde Innotec estamos convencidos de que seguirá el incremento exponencial de las amenazas a entornos industriales e infraestructuras críticas. Desgraciadamente, quizá sea solo cuestión de tiempo, antes de que los ciberdelincuentes usen sistemas secuestrados para apagar, encender, dañar o, peor aún, descontrolar una infraestructura crítica con un impacto significativo".