Discurso invitado

Sr. José Sancho
Presidente de Panda Security
Socio tecnológico

Como no soy investigador ni pertenezco a un instituto de defensa, mis opiniones sobre ciberseguridad proceden de la perspectiva de un emprendedor en una empresa de ciberseguridad.

En primer lugar, el origen de los ciberataques se remonta a la digitalización. La digitalización está en todas partes. Seamos individuos, empresas o estados, todos la utilizamos. La única diferencia está en sus aplicaciones. Los individuos la usan para las cámaras digitales, los mapas, los despertadores o los periódicos; las empresas, para el marketing, las ventas y la atención al cliente; los estados la utilizan, por ejemplo, para la recaudación de impuestos o las elecciones.

Así pues, todo el mundo (personas, empresas y estados) utiliza aplicaciones digitales, y estas entidades compiten unas con otras. Las personas compiten entre sí por un ascenso en una empresa, por la riqueza o por motivos de vanidad. Las empresas compiten entre sí por la cuota de mercado. Los estados compiten por el producto interior bruto y la renta per cápita.

Y dado que todos compiten por la riqueza, ¿quién gana la competición? Los que son más productivos. En los últimos 20 años, el 80 % del incremento en la productividad ha estado relacionado con las tecnologías de la información, es decir, hardware, software o comunicaciones. A pesar de que parecen tres cosas muy distintas, todas están basadas en software y este, por definición, es vulnerable. Ni siquiera el ordenador más potente, un computador cuántico actual, puede verificar minuciosamente un solo programa con 1000 líneas de código.

Piensen en una aplicación de TI, por ejemplo en un coche autónomo, que tiene 100 millones de líneas de código. Es imposible verificar a fondo ese software, y por ese motivo las empresas de producción de software tienen a más personas en control de calidad que en desarrollo de software.

En el mercado hay trabajadores independientes que buscan *bugs* (errores) en el software. Venden los *bugs* que descubren en el mercado negro.

Dentro del ecosistema del software, en el mercado están los trabajadores independientes que buscan *bugs* en el software. Estos trabajadores independientes venden los *bugs* que descubren en el libre mercado, y algunos son incluso empresas con cotización. Zerodium es una de ellas. Es una empresa que cotiza en Nasdaq y un mercado de venta de vulnerabilidades de software. Muy a menudo, un desarrollador de software, como Microsoft o Cisco, corregirá los *bugs*, pero otras veces las empresas o estados los utilizarán para desarrollar malware.

El malware y el hackeo son las fuentes de los ciberataques, las vías criminales para obtener riqueza en un mundo digital.

Otras fuentes de ciberataques son el robo y la suplantación de identidad. El malware y el hackeo son las fuentes de los ciberataques, las vías criminales para adquirir riqueza en un mundo digital. Se trata de un nuevo tipo de delincuencia que ha surgido a raíz de la digitalización.

¿Quiénes son los atacantes a día de hoy? Existen tres grupos diferentes de atacantes. Los dos más grandes son los EE. UU. y China, ya que cuentan con más recursos. Las compañías de servicios de ciberseguridad en

EE. UU. que cotizan en Nasdaq dan trabajo a 250.000 personas, empleadas a tiempo completo en agencias de inteligencia estadounidenses.

En China la situación es menos transparente, pero teniendo en cuenta solo los informes que publican las empresas con cotización, podemos suponer que China tiene incluso más personal que los EE. UU. dedicándose a la ciberseguridad, y con las líneas que separan estado y empresas más desdibujadas.

Países como Rusia, Irán o Corea del Norte tienen interés en influir en los votantes indecisos en las elecciones.

La clave está en la necesidad de cooperación entre gobiernos, empresas e industria. En el sector militar existe una situación similar en el caso de los aviones de combate que los ingenieros desarrollan y los soldados operan, y de las armas cibernéticas desarrolladas por cientos de miles de ingenieros. Por supuesto, otros actores también pueden comprar armas cibernéticas en el mercado. Estos mercados incluyen a países estables, como Rusia, Irán o Corea del Norte, con un interés por desestabilizar otros países. Por ejemplo, tratando de influir en los votantes indecisos en sus elecciones. Gracias a toda la información disponible con la que cuentan, saben exactamente quiénes son los votantes indecisos y el tipo de mensaje al que responden.

Esos estados atacan a otros estados. A día de hoy, Europa es un blanco prioritario, pues cuenta con la segunda mayor concentración de riqueza del mundo y no está bien organizada y estructurada. Para darles un ejemplo: el año pasado, un país europeo sufrió 110.000 ataques, según los datos denunciados a su equipo nacional de respuesta a incidentes de seguridad informática (CSIRT). De ellos, 1000 procedieron de servicios de inteligencia de otros estados e iban dirigidos a instituciones de administración pública o defensa muy específicas. Algunos de estos ataques han trascendido a los medios de comunicación.

Muchos ataques se basan en armas baratas, como WannaCry o Petya, que se han sustraído a los grandes estados.

Así pues, de los tres tipos de actores, los dos mayores son estados que utilizan armas baratas. Otros actores, empresas o individuos, son los autores de los 110 000 ataques que mencioné antes. La gran mayoría de estos ataques tienen ánimo de lucro y muchos se basan en armas baratas, como WannaCry o Petya, que se han sustraído a los grandes estados.

¿Cuál es el panorama de los defensores en la actualidad? En vista de la amplia ventaja de los atacantes, ¿qué pueden hacer los defensores, por su parte? Tenemos productos como los que crea mi empresa, pero el desarrollo típico del software tarda al menos tres años y nuestros laboratorios detectan más de 300.000 nuevas muestras de malware a diario. Esto significa que, cada día, la industria de producción de malware crece más rápido de lo que podemos producir software. La otra característica de estos productos es que son globales. Una vez dispones de un producto, tienes los medios para defenderlo de todo el malware que proceda de esa fuente en ese momento. Este mercado tiene un valor anual de 35.000 millones de dólares en ingresos.

La otra cara de la industria son los servicios. Como se tardan tres años en desarrollar un producto nuevo y los ataques llegan a diario, necesitamos servicios que se basen en personas para prevenir y defendernos de esos ataques en el plano local. A nivel mundial, este mercado alcanza unos 45.000 millones de dólares, un valor superior al del mercado de productos. En términos de capital humano, significa que hay 600.000 personas trabajando en servicios. Creo que China tiene incluso más, y probablemente los EE. UU. estén al mismo nivel que China. Sabemos con certeza que en este sector trabajan al menos 250.000 personas. Esto les da una idea de por qué tenemos ataques, cuál es el panorama para los atacantes y qué pueden hacer los defensores.

¿Cómo podemos avanzar hacia un mejor control de la situación? Una analogía puede darnos una idea sobre cómo proceder. La analogía a la que me refiero es el blanqueo de capitales. Necesitamos un detonante, y el

detonante para lidiar con el blanqueo de capitales fue el 11S. Antes del 11S parecía imposible luchar contra el blanqueo de capitales, porque había personas detrás de empresas falsas y en teoría residían en estados rebeldes. Si tienes acceso a la cadena completa de capital, no obstante, parece imposible que un solo estado autónomo vaya a la guerra contra otro.

Antes del 11S parecía imposible luchar contra el blanqueo de capitales, porque había personas detrás de los estados rebeldes.

Para atajar el blanqueo de capitales, las palabras clave fueron «último beneficiario activo». Las autoridades fiscales quieren saber quién es el último beneficiario activo, quién está detrás de las empresas, quién está detrás de los estados. El último beneficiario activo es aquel que recibe el dinero y se lo embolsa. ¿Quién es el último beneficiario activo de Facebook? Probablemente Mark Zuckerberg. Incluso aunque compres el 99 % de las acciones de Facebook, la persona que dará las órdenes en la empresa será Mark Zuckerberg porque así se dispuso en el momento en que se estableció la OPV. ¿Quién es el último beneficiario activo de Google? Larry Page. Queda meridianamente claro en los estatutos sociales de la empresa. Si puedes encontrar al último beneficiario activo y seguir la cadena, encontrarás la empresa, la dirección IP, el operador de telecomunicaciones y el estado. Esta cadena en los ciberataques es análoga a la del blanqueo de capitales. Naturalmente, necesitaremos legislación específica que permita seguir la cadena, así como la capacidad de hacer cumplir dicha legislación.

Si puedes encontrar al último beneficiario activo y seguir la cadena, encontrarás la empresa, la dirección IP, el operador de telecomunicaciones y el estado.

A mi simple modo de ver, ¿qué camino debemos seguir para avanzar? Es un camino para el que, de nuevo, uso otra analogía: la disuasión respecto a las armas nucleares, que se consigue mediante la cooperación mundial entre los estados. Tenemos que descubrir las IP criminales detrás de las empresas y detrás del último beneficiario activo. Para las personas están las leyes, el derecho civil y el penal; para las empresas, el derecho mercantil, y para los estados, el derecho internacional. Deberán aplicarse las leyes correspondientes en cada caso. También tenemos que regular las compañías de telecomunicaciones, de redes sociales y de publicidad en cuestiones de seguridad o manipulación. No creo que sea fácil, pero sí factible con la tecnología actual.

Tenemos que regular las compañías de telecomunicaciones, de redes sociales y de publicidad en cuestiones de seguridad o manipulación.

Para continuar con esta analogía, necesitamos una cooperación a nivel mundial, medios de vigilancia mutua y recíproca y hacer cumplir las leyes. ¿Cuánto tiempo llevará? A lo largo de los últimos cinco años, cada edición dominical del *Financial Times* ha anunciado casas a la venta en la Isla de Man o las Bahamas. El motivo detrás está muy claro: las Bahamas y la Isla de Man exigen la residencia presencial más del 50 % del tiempo para beneficiarse de las leyes que amparan a sus residentes. Esto demuestra, pues, las prácticas que los evasores de impuestos tienen que seguir. ¿Pero existen aplicaciones legales para evitarlas? ¿Cuánto tiempo nos llevará a nosotros? ¿Quince, veinte años? Por supuesto, necesitamos un detonante, y WannaCry fue significativo, pero no lo suficiente como para convertirse en el detonante necesario. No digo que necesitemos un equivalente al 11S, pero sí que necesitamos un detonante. Si ese detonante se produce, probablemente llegaremos al objetivo en 20 años.

La UE es importante, pero sus grandes estados miembros probablemente lo son incluso más: Alemania y Francia, así como Italia y España.

A modo de conclusión, ¿qué debe hacer Europa por ahora? Para empezar, en la Europa actual probablemente nos encontremos sin capacidad de influencia, ya que los grandes actores, China y los EE. UU., pueden actuar como solistas. En Europa no existe ese papel de voz cantante. Primero, necesitamos la mencionada

cooperación entre estados y empresas. La UE es importante, pero sus grandes estados miembros probablemente lo son incluso más, son los que remolcan al resto. Por grandes estados miembros me refiero a Alemania y Francia y, a nivel secundario, Italia y España. Respecto al Reino Unido, esperemos a ver qué ocurre con Brexit: el Reino Unido podría ser muy importante para la cooperación entre estados y empresas.

Segundo, tenemos que conseguir un efecto multiplicador a través de nuestros productos. Los EE. UU. tienen más personal en el sector que toda la industria de servicios junta, desde luego, y en cuestión de productos cuentan con el 80 % de todos los ingresos. Además, los últimos beneficiarios activos de estas compañías residen en los EE. UU. y están gobernados por normativas legales estadounidenses. Por tanto, no tenemos un equivalente al nivel de fortaleza que poseen los EE. UU. o China con Huawei o Qihoo. Necesitamos un factor multiplicador para nuestros productos.

Otra clave se halla en que, en Europa, tenemos que eliminar algunas dificultades que tenemos con los presupuestos. Si una empresa quiere ganar un concurso para dar servicio a una administración pública, probablemente tenga que luchar sobre el punto de partida del precio frente al que ofrecen compañías estadounidenses, que sabrán mejor que nosotros cómo ganar en este contexto. Así que necesitamos la cooperación. Hay una cláusula que se puede utilizar para la cooperación, una cláusula de seguridad nacional, pero se aplica muy raramente en Europa. Tenemos que luchar para que se emplee, porque debemos tener en cuenta que la causa fundamental de los ciberataques nace de la condición humana, que siempre estará presente. Como habrá software, habrá hackers. Esa condición humana es la avaricia, y la única manera de contrarrestarla es asociarla a otra condición humana: el miedo.

En Europa existe una cláusula de seguridad nacional que raramente se usa y que se puede emplear para la cooperación, y tenemos que luchar para hacerlo.