MONOGRÁFICO

Ciberseguridad, ¿juegos de guerra?

El ciberespacio es un gran tablero de juego en el que las organizaciones públicas y privadas se defienden de ciberdelincuentes, terroristas, hacktivistas o espías. ¿Quién ganará la partida? En este monográfico analizaremos el panorama de la ciberseguridad nacional desde el punto de vista de los actores más relevantes en la materia.

(Continúa en la página 18)

Ciberseguridad, ¿Juegos de guerra?

(Viene de la página 18)

MIGUEL ÁNGEL RODRÍGUEZ RAMOS
Jefe de Área Informática.
Subdirección General de Tecnologías de la Información y de las Comunicaciones.
Ministerio de Industria, Energía y Turismo

La sociedad de la información en la actualidad es una sociedad hiperconectada, en la que las conexiones de banda ancha, los dispositivos móviles smartphones y las tabletas están plenamente extendidas entre los ciudadanos. El crecimiento del uso de las redes sociales y los sistemas de mensajería instantánea han convertido a Internet en una red en la que estamos todos y en un medio casi imprescindible en nuestra vida diaria. Los servicios multimedia están cobrando un papel destacado y el ocio ha pasado a ser el motivo principal para conectarse a Internet. Los servicios en la nube han permitido la interoperabilidad multidispositivo en entornos domésticos, y cada vez son más los usuarios que almacenan su información personal para tenerla accesible desde ordenadores, tabletas, videoconsolas o Smart TVs.

En el ámbito de las empresas y de las Administraciones Públicas, los servicios de comercio electrónico, banca electrónica y administración electrónica son una realidad en constante cambio para adaptarse a las necesidades de los clientes o ciudadanos a través de los avances que permite la evolución de la tecnología. Los conceptos de *Cloud Computing, Big Data*, Internet de las cosas, *Bring Your Own Device* (BYOD) o *Bring Your Own Application* (BYOA) son una fuente de oportunidades de mejora para las organizaciones, pero llevan aparejados nuevos riesgos que hay que gestionar de la manera más eficiente posible.

El avance de la tecnología en nuestra sociedad es imparable y, además de proporcionar beneficios a los ciudadanos, contribuye a un modelo productivo más eficiente para las empresas y las Administraciones Públicas. La demanda de los usuarios y la competitividad de los mercados empresariales y de consumo presionan continuamente para reducir el time to market a la hora de ofrecer nuevos servicios, quedando descuidados en muchas ocasiones los aspectos relacionados con la seguridad de la información. El ecosistema digital es cada vez más complejo y evoluciona de forma vertiginosa, dejando a la regulación un paso por detrás de la tecnología y un escenario de riesgo de ciberseguridad creciente que debería preocuparnos.

Las piezas negras

Aprovechando la terminología "hacker de sombrero blanco" que representa a los que se ocupan de mejorar la seguridad de los sistemas y "hacker de sombrero negro" para los que utilizan sus conocimientos con fines maliciosos e incluso delictivos, hablaremos de "los malos" del juego en el panorama de la ciberseguridad, como las piezas negras. Las principales amenazas en la actualidad son el ciberespionaje, la ciberdelincuencia y el hacktivismo.

El ciberespionaje lleva a cabo su actividad mediante ataques dirigidos a través de amenazas persistentes avanzadas (*Advanced Persistent Threats*, APT). Las APTs son altamente sofisticadas y explotan vulnerabilidades de día-cero o técnicas personalizadas adaptadas a cada objetivo. Algunas de ellas han estado operando durante años sin ser detectadas. Estas amenazas, originariamente dirigidas a empresas e insti-

Máscara de Guy Fawkes. Avatar de Anonymous y del hacktivismo

tuciones públicas, actúan también sobre personas individuales, incluyendo altos directivos de compañías y de organismos públicos, personajes notorios y responsables políticos.

En algunos casos, las APTs son auténticas ciberarmas al servicio de ejércitos o agencias de inteligencia. Aunque son muchos los países que están desarrollando sus capacidades de seguridad ofensiva y defensiva, los más activos en esta ciberguerra fría son Estados Unidos, China y Rusia, apareciendo como amenazas emergentes Corea del Norte y el Estado Islámico.

A continuación se describen las fases de una APT.

1.Reconocimiento. El atacante analiza el perfil de la organización objetivo y obtiene toda la información posible desde el exterior para desarrollar una estrategia de ataque dirigido.

2.Intrusión. El atacante se introduce en la red del objetivo usando ingeniería social con un malware dirigido a sistemas y personas vulnerables.

3.Descubrimiento. Una vez colonizado un sistema del objetivo, el atacante analiza la red interna desde dentro de manera sigilosa para establecer un plan de persistencia y desplegar alternativas mediante infecciones a través de saltos laterales en la red.

4.Búsqueda de información sensible. Una vez asegurada la persistencia y comunicación continuada con el atacante, la APT se dedica a localizar información sensible robando credenciales, buscando unidades de red mapeadas o bases de datos corporativas.

5.Exfiltración de datos. Finalmente, se envían los datos robados de manera cifrada a través de protocolos comunes (http, https, FTP) para pasar desapercibido entre el tráfico legítimo de la organización.

Las fases pueden tener una larga duración en el tiempo, el suficiente hasta cumplir su objetivo, ya que este tipo de ataques son muy persistentes y están muy bien financiados por los gobiernos o agencias de inteligencia, así que se dispone de suficientes recursos y tiempo para llevarlos a cabo.

La ciberdelincuencia persigue fines lucrativos cometiendo diversas acciones delictivas en Internet. El mundo del cibercrimen está muy bien organizado y los procesos relacionados con la tecnología están altamente industrializados. Según Microsoft, el cibercrimen le cuesta a la economía global 500.000 millones

Agencia de Seguridad Nacional (National Security Agency, NSA)

de dólares. Hoy en día nadie realiza una acción delictiva extremo a extremo porque todo puede comprarse como un servicio en el mercado negro. El coste de infectar un ordenador es de 2$ y el de obtener 10.000 ordenadores bots para realizar un ataque de denegación de servicio durante una hora es de 200$. Las acciones masivas de estafa por Internet o de secuestro de datos mediante cifrado por infección requieren un coste de inversión muy bajo que se rentabiliza en cuanto un par de víctimas inocentes caen en el engaño. La Internet Profunda (Deep Web), ajena al mundo conocido indexado por los grandes buscadores, está plagada de asuntos ilegales y mercados no regulados en los que se paga con la moneda virtual BitCoin para evitar dejar rastro.

La persecución de los delitos telemáticos es compleja debido a la falta de fronteras de Internet y a la falta de legislación global sobre la materia. En la actualidad, un gran porcentaje de casos de ciberdelincuencia no se denuncian, y de los pocos que se denuncian son muy pocos los que consiguen resolverse con éxito.

El hacktivismo o ciberactivismo se apoya en la utilización de herramientas digitales con fines sociopolíticos. Estas acciones pueden incluir la interrupción de los servicios públicos o las actividades empresariales mediante ataques de denegación de servicio, modificación de contenidos o deterioro de la reputación online de las víctimas. Existen diversos grupos hacktivistas a nivel regional pero el más conocido a nivel global es Anonymous.

Las reglas del juego

Viendo la situación del tablero de juego en la que todo parece favorable y la situación de las piezas negras en la que "los malos" parecen tener una posición ganadora, cabe preguntarse, ¿Cómo hemos llegado hasta aquí?

A principios de los 80 la película "Juegos de guerra" contaba la historia de un adolescente inadaptado con conocimientos informáticos que, con la única intención de jugar a videojuegos, acababa introduciéndose en los sistemas del Departamento de Defensa de los Estados Unidos y estuvo a punto de provocar la tercera guerra mundial. Aunque pudo ser una película inspiradora para algunos de los que crecimos con ella, instauró una imagen de la amenaza en ciberseguridad que se ha mantenido a lo largo del tiempo y que todavía sigue vigente en nuestros días entre los profanos en la materia.

La competitividad de los fabricantes de productos de tecnologías de la información por hacerse con el mercado ha exigido funcionalidad, usabilidad y diseño, pero ha sido tolerante con la inseguridad de los productos. Los usuarios hemos aceptado como algo normal que los productos sean vulnerables cuando salen a la venta y que tengan que parchearse continuamente. Un nivel de calidad y seguridad tan bajo sería inaceptable en cualquier otra industria.

Las organizaciones públicas y privadas no han priorizado sus inversiones en seguridad porque no han visto claro el retorno de la inversión, con los métodos de análisis más utilizados, frente a otros tipos de proyectos tecnológicos. Para evitar esta baja prioridad de los proyectos de seguridad, los gobiernos y las organizaciones dedicadas a la estandarización y normalización han impulsado normas y leyes para forzar el cumplimiento normativo.

Actualmente, nos encontramos en la era post Snowden que, con su confesión sobre el programa de espionaje PRISM nos quitó la venda de los ojos para mostrarnos que la Agencia de Seguridad Nacional (National Security Agency, NSA) nos espía en colaboración con empresas como Microsoft, Google, Apple, Facebook o Yahoo. En este ambiente de desconfianza, los investigadores de vulnerabilidades de seguridad han descubierto fallos en protocolos de comunicaciones seguras como SSL o TLS en los que todos confiábamos y sobre los que construíamos productos supuestamente seguros.

Las piezas blancas

A la vista de la situación del tablero de juego y de la posición aventajada de las piezas negras, las piezas blancas, "los buenos", no se han quedado de brazos cruzados y han movido ficha. Con la única pretensión de que este monográfico sea de su agrado y que no se tomen la ciberseguridad como un juego, algunos de los actores más relevantes en esta materia en nuestro país relatarán su visión de la situación y las medidas que están adoptando en cada ámbito de actuación. ✱

La persecución de los delitos telemáticos es compleja debido a la falta de fronteras de Internet y a la falta de legislación global sobre la materia

En el año 1998, ASTIC publicó en su Boletic nº 8 un monográfico de Seguridad Informática coordinado por Miguel Ángel Amutio. Puedes acceder al contenido en http://www.astic.es