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

CCN – CENTRO CRIPTOLÓGICO NACIONAL

Carlos Abad
Jefe de área de Sistemas de Alerta
y Respuesta a Incidentes
Coordinador del CCN-CERT

"Muchas de las técnicas detectadas en 2018 seguirán vigentes este año, pero por supuesto irán surgiendo otras nuevas. En este sentido, habrá más ataques contra la privacidad de los datos –especialmente en el sector salud, compañías del sector bancario y de comercio electrónico, o de manera masiva de importantes redes sociales y proveedores de servicios digitales–. Se verán ataques más avanzados contra entornos móviles y cloud, así como contra sistemas de control industrial (ICS), sin olvidarnos de los ataques DDoS y del uso de un amplio abanico de otras técnicas ya al alcance de muchos gracias al *Cybercrime as a Service*.

Por otra parte, el *ransomware* dirigido ya es una realidad –donde la intrusión y el rescate solicitado se adapta al tipo de víctima–. El robo de *wallets* de monedas virtuales seguirá siendo tentador también. Asimismo los *routers* domésticos serán objetivo de muchos actores como medio para lanzar ataques de amplia escala o para anonimizar la infraestructura operativa del atacante (*botnets*, *hide behind the noise*, etc.); en este campo los ISP y fabricantes deben mejorar la política y frecuencia de actualización de estos dispositivos (credenciales *hardcodeadas* en *firmware*, puertas traseras, recursos accesibles desde WAN, etc).

El mayor uso de técnicas *fuzzing* permitirá la detección de más vulnerabilidades críticas en librerías básicas y fundamentales, como lo sucedido este año con Lib-SSH, de las cuales tenemos constancia años después. También se detectarán más fallos en el diseño de los microprocesadores, que requerirá el esfuerzo conjunto de fabricantes y desarrolladores de sistemas operativos para alcanzar soluciones de compromiso.

Igualmente se observa una creciente tendencia en la explotación de vulnerabilidades *1-day* (recién publicadas). Tendemos a pensar que los grupos APT usan sólo 0-days, pero APT28, entre otros actores APT, usa constantemente vulnerabilidades 1-day para lanzar las campañas masivas de *spear-phishing* para infectar a sus víctimas (*TIME TO EXPLOIT < TIME TO PATCH*).

Por último, no debemos olvidar los posibles intentos de influir en el estado de opinión de la ciudadanía aprovechando la potencia y capilaridad de la red como otro de los vectores a explotar por diferentes grupos o Estados para conseguir sus objetivos. Y teniendo en cuenta el mapa Geopolítico y el auge de ciberataques "esponsorizados" especialmente por superpotencias, el 2019 nos deparará sin ningún lugar a dudas una mayor respuesta, disuasión efectiva, la necesidad de compartir y unir esfuerzos".