Virus letales

Con frecuencia, Hollywood juega con la realidad manipulándola, distorsionándola y exagerándola, con lo que en ocasiones crea mezclas divertidas de ficción. Sin embargo, en asuntos relacionados con la seguridad informática, tarde o temprano realidad y ficción inciden en un mismo punto. Películas como *Juegos de Guerra*, *Hackers* o *La red* hacen referencia a amenazas informáticas que vulneran la seguridad no solo de la infraestructura informática de una organización, sino de toda una nación, continente o el mundo entero. Desde que en *Duro de Matar 4.0* (2007) Matt Farrell (Justin Long), el *hacker* que ayuda al policía John McClane (Bruce Willis) a detener a un grupo de ciberterroristas que controlan y logran colapsar los sistemas de comunicación, financieros, de servicios, transportes y militares de Estados Unidos, hasta la detección en 2010 de un gusano capaz de controlar ciertos procesos de una planta nuclear localizada en el medio oriente, transcurrieron tan solo tres años. Si bien los acontecimientos mostrados en estas cintas son desmedidos, tendenciosos y en muchos casos irreales, pareciera que en los últimos años están siendo premonitorios.

En efecto, el primer caso fue justo en septiembre de 2010 en Irán, cuando un gusano denominado Stuxnet se infiltró vía USB en los sistemas operativos Windows, dispersándose hasta localizar una red local interna específica; una vez ahí, inició la búsqueda de los sistemas de control industrial, en particular aquellos diseñados por la empresa alemana Siemens. Después de haber localizado su objetivo, comenzó la reprogramación de su código (denominado PLC), lo que permitió controlar las válvulas de centrifugado de uranio de la planta nuclear ubicada en Natanz, todo ello sin que se enteraran los operadores. Los expertos en seguridad informática aseguran que este gusano era tan complejo y específico que solo un grupo de *hackers* altamente especializados y con financiamiento gubernamental habrían sido capaces de desarrollarlo; se sospechaba de países como Estados Unidos e Israel.

Otro caso, detectado en 2012 por distintas instancias relacionadas con la seguridad de la información, fue de un gusano denominado Flame o Skywiper, desarrollado con un alto grado de complejidad, incluso varias veces mayor al de Stuxnet. Este *malware* era capaz de propagarse a través de redes de área local o mediante memorias USB. Su función básica era espiar y robar información a través de distintos medios: *screenshots* (capturas de pantallas), *keylogger* (registro de toda actividad realizada por medio del teclado), monitoreo de tráfico de red, grabación de conversaciones (mediante la activación del micrófono), control de bluetooth identificando dispositivos cercanos e intentando acceder a ellos, control de la *webcam*, mensajes de correo electrónico, entre otros; una vez recolectada la información, era enviada directamente a los atacantes.

Gauss, también detectado en 2012, era un gusano capaz de espiar transacciones bancarias, así como de obtener información de correos electrónicos, configuración de equipos, contraseñas, mensajes o datos de acceso a redes sociales. Este gusano recibe su nombre en honor al científico Carl Friedrich Gauss y está compuesto por varios módulos cuyos nombres también están vinculados con la sociedad matemática: Lagrange, Gödel, Tailor y Kurt; cada uno de ellos tiene una función específica en el proceso de infección, captación, procesamiento y envío de información. Se ha sugerido que esta labor estaba vinculada a una actividad de espionaje más que al simple robo de información. Su propagación se centró en bancos del Líbano, aunque también se registraron incidentes en Israel y el territorio de Palestina.

Según los expertos, los tres casos anteriores tienen enormes similitudes en alguno de sus módulos, lo que ha llevado a pensar que fueron creados por los mismos autores. Parte de estos análisis la desarrollaron Kaspersky Labs, Laboratory of Cryptography and System Security (CrySys) de la Universidad de Budapest, Iran-CERT, entre otras.

Estos son solo algunos ejemplos de lo que un *malware* sofisticado es capaz de realizar, y si bien es cierto que las intenciones de su desarrollo, propagación y daños tuvieron tintes políticos, también es claro que deja la puerta abierta para crear virus cuyo alcance y letalidad sobrepasen los límites de la imaginación. Códigos malignos que puedan acceder y controlar a modo sistemas de generación y suministro de energía eléctrica o sistemas de control que monitoreen erróneamente cadenas de suministro de alimentos, gas o productos farmacéuticos; o quizá equipo médico como tomógrafos, mastógrafos o aceleradores lineales ilegalmente intervenidos, que alteren posibles detecciones de cáncer, realicen mediciones incorrectas o reporten diagnósticos falsos.

Aunque la integración e interconexión de la tecnología a Internet es una realidad y promete innumerables beneficios para el ser humano, es preciso crear conciencia de las repercusiones negativas si no se desarrollan a la par sistemas de seguridad eficaces que minimicen la intromisión de usuarios indeseables.