Las amenazas persistentes avanzadas (APT, por su sigla en inglés) son ataques cibernéticos personalizados y dirigidos a un blanco específico, ya sea una entidad gubernamental o empresarial. Debido a su diseño “a la medida” para intentar vulnerar un sistema, los métodos de protección tradicionales como los antivirus resultan ineficaces. Y detrás de estas amenazas generalmente están los mismos gobiernos.

Estas amenazas se caracterizan porque son ejecutadas por alguna entidad que tiene dictada una agenda, cuentan con vasto financiamiento y no se comparan con las formas de hackeo anónimo que buscan robar información o infectar sistemas aleatoriamente.

Marco Lux, director ejecutivo de Curesec GmbH, una empresa con sede en Berlín integrada por profesionales dedicados a la seguridad de TI, dice que este tipo de ataques, por su complejidad y necesidad de recursos monetarios, pueden ser perpetrados en su mayoría por gobiernos o contratistas secretos del gobierno.

> “Esto ha estado ocurriendo por algún tiempo. Cuando esto sucede, es alrededor de estados que espían para obtener información. Por ejemplo, el grupo Hacking Team de Italia ha sido empleado por algunos gobiernos y habrá más jugadores”, aseguró durante la conferencia The Be Mobile, organizada por Blackberry.

The Hacking Team es desarrollador de un programa espía conocido como «DaVinci» or «Galileo», que fue descubierto por el grupo The Citizen Lab de la Universidad de Toronto. También figuran competidores como FinFisher y otras amenazas como Ghostnet, Uruburus, Stuxnet o Careto y que han tenido actividad en México.

El experto en seguridad Bruce Schneier dice que con este tipo de amenazas son desarrollos de alta habilidad y enfoque, donde las medidas de seguridad son relativas pues “tú eres el objetivo y los ataques no descansarán hasta que se quebranten los sistemas”.

Si bien no hay una medición certera sobre cuántas y cuáles gobiernos realizan este tipo de campañas informáticas pues se trata de operaciones encubiertas y sin transparencia, este tipo de ataques ya preocupa a las compañías tecnológicas como Cisco pues cambian el paradigma de la protección informática.

Estos ataques encuentran además un sinfín de puertas de entrada a las redes informáticas gracias al crecimiento de la adopción de dispositivos móviles en las empresas y organizaciones que administran información confidencial.

Un análisis de la firma de seguridad informática Trend Micro calcula que tan sólo en marzo se registraron 2.1 millones de ataques a dispositivos móviles.

> "La amplitud de dispositivos generó la capacidad de los hackers para tener una solución específica y tomar provecho de eso. Existen amenazas específicas que no son reconocidas por ningún dispositivo de seguridad pues se enmascara y las soluciones antivirus tradicionales no los reconocen. El 40% de las amenazas actuales, las reconoce el antivirus y el resto son amenazas muy específicas", aseguró Ghassan Dreibi, de la tecnológica Cisco Systems.

Ante la ineficacia de los sistemas tradicionales de protección contra virus y programas malignos, tanto Cisco como Bruce Schneier consideran que será fundamental el análisis en tiempo real de la actividad en las redes de Internet para la detección temprana de los intentos de ataque y equipos comprometidos o infectados que podrían representar un peligro para empresas e instituciones.

Dreibi, de Cisco, dice que es fundamental identificar el origen de los problemas que comienza con una visualización total de los accesos y la actividad que existen en las redes corporativas e institucionales, pues una amenaza puede valerse además de las cámaras y los micrófonos de los dispositivos para obtener información y realizar actividades de espionaje.

> “No se puede esperar 2, 3 o 4 años para reconocer una amenaza. Tiene que ser en minutos, saber cuál fue el paciente cero. La persona, el dispositivo, la sucursal que generó el problema inicial.

Estamos en un momento muy crítico y las amenazas son avanzadas, las personas que lo manipulan saben lo que quieren hacer y se enmascaran”, aseguró el experto.

Y es que el fortalecer la seguridad de las redes, más allá de la instalación de un antivirus tradicional, será fundamental para el desarrollo del Internet de las cosas (objetos conectados y que se comunican entre sí a través de la Internet) y de la conformación de las ciudades inteligentes, que son urbes tecnológicas que buscan mejorar la calidad de vida de la sociedad mediante la tecnología.

Fuente: eleconomista