Los cuatro elementos de un ciberataque espectacular

Gonzalo Toca

Fotolia. Autor: dina_asileva

Los ataques cibernéticos más asombrosos y recientes tienen siempre cuatro grandes protagonistas: los países o las cibermafias; la falta de suficiente preparación por parte de Estados, empresas y particulares; la radical transformación del papel de los* hackers *(ayer románticos y hoy, normalmente, mercenarios); y la existencia de un mercado eficiente y bien estructurado de botines delictivos en el Internet oscuro.

En lo que va de año, hemos conocido que unos *hackers* sustrajeron 101 millones de dólares de la cuenta del Banco Central de Bangladés en la Reserva Federal estadounidense en Nueva York, que a un gigante tecnológico como Yahoo! le han robado datos privados de 500 millones de usuarios, que 12 entidades financieras de países emergentes sufrieron ataques cibernéticos coordinados y que la campaña de Hillary Clinton se ha visto seriamente afectada por el robo digital de información y el intento de acceder a los móviles de algunos líderes del Partido Demócrata.

Primer elemento: cíbermafias y Estados criminales

Los principales protagonistas son, por supuesto, sus autores. Aquí hablamos esencialmente de cibermafias –grupos organizados de criminales que atacan una red para secuestrar equipos o robar dinero o datos– y de las unidades de cíberseguridad de determinados Estados, enclavadas en ocasiones dentro del ejército o en el corazón de sus agencias de espionaje.

Marta Beltrán, profesora e investigadora de ciberseguridad de la universidad Rey Juan Carlos, recuerda que “el cibercrimen ya es el tercer tipo de delitos con el que los delincuentes obtienen más dinero en todo el mundo” y que sólo lo preceden “el tráfico de armas y la trata de personas”.

El grado de sofisticación de estos grupos es tal que, después de los éxitos obtenidos colándose en bancos, en la Agencia de Seguridad Nacional o con el Pentágono, Jorge López, experto en ciberseguridad y profesor de la Universidad Carlos III, cree que si disponen de los recursos, el talento y la paciencia necesarios, sólo es cuestión de tiempo que penetren en un sistema. Sea cual sea. “De hecho, nosotros partimos muchas veces de la premisa de que ya han entrado y de que tenemos que diseñar fórmulas para sacarlos”, afirma. Todos, sin excepción, somos y son vulnerables.

¿Cómo logran los delincuentes blindar su anonimato? Lo más común, advierte Marta Beltrán, es que estos criminales utilicen “sistemas y navegadores encriptados como, por ejemplo, la red Tor, Freenet o I2P”. Además, señala, suelen operar “desde decenas o centenares de equipos” (casi cualquier dispositivo conectado a la Red: ordenadores, teléfonos, televisiones y hasta

electrodomésticos inteligentes) que han sido previamente secuestrados sin que los usuarios se percaten.

La tercera capa de seguridad para borrar el rastro sobre la identidad, según la experta, es lanzar el ciberataque desde un ordenador *público* como el de un locutorio o desde uno conectado a una red con cientos de usuarios como las de un aeropuerto o un hotel.

Jorge López añade otro rasgo típico que también hace, muchas veces, casi imposible el rastreo. Se refiere a la externalización de muchos de los componentes que, bien ensamblados, permiten llevar a cabo un crimen cibernético. Todos esos eslabones –desde el diseño de un programa para robar datos de tarjetas hasta la compra de una flota de ordenadores secuestrados– son imprescindibles y, muchas veces, "sus autores ni saben ni quieren saber para qué se van a utilizar al final los productos que venden". Ellos son únicamente proveedores. Vender la dinamita a un terrorista no es lo mismo que cometer el atentado.

Seguramente, el caso más extremo es el de los llamados "muleros", que son los *hombres de paja* que guardan el dinero de los robos durante algunos minutos en sus cuentas en bancos de países de moral relajada o escasos de medios a cambio de no hacer preguntas y de cobrar una cantidad que no proviene del botín. Argumentarán que les ofrecieron ganar miles de euros por no hacer nada y que son malos tiempos, que cómo iban a negarse.

Como decíamos antes, no sólo hay cibermafias sino también Gobiernos y Estados que practican los ciberataques o los toleran en su suelo. Los que los practican, entre quienes destaca Rusia, suelen hacerlo, según Marta Beltrán, "por motivos estratégicos y geoestratégicos, porque resulta mucho más barato un ataque informático que un ataque militar o de una agencia de inteligencia y porque es un buen modo de dañar la reputación de los Estados y empresas que sufren los daños, que ven cómo les roban sus datos y se hunden sus acciones o cómo dejan de poder acceder a sus sistemas".

Un buen ejemplo ha sido la irrupción de los *hackers* presuntamente rusos en las elecciones presidenciales estadounidenses. La infiltración en los equipos del Partido Demócrata perseguía un triple objetivo: estratégico (erosionar la candidatura de Hillary Clinton, mucho más hostil con el Kremlin de Vladímir Putin, en beneficio de la mucho más favorable de Donald Trump), geoestratégico (perjudicar a la superpotencia rival) y reputacional (poner en evidencia los sistemas de cibervigilancia, teóricamente inexpugnables, de Estados Unidos no sólo ante el resto del mundo sino también ante sus preocupadísimos ciudadanos).

Segundo elemento: víctimas demasiado vulnerables

Otro componente de un ciberataque espectacular son las propias víctimas y la falta de suficiente preparación por parte de estados, empresas y particulares. Andrés Marín, profesor y director del Máster en Ciberseguridad de la Universidad Carlos III, subraya que, por ejemplo en España, existen instituciones como el instituto oficial Incibe y mecanismos como la Estrategia Nacional de Ciberseguridad.

Marta Beltrán añade que, también en España, se ha producido un fuerte avance en la prevención y persecución de la pornografía infantil en la Red y que, internacionalmente, la Interpol o las fuerzas de seguridad están realizando importantes esfuerzos para contar con efectivos adecuados y que existen centros de excelencia internacionales como el que posee la OTAN en Estonia, uno de los primeros países que fueron atacados cibernéticamente por Estados, en este caso, Rusia.

Dicho esto, advierte Beltrán, “es importante recordar que vamos con retraso en comparación con los países anglosajones, que internacionalmente no existe ni siquiera en Europa un marco armonizado de lo que se consideran delitos informáticos y de sus penas, que la Justicia española no tiene una sección dedicada en exclusiva a delitos informáticos, que muy pocos jueces, fiscales y abogados poseen la formación necesaria para entenderlos y que la calidad de las regulaciones, que se centran mucho en la privacidad y demasiado poco en la ciberseguridad, demuestra que los legisladores tampoco”.

Miles de particulares y empresas, señala Beltrán, tampoco tienen claro que “hay que proteger todos los dispositivos conectados a la Red y no sólo los móviles o los ordenadores”. Cisco calcula que, en 2020, habrá 50.000 millones de dispositivos conectados a Internet. Hablamos de televisores, coches, infraestructuras, ropa inteligente o electrodomésticos y de que, según la experta, “algunos de ellos ya están en el mercado y ni siquiera cuentan hoy con un triste antivirus”.

Jorge López lanza otra advertencia: “Muchos programas que se utilizan masivamente no tienen la protección necesaria”. Hay que recordar que nunca había sido tan fácil crear una aplicación móvil y que “la profesión de informático no está regulada –en parte por suerte, porque eso ha vuelto el entorno más competitivo y ha espoleado la innovación– y casi cualquiera con conocimientos avanzados [de computación] puede dedicarse a ella”. Ese *cualquiera* es posible que sepa crear una aplicación, pero no protegerla. Dejará a sus usuarios a merced de los piratas.

Además, apunta el experto de la Universidad Carlos III, “los especialistas en seguridad tenemos

que admitir que *los malos* van normalmente por delante y que es mucho más difícil proteger una infraestructura que atacarla". Y lo describe gráficamente afirmando que "no es lo mismo tener que encontrar un buen hueco para atacar un queso de gruyere que tener que defenderlo identificando y protegiendo todos los agujeros".

Tercer elemento: la transformación de los hackers

El tercer gran elemento de los ciberataques espectaculares es la radical transformación del papel de los *hackers* en las últimas tres décadas. A principios de los 90, recuerda Jorge López, los piratas "eran románticos, a veces activistas y casi siempre muy jóvenes, de entre 15 y 18 años, y su principal objetivo era demostrar lo hábiles que eran atacando sistemas sin quitarse el pijama". También había investigadores que, simplemente, querían comprobar cómo reaccionaban las ciberdefensas.

La situación ha cambiado gradualmente y hoy, afirma López, "existe la profesión de *hacker* y el crimen se ha convertido en uno de los servicios, perfectamente verticalizados, que ofrecen". Según Marta Beltrán, de la Universidad Rey Juan Carlos, "estos delincuentes son reclutados en grandes conferencias a las que acuden muchos expertos en seguridad de todo el mundo y

entre los que se encuentra una minoría que prefiere el riesgo y el dinero fácil aunque eso signifique cometer delitos".

Existe, según ella, también la figura de los expertos en ciberseguridad que alternan trabajos legales e ilegales a lo largo de sus carreras o que delinquen muy puntualmente para hacer frente a gastos inesperados. En una profesión tan competitiva tampoco debe descartarse la excitación que producen los retos.

Cuarto elemento: el Internet oscuro

El cuarto elemento de un cíber-ataque espectacular es, claramente, la llamada Internet oscura o *dark web*. Según Andrés Marín, profesor y director del Máster en Ciberseguridad de la Universidad Carlos III, ese espacio consiste en un lugar virtual "donde los ciberdelincuentes intentan hacer que se pierda el rastro de los delitos o del dinero robado y donde se ofrecen entre sí y se cierran las ventas de productos o datos obtenidos ilegalmente y de sistemas o recursos para llevar a cabo los ciberataques". Las transacciones se cierran habitualmente en bitcoins o en otros medios de pago virtuales que faciliten el anonimato.

Esa *dark web* forma parte de la llamado "Internet profundo", que no es otra que la que permite fuertes garantías de anonimato y sólo se puede consultar con navegadores o programas especializados como Tor, Freenet o I2P.

Marín recuerda que "existen muchos motivos legales para que los particulares se beneficien de una navegación anónima", que protegería mucho mejor su intimidad que la tradicional y la privacidad de algunas de sus transacciones financieras, y también "para unos servicios de inteligencia o fuerzas de seguridad que, lógicamente, no quieran dejar rastro". También pueden sacar provecho, por ejemplo, activistas o denunciantes de ilegalidades o abusos del poder que teman represalias.

Un aspecto que llama, especialmente, la atención del Internet oscuro es que, según Jorge López, experto en ciberseguridad y profesor de la universidad Carlos III, nos encontramos "ante un mercado perfectamente estructurado y eficiente donde los precios de cada producto ilegal están más o menos tasados y se deciden, normalmente, mediante subastas en foros anónimos".

Según él, los datos de unos 1.000 usuarios de Yahoo! pueden valer en torno a seis y 20 dólares y las claves de acceso y los números impresos de una tarjeta Visa Classic con fondos ronda los 150 dólares. La sofisticación ha llegado hasta tal punto que los criminales tienen formas establecidas de comprobar que la calidad de la mercancía está a la altura de lo prometido y se

venden también productos físicos –es decir, no virtuales– como fármacos y relojes falsos.

Recientemente, y tras la pantalla del Internet oscuro, ha empezado a fraguarse una siniestra relación de negocios entre los delincuentes cibernéticos y algunas empresas *de nombre respetable*. Marta Beltrán subraya que hasta hace poco “los productos robados más valorados de la *dark web* eran tarjetas de crédito, cuentas bancarias, números de la seguridad social o claves para suplantar la identidad de alguien en las redes sociales”.

Hoy, sin embargo, apunta, “lo más apreciado son los informes e historiales clínicos de los hospitales que se venden después a algunas aseguradoras y a empresas dedicadas a sectores o actividades que exigen una determinada condición de salud a los trabajadores que contratan”.

Es el último reducto de nuestra intimidad y resulta tan vulnerable como todo lo demás a las acciones de los ciberdelincuentes.

Fecha de creación
19 octubre, 2016