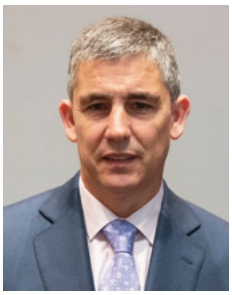


Ciberespionaje, una amenaza al desarrollo económico y la defensa

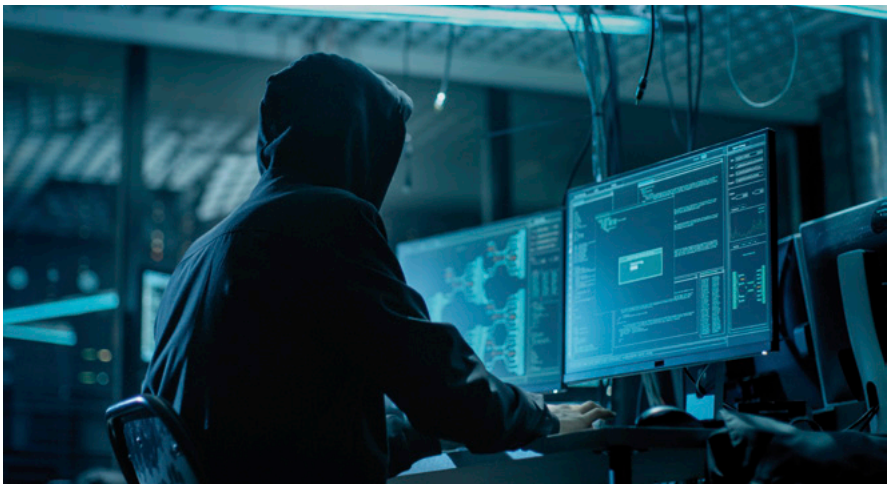
Javier Candau / Jefe de Ciberseguridad del Centro Criptológico Nacional

La situación geopolítica actual marca la tendencia creciente al ciberespionaje, una amenaza que confirma el interés de los atacantes por obtener información sensible de sus víctimas. Estos agentes de la amenaza están creando nuevas técnicas y herramientas para intentar robar la propiedad intelectual de sus objetivos. Ante esta situación, el Centro Criptológico Nacional apuesta por la mejora continua de las capacidades de vigilancia y detección a través de Servicios de Alerta Temprana (SAT) y de evaluación continua (Centro de Operaciones de Seguridad).

En los últimos años, ha crecido enormemente el número de países que ha adquirido la capacidad de recopilar inteligencia del ciberespacio. El ciberespionaje es un método relativamente económico, rápido y tiene menos riesgos que el espionaje tradicional porque, dada la dificultad de atribución de la autoría, siempre cabe la posibilidad de negar su uso. Durante 2017, las agencias gubernamentales de muchos países del mundo –incluyendo a España– fueron víctimas de ataques persistentes a gran escala, originados en terceros países, incluidos algunos que no habían sido previamente identificados como una amenaza para las redes de los gobiernos atacados.

Puede afirmarse que, en la actualidad, más de cien países tienen la capacidad de desarrollar ataques de ciberespionaje y su especialización sigue creciendo, de la misma manera que lo hace la amenaza que representan. Esta amenaza, utilizada principalmente por servicios de Inteligencia, está dirigida tanto al sector público como al privado y suele provenir de países que desean posicionarse de manera más favorable desde los puntos de vista político, estratégico o económico. Todo ello sin olvidar las mafias organizadas cuyos pingües beneficios no hacen prever una disminución de su actividad.

El resultado es el incremento de las campañas detectadas de ciberespionaje, tanto de motivación económica, como política. Importantes datos de investigaciones avanzadas en materia de tecnologías de la información, marítima, energética o de Defensa se han exfiltrado junto con datos personales, en ciertos casos. Tales ataques son una amenaza para el desarrollo económico y la capacidad de defensa militar y confirman el interés de los atacantes en la información sensible de las empresas e instituciones españolas y, en general, occidentales.



Así, por ejemplo, en el año 2017 las agencias gubernamentales holandesas AIVD (Servicio General de Inteligencia y Seguridad) y MIVD (Servicio Militar de Inteligencia y Seguridad) sufrieron varios ataques persistentes y a gran escala de ciberespionaje (ver CCN-CERT IA-09/18 *Ciberamenazas y Tendencias. Edición 2018*). Del mismo modo, diversos ataques dirigidos a empresas con un alto nivel en I+D+i tuvieron éxito y fueron capaces de exfiltrar información comercial confidencial de alto valor.

Capacidades ofensivas

Los servicios de Inteligencia occidentales han identificado que muchos países están invirtiendo en la creación de capacidades digitales ofensivas (esencialmente: ciberguerra o guerra híbrida). El objetivo parece claro: influir en las operaciones de información. Así, se atacan cuentas de usuario para recabar información confidencial que más tarde publica un tercero (aparentemente) independiente, al objeto de sembrar confusión y división en los oponentes. Además de ello, se ha evidenciado que muchos países están invirtiendo notablemente en la creación de capacidades digitales destinadas a un eventual o futuro sabotaje de procesos críticos.

La ocultación de los atacantes también se ha profesionalizado. Los servicios de Inteligencia han observado que varios actores estatales están utilizando estructuralmente compañías privadas de TI como tapaderas para disfrazar sus

actividades de espionaje. Además de ello, es sabido que las empresas de TI y las instituciones académicas son utilizadas por muchos Estados para desarrollar código dañino, lo que incrementa el potencial de los actores estatales para perpetrar ciberataques.

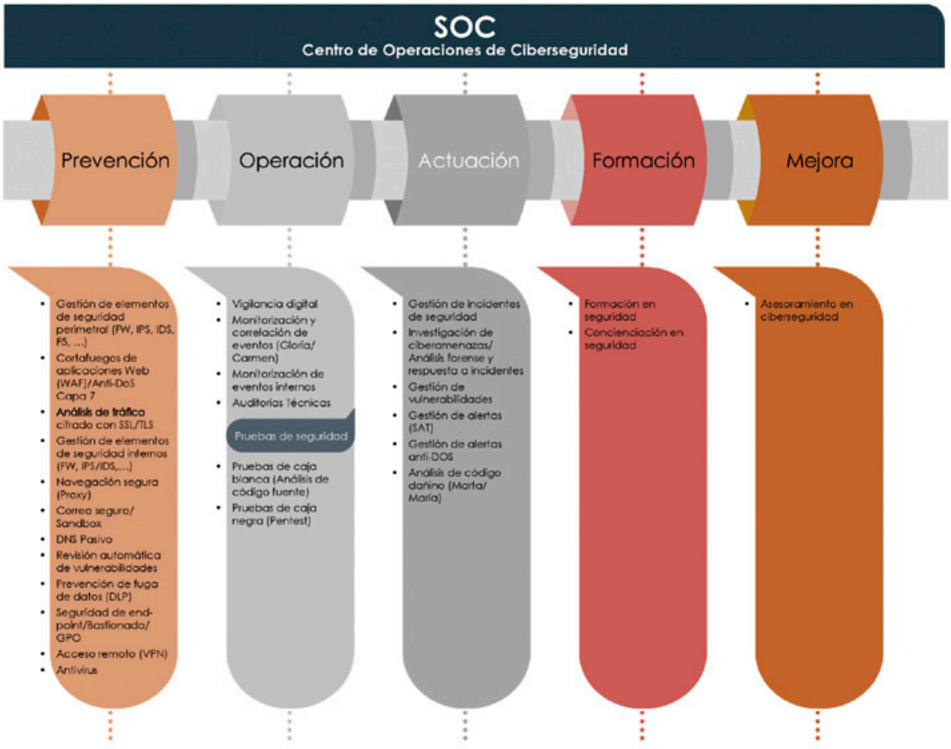
Incremento de la vigilancia

Ante esta situación, el Centro Criptológico Nacional (CCN) apuesta por sus capacidades de detección y análisis (sistemas de alerta temprana), así como por la implantación de servicios de evaluación continua que permitan conocer, en cada momento, la superficie de exposición ante una posible amenaza y así asignar recursos de manera óptima y priorizada.

A través de un Centro de Operaciones de Ciberseguridad (SOC) se realizan tareas de prevención, detección y vigilancia, supervisando a las personas, los procesos y la tecnología que intervienen en todos los aspectos operativos de la ciberseguridad.

El CCN y su Capacidad de Respuesta a Incidentes, CCN-CERT, ofrecen servicios de vigilancia, sin coste asociado, a diversos organismos de la Administración Púbica española, promocionando la creación de este tipo de centros, como el SOC de la Administración General del Estado, creado recientemente, junto con la Secretaría General de Administración Digital.

Todo ello, conscientes de la necesidad de reforzar la capacidad de prevención, monitorización, vigilancia y respuesta en el sector público a través de un SOC, además de incrementar y mejorar las capacidades para parametrizar la amenaza, identificar a los atacantes, determinar los objetivos y difundir Inteligencia al respecto.



Fuente: Centro Criptológico Nacional.

Ataques de ciberespionaje más significativos

APT33: En septiembre de 2017, se descubrió que este grupo estaba detrás de un supuesto espionaje a empresas de EEUU, Medio Oriente y Asia. La mayoría de las compañías pertenecen a la industria petroquímica, militar y de aviación comercial.

APT32 (Ocean Lotus Group): Es un grupo de ciberespionaje del sudeste asiático que amenaza a compañías multinacionales que operan en Vietnam. En 2017, se descubrió que este grupo desarrolló una campaña contra dos filiales de empresas norteamericanas y filipinas de venta de productos de consumo ubicadas en el país asiático.

APT28 (también conocido como Fancy Bear, Pawn Storm, Sofacy Group, Sednit y Strontium): Se trata de un grupo de ciberespionaje probablemente patrocinado por el gobierno ruso. A principios de julio de 2017, se descubrió una nueva campaña contra varias compañías de hostelería, incluyendo hoteles de, al menos, siete países europeos y un país de Oriente Medio.

APT29 (conocido también como Cozy Bear): Es un grupo ruso, presumiblemente asociado a los servicios secretos. En 2017, este grupo se vio involucrado en el ataque a varias instituciones públicas de Noruega (Ministerio de Defensa, Ministerio de Asuntos Exteriores y el Partido Laborista) y de Holanda (varios ministerios, entre ellos el Ministerio de Asuntos Generales).

APT17: Es un grupo con base en China que ha realizado intrusiones de red contra entidades gubernamentales de EEUU, la industria de la Defensa, bufetes de abogados, empresas de tecnología de la información, empresas mineras y organizaciones no gubernamentales. Los investigadores han analizado la posibilidad de que el ataque a CCleaner fuera impulsado por un actor estado-nación, probablemente este grupo chino.