WHO AM I (2014), de Baran Bo Odar

BONNIE Y CLYDE

EN LA ERA DIGITAL

DE LA MISMA FORMA EN LA QUE EL DINERO PASÓ DE ENCONTRARSE EN LAS BÓVEDAS A ESTAR REGISTRADO EN BASES DE DATOS, LOS CRIMINALES INTERESADOS EN HURTARLO TAMBIÉN EVOLUCIONAN CON ROBOS DE PELÍCULA. EN ESTE PAÍS LOS LADRONES HAN EMPEZADO A CAMBIAR LOS CARROS DE ESCAPE POR CIBERMULAS, LOS PASAMONTAÑAS POR HERRAMIENTAS PARA ESCONDER SU DIRECCIÓN IP, Y LOS REVÓLVERES POR VIRUS INFORMÁTICOS. ASÍ SE ROBA UN BANCO EN COLOMBIA CON UN COMPUTADOR.

POR **RODRIGO RODRÍGUEZ**

La tarde del sábado 18 de enero de 2014, el personal de seguridad informática de un banco colombiano advirtió que los estaban robando. Una serie inusual de retiros y compras grandes, todas desde cuentas de su propio banco, se estaba dando a lo largo del país. Cuentas que no manejaban más de un par de millones de pesos al mes, o incluso menos, estaban retirando cantidades increíbles de dinero por ventanilla, mientras otras hacían compras de joyería, vehículos y hasta propiedades de finca raíz. Una persona en Bucaramanga fue a comprar dos relojes Rolex de veinticinco millones cada uno sin tener la apariencia de poder costearlos. Otro sujeto en Cúcuta insistió en comprar siete motos con su tarjeta débito; por su parte, el subintendente Julio César López, investigador criminal del Centro Cibernético Policial, recuerda que alguien compró un par de marranos, que no dejan ningún registro ante la Secretaría de Movilidad ni nada por el estilo, con tal de gastar sin dejar rastros un dinero que nadie se explicaba cómo había llegado a su cuenta.

Cuando el banco congeló los movimientos de las cuentas sospechosas y dio aviso a la policía, ya había perdido cerca de 7.500 millones de pesos en compras estrafalarias y retiros en cinco ciudades. Una ganga, si consideramos que los criminales detrás de este golpe tenían planeado llevarse un monto mucho mayor, 160.000 millones.

¿Cómo lo hicieron? Eso mismo se preguntaban en el banco.

★

SEÑOR CONDUCTOR

Se notifica a usted que presenta un comparendo por fotomulta, valor de la sanción $ 736.757 (setecientos treinta y seis mil setecientos cincuenta y siete pesos).
Se le anexa a descargar archivos adjuntos en el siguiente enlace: [...]. EVIDENCIAS: Fotos, lugar y fecha de la infracción.

Este es un correo que me llegó en 2016. La primera pista que tuve que se trataba de un engaño fue el hecho de que no tengo carro. La segunda, que el correo tenía como remitente la dirección "transito@colombiagov.com", que suena tan legítimo como unos tenis marca "Adimas". Una búsqueda en Google reveló que la ley que citaba como causa del comparendo ni siquiera existe.

La peor parte es que hay quienes caen en estos engaños. Copian el enlace, descargan un archivo, lo abren y isorpresa! En un mes tienen gastos por compras que no hicieron en sus tarjetas de crédito, sus cuentas bancarias están vacías y quizá hasta les hayan robado la identidad y secuestrado sus redes sociales. Un virus les daña la vida. Las víctimas son gente del común, los que todavía bajan música pirata y entran a Cuevana a ver películas en lugar de pagar Netflix y que cambian su contraseña una vez cada dos años. A ellos es a quienes les llegan correos de un

DURO DE MATAR 4.0 (2007), de Len Wiseman

CUANDO EL BANCO CONGELÓ LOS MOVIMIENTOS DE LAS CUENTAS SOSPECHOSAS Y DIO AVISO A LA POLICÍA, YA HABÍA PERDIDO CERCA DE 7.500 MILLONES DE PESOS EN COMPRAS ESTRAFALARIAS (RELOJES, MOTOS, MARRANOS) Y RETIROS EN CINCO CIUDADES.

príncipe nigeriano que quiere compartir su fortuna y la notificación de una herencia que les dejó un familiar que no sabían que existía. Las estafas por *email* y los virus troyanos son cotidianas. El delito informático ya es común, unos 556 millones de personas en el mundo son víctimas de él cada año (estafados, o al menos infectados por un virus); está tan presente como los asaltantes que se esconden en las esquinas más oscuras[1]. Pero en esos engaños solo caen los ciudadanos ordinarios, ¿cierto? Una institución que dedica millones de dólares al año en seguridad nunca caería en un truco tan barato; una institución como un banco.

Pero hace unos años, en Rusia, varios banqueros recibieron un correo como este:

Alexander, ¡buenas tardes!

Le envío nuestros datos bancarios para el contrato y los documentos para verificar la cantidad a depositar de 32.000.000 rublos y 6,00 kopeks, durante un año.

Sinceramente, Sergey Tsimonov
Teléfono: +7 (962) 7135296

En defensa de los banqueros, estos estafadores se esforzaron un poco más con sus correos. Parecían *emails* legítimos de clientes y reguladores financieros; en algunos casos los criminales lograron enviarlos desde direcciones de correo de colegas del propio banco. Los archivos que traían adjuntos tenían nombres como "ley federal". Como no había razón para sospechar, los empleados los descargaban. Así liberaron en sus computadores el virus de nombre Carbanak.

"En un caso como este, es un *malware* con características de *backdoor* –un programa que permite entrar y controlar un equipo sin tener que lidiar con sus protocolos de seguridad–. Para evitar la detección inicial, los atacantes pueden incluir malware que no hace nada excepto bajar el código que comprometerá el equipo". Roberto Martínez, con su acento mexicano, me explicó con esas palabras cómo funcionaba este virus. Es un investigador informático que trabaja para Kaspersky Lab, una de las firmas de seguridad más grandes del mundo que estudió el caso. "Luego este malware puede usar herramientas que le permitan capturar o ver lo que un usuario haga. Se conoce como *spyware*. En otros casos activan herramientas que permiten usar el acceso remoto de los equipos y controlarlos a distancia. A través de esta herramienta del sistema, los atacantes también pudieron pasar de un equipo a otro, y fueron descubriendo cómo tener acceso, desde dentro de algunas instituciones financieras, a los cajeros automáticos. En otras tenían que conocer cómo hacer transferencias a determinadas horas, por ciertos montos y de manera que no pudieran ser rastreados".

Kaspersky Lab entró a la ecuación en 2013, cuando un banco en Kiev se dio cuenta de que, a ciertas horas, uno de sus cajeros automáticos dispensaba dinero sin que nadie hubiera pulsado ni una tecla. En las cintas de seguridad se ve a un hombre de abrigo grueso y con una maleta, agachando la cabeza para no mostrar la cara, esperando a recoger el dinero que el cajero escupe sin razón. Los estaban robando y no tenían idea de cómo. Llamaron a Kaspersky. Descubrieron que 52 cajeros en Europa estaban infectados y que el mismo malware que había usado la banda criminal para manipularlos les había permitido robar de diversas maneras a docenas de instituciones, contando retiros en cajeros, transacciones a cuentas en el exterior e inflando el balance de cuentas en los propios bancos. Más de mil millones de dólares se esfumaron del sistema bancario mundial con la ayuda de Carbanak.

Nunca los capturaron.

Si los criminales que intentaron estafarme con un comparendo falso son el equivalente a ladrones comunes, a carteristas de transporte público, una banda como la de Carbanak son el equivalente al equipo de *La gran estafa*. El método de estos "ciberhampones" rusos es elegante, su planeación es de precisión suiza y su botín tiene tantos ceros que la banda ocupa el primer lugar entre los cibercriminales más exitosos de la historia. Desde hace años existe gente como ellos, que mete sus manos en los bolsillos virtuales de Wall Street. Entre junio y octubre de 1994, desde su computador de trabajo en San Petersburgo, el ingeniero Vladimir

VLADIMIR LEVIN robó diez millones de dólares a Citibank en 1994, en lo que el FBI llama el primer robo bancario digital.

[1] En 2016 se registraron 314.511 hurtos en todo el país. En contraste y según lo reportaron varios medios como *El Tiempo*, la firma de seguridad informática Digiware asegura que en Colombia se da un promedio de 542.465 ataques informáticos a diario. Casi la mitad de estos ataques van dirigidos al sector financiero.

DARIUS BOULDER se hizo pasar por un trabajador de soporte técnico para conectarse a la red de un banco y robar 1,2 millones de libras esterlinas.

Levin entró a la red de telecomunicaciones de Citibank y transfirió diez millones de dólares a cuentas de todo el mundo, desde Finlandia y Estados Unidos hasta Israel. Tenía gente lista para ir al banco y retirar los fondos en cada país. El FBI no tenía siquiera un equipo de crímenes informáticos en ese entonces, pero pudieron arrestar a Levin y a sus cómplices. Según el FBI, ese fue el primero, pero no el último de los "ciberasaltos" a bancos. A principios de 2016 un grupo criminal robó la información del Banco Central de Bangladesh y, haciéndose pasar como un oficial de esa entidad, mandaron más de treinta correos electrónicos a la Reserva Federal de los Estados Unidos –donde Bangladesh tiene miles de millones de dólares guardados– con solicitudes de transferencias de un total de mil millones de dólares a ONG falsas repartidas por todo el mundo; cuatro solicitudes fueron aprobadas, el equivalente a 81 millones de dólares, y hubieran logrado robar más si los criminales no hubieran escrito mal la palabra "foundation" –escribieron "fandation"– en uno de los correos, lo que obligó a una entidad a llamar a Bangladesh para pedir clarificación y así se descubrió el engaño. Mala suerte. Unos años antes, un ladrón entró por la puerta principal de Barclays Bank, en Londres; el personaje en cuestión, Darius Bolder, es un hombre con unos cuantos kilos de más y el pelo corto de alguien que ya predice su calvicie, la clase de persona que si se presenta como un "tipo de soporte técnico", no levantaría ninguna sospecha. Hizo exactamente eso: dijo que trabajaba en sistemas. Los empleados del banco le creyeron, lo llevaron a las oficinas de la parte trasera para que revisara los equipos y ahí conectó un dispositivo para controlar los computadores de manera remota –un switch KVM, aparato que no cuesta más de USD 400–. Sus cómplices usaron esa conexión para robar más de 1,2 millones de libras esterlinas al día siguiente. Fácil, simple y rápido, a veces sin necesitar más que un computador. Pasa desde Londres hasta Daca, y funciona con la misma efectividad tanto aquí como allá.

Sin muchas esperanzas de encontrar robos así en Colombia, me reuní con Fabio Herrera, director de la Unidad de Delitos Informáticos de la Fiscalía. Es un hombre grueso, con una voz calma que siempre suena entretenida sin importar el tema de discusión; parece hablar con más fascinación que preocupación sobre los crímenes digitales que suceden a diario en el país. Después de conversar un poco sobre el tema de este reportaje, le pregunté:

–¿Qué tanto se ve esto en Colombia?

–Realmente, esta tendencia no es nueva –respondió–. Siempre ha sucedido. Acá en Colombia a la mayoría de los bancos los atacan todos los días. Un banco promedio puede recibir entre 15 y 20 ataques diarios. Por eso ellos blindan su información con alta tecnología en seguridad y tienen grupos de respuesta a incidentes. Aunque muchas veces son las oportunidades las que hacen que sucedan estos hechos.

Entonces me cuenta sobre este sujeto...

★

Este sujeto era un programador. Su nombre no se puede revelar, tampoco el banco en el que trabajaba, porque en estos momentos es procesado por la justicia. Tal parece que se trataba de un sujeto con mucho tiempo libre, porque en 2013 se puso a pensar en esos centavos –no en los pesos, sino las fracciones de pesos– que dejan todas las transacciones. Tan inútiles para los clientes que ni siquiera salen en las facturas o los recibos de los cajeros, pero eso no significa que no existan. Este sujeto pensó que, quizá, si los pudiera juntar todos, podría llegar a reunir una cifra tangible. "Él tuvo acceso a desarrolladores de *software* del banco y colocó una rutina de código", cuenta Fabio. "De todas las transacciones que se hacían, los centavos los almacenaba en una cuenta aparte".

Tres meses después. Una de las personas encargadas del balance de cuentas en el banco

HACKERS (1995), de Iain Softley

UNA RUTINA DE CÓDIGO REDIRIGÍA TODOS LOS CENTAVOS DE CADA TRANSACCIÓN A UNA CUENTA EN BLANCO, SIN DATOS BIOGRÁFICOS NI NINGÚN OTRO TIPO DE INFORMACIÓN. "TENÍA MÁS DE 700 MILLONES DE PESOS, ¡A PARTIR DE CENTAVOS!".

notó que desde hacía un tiempo las transacciones no presentaban ningún centavo. Era muy inusual. El personal hizo un análisis y descubrieron que, desde hacía meses, esos centavos no aparecían en ninguna parte. Miraron en su plataforma y encontraron una rutina de código que redirigía toda fracción de peso a una cuenta en blanco, sin datos biográficos ni ningún otro tipo de información. "Tenía más de 700 millones de pesos, ¡a partir de centavos!". Cuando Fabio dice la cifra, lo hace con genuino asombro.

Lo más curioso es que el culpable nunca tocó el dinero ni nunca intentó gastarlo. Solo quería hacerse conocer en el "mundo de los *hackers*". Lo sabemos porque tiempo después de realizar el golpe publicó sus hazañas en un blog escondido en la web. No fue difícil atraparlo después de que la Fiscalía encontró su publicación.

★

Casi todas las personas entrevistadas para este artículo, pasando por oficiales de la Dijin y peritos de la Fiscalía y expertos en seguridad informática que trabajan para firmas privadas, coinciden en que cualquiera puede cometer un robo de este estilo. Cualquiera. Solo se necesita algo de dinero para financiar el "emprendimiento" y la gente adecuada para hacer el trabajo.

Incluso un periodista como yo, con algo de esfuerzo, podría dedicarse a robar bancos en docenas de formas diferentes. Podría, por ejemplo, robar los cajeros automáticos. Solo se necesita encontrar uno con sus puertos USB al descubierto e inyectarle un malware ruso barato, o desconectarlo de la red del banco y conectarlo a un computador que actúe como su centro de procesamiento para engañar al cajero y que escupa el dinero haciendo parecer todo una transacción legítima (todos métodos que Kaspersky Lab registró en su blog). También podría robar un banco a partir del cambio de divisas, como lo expone la firma de seguridad Acros Security: imagine cambiar un centavo de dólar a pesos a través de la plataforma *online* de un banco. Al precio actual, un centavo son 29,67 pesos, pero muchos bancos redondean esos decimales al peso más cercano. Se convierten en 30 pesos y termina ganando un peso extra. ¿Qué pasaría si cambiara centavo tras centavo, uno a uno, en miles de transacciones? Un simple programa podría hacer esta transacción automáticamente durante un día entero. Si la entidad bancaria no se da cuenta, en una hora alguien puede ganar $360.000 haciendo cien conversiones por segundo y, en un solo día, ganaría más de ocho millones de pesos. Si se encuentra un banco que no se haya protegido de esta trampa, es legal hacerlo. ¡Tantas posibilidades![2].

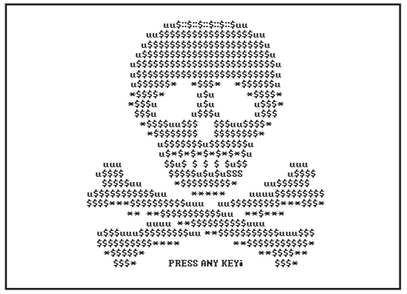
Sin embargo, por un momento, apuntemos a las grandes ligas. Robar millones de millones de pesos en un solo golpe, al mejor estilo de la banda Carbanak. ¿Qué se necesitaría?

El primer paso hacia el éxito en un golpe de este estilo es el *spear phishing*, la práctica de suplantar a una persona o entidad, generalmente vía email, para engañar al receptor. El spear viene de que, mientras hay phishing perezoso como el que me quiere hacer creer que tengo un comparendo pese a no tener carro, este recoge información sobre una persona y crea un correo o mensaje especializado para ella. Jaime Restrepo lo explica un poco mejor:

"Ahora todo el mundo quiere publicar su vida en redes sociales e internet. Solo con que se sepa el nombre de una persona ya puede hacer una búsqueda por fuentes abiertas y utilizar esa información para crear algo específico". Jaime es el fundador de DragonJAR, una firma de seguridad radicada en Manizales y experta en exponer las malas prácticas informáticas de este país, encontrando cajeros con sus puertos al descubierto y extrayendo información de celulares en sitios públicos. "Si le mando un mail diciendo '¡Te regalamos dos entradas VIP a una exhibición de perros de pedigrí!', ¿qué probabilidad tiene uno de que la persona abra ese correo y ejecute lo que está adentro? Una probabilidad bastante alta. Cuanta más información se tenga de la persona, más fácil armar algo a la medida; y mientras más personalizado sea el engaño, más fácil es que esa persona caiga".

Lo mejor sería contratar a un "profesional" que cobrará cerca de USD 200 por recopilar esa información, pero cualquiera podría intentarlo. Como dice Jaime, la gente ama publicar su vida en internet. Supongamos que decido rastrear a alguien que trabaje en un banco. A los dos minutos de buscar en Google puedo encontrar al gerente regional de uno. Su

[2] Pero cuando se trata del *ransomware* (un virus que encripta los archivos de un PC o una red y exige dinero por desencriptarlos, como el caso del virus WannaCry que atacó en mayo), no es la mejor opción. Los bancos usan sistemas muy cerrados, lo que impide que el virus se pueda expandir, y hacen copias de seguridad con regularidad, lo que les permite recuperar casi la totalidad de los archivos.



nombre, su foto y su cargo. A los cinco minutos, indagando en algunos archivos, tendría su número de cédula. A los diez minutos ya tendría abierto su Facebook y podría ver a dónde ha ido de vacaciones, las fotos del diploma de su especialización, saber que le encanta el fútbol y es fan del Real Madrid, ver las fotos de sus hijos y saber a qué colegio asisten, rastrear a su familia y a sus amigos del trabajo. Quizá ya lo hice. Todo esto es un poco aterrador y es muestra de que una persona que se dedique a esto podría llegar a conocer su vida en solo un día. Con su biografía digital a la mano, sería sencillo crear un correo al que no se pueda resistir.

Y cuando ese gerente abra ese correo, que es el tiquete de entrada al sistema, habrá un un virus en él. Es ahí cuando entra el programador (a veces mal llamados hackers).

"No cualquier persona que sabe de informática se presta para esto", dijo Julio César López, investigador criminal del Centro Cibernético Policial. Es un hombre cuyo porte grita "policía", con una voz seria y algo cortante, pero que a partir de mandar emoticones sonrientes por WhatsApp se vuelve un sujeto agradable. "Ellos saben que, por muy bien elaborado que les quede un trabajo, van a dejar rastros. *Cookies*, direcciones IP, cámaras y otros medios tecnológicos por los que se les podría rastrear".

Según López, en algunos casos personas de otras nacionalidades se han prestado para estos delitos. En efecto, un cibercriminal puede trabajar desde cualquier lugar, así que las fronteras no son excusa para no contratarlos. Buscando un poco, encontré la página de un mercenario informático en la *deep web*, en un directorio que también ofrecía sitios para comprar información de partidos de fútbol arreglados y pasaportes americanos "reales". El hacker en cuestión dice ser un hombre de Europa oriental que hace cualquier trabajo por dinero. Ante la solicitud de entrevistarlo para este artículo, respondió a través de un mensaje encriptado:

Sin dinero, no hablo.

Le expliqué que, por cuestión de principios periodísticos y por el hecho de que mi sueldo no me da para cubrir ni una parte de sus precios (lo mínimo que cobra, por los trabajos más sencillos, son 200 euros), no podía pagarle. Respondió una sola cosa:

¡Piérdete!

Mis intentos de contactar a otros mercenarios, ofrecen servicios como desarrollar malware personalizado[3], atacar sitios web y robar contraseñas de todo tipo de correos, fueron igual de inútiles. Pero según la Dijin, la mayor parte de los mercenarios no cobran una cuota fija, sino un porcentaje de las ganancias de acuerdo con el trabajo, incluso si involucra robar un banco. Tienen que ser personas pacientes, pues un trabajo como este puede tardar meses o años, vigilando sin pausa el funcionamiento del software del banco, esperando el momento para saltar de un computador a otro sin ser detectado, buscando la oportunidad para mover el dinero o poner unos cuantos ceros de más en ciertas cuentas.

Son las cuentas que les pertenecen a las llamadas "cibermulas". Hay reclutadores encargados de encontrar a estas personas dispuestas a prestar su cuenta para poner en ellas el dinero robado. Los agentes de la Dijin dicen que por lo general se trata de gente normal y de estratos bajos que es reclutada en lugares públicos con la promesa de un porcentaje del botín que reclaman. Si les consignan diez millones, pueden quedarse con mínimo cien mil pesos y máximo un millón. Mal pagados, a veces amenazados por sicarios contratados para hacerlos "cooperar" (en crímenes de este tipo en Colombia, las autoridades han sospechado de la participación de la mismísima oficina de Envigado) y casi siempre los primeros que caen cuando la policía empieza a investigar.

Por obvias razones, no fui a buscar reclutadores de la oficina de Envigado. Esa historia no terminaría bien. Habrá que tomarle la palabra a la policía.

Después de todo eso, solo falta encontrar a esa persona que sabe la respuesta a la pregunta "¿cómo esconder cientos, miles de millones que son buscados por las autoridades?". Un ingeniero financiero puede hacer esa gracia; una persona que entienda cómo perder el rastro del dinero, lavarlo y esconderlo. Algunas de las técnicas que usan son mandar los fondos a cuentas en el extranjero para luego retirarlos allá, o convertirlos a monedas digitales como bitcóins. Esta se envía a un *pool*, un sistema que mezcla el dinero de un usuario con el de otra gente y luego lo devuelve de a poco, en cuotas, lo que hace imposible decir de dónde viene o a dónde va a parar.

Y así de fácil resulta robar un banco. Y esta es tan solo una manera de hacerlo.

★

"Hace unos años se identificó que se había vulnerado un par de ATM", cuenta Fabio, refiriéndose a los tiempos remotos del año 2012. "Les habían instalado un *malware*, un virus. Eran cajeros de un centro comercial, aquí en el país, en los que las transacciones eran de mil, dos mil millones al día. Las personas que alimentaban el cajero le habían instalado una memoria USB. La dejaban un mes y a la siguiente alimentación del cajero la retiraban. Lo que hacía era capturar los archivos de las transacciones".

La información que recopilaban en la memoria USB –que incluía números de tarjeta, números de cuenta, claves de acceso y montos de las transacciones– estaba encriptada, probablemente con un cifrado estándar de 256 bits que la hace casi impenetrable. Tiene 2^{256} posibles contraseñas. Esa cifra equivale a escribir el número 116 en una hoja y luego poner 75 ceros a su derecha. Una de las computadoras más potentes del planeta tardaría más de nueve años en descifrar la contraseña. Por suerte para los delincuentes, tenían las llaves para desencriptar toda la información: el líder de la banda las había hurtado en Europa, en la misma fábrica que hacía los módulos de los cajeros. Era un criminal en posesión de la llave de docenas de cofres de tesoro.

Su racha duró ocho meses. El personal del banco se dio cuenta de que, en un video de una cámara de seguridad del cajero, se podía ver que las personas que lo alimentaban insertaban una USB en él. La policía intervino y no pasó mucho tiempo antes de que capturaran a los catorce integrantes de la banda, que también incluía a personas que hacían mantenimiento a los ATM. En las casas de los sospechosos se encontraron pequeñas máquinas con las que fabricaban tarjetas clonadas (habían instalado un dispositivo en los cajeros para esto también), que troquelaban para que parecieran reales. Ya para ese entonces habían realizado transacciones por más de 1.400 millones de pesos. La mayor parte de ese dinero se perdió para siempre en cuentas en el extranjero.

–Ya lo habían hecho en Ecuador, en Perú, en Bolivia y en Venezuela –cuenta Fabio–. En todos estos países el jefe de la banda robó, más o menos, unos siete millones de dólares.

–¿Y esta persona era de origen europeo? –le pregunto.

–No, colombiano –responde tras una carcajada–. El que estaba haciendo todo esto era colombiano.

★

Hola, Rodrigo

Se revisó el tema internamente y consideramos no conveniente proporcionar este tipo de información.

Esa fue la única respuesta directa que obtuve de un banco para este reportaje. Llegó en un correo de BBVA, tras semanas de insistir. Muchos de los otros bancos que hay en el país optaron por el silencio.

Asobancaria, la asociación que reúne a los 24 bancos nacionales y extranjeros que operan

WHO AM I (2014), una película alemana dirigida por Baran bo Odar.

[3] También puede comprarse en mercados negros digitales donde se consiguen virus como Zeus (uno de los más versátiles y peligrosos de los últimos tiempos), ataques de DDoS y listas de millones de correos en Colombia para *phishing*. "Entras a la *deep web*, buscas un *malware* que haga determinada función y lo pagas con bitcóins", es como lo resume Fabio Herrera, de la Fiscalía.

en Colombia, sí accedió a hablar. No dijeron mucho y respondieron con cierto recelo:

"En general, cuando se trata de seguridad y bancos, hay que tener mucho cuidado con qué se transmite, porque eso es un tema de confianza", dijo Gina Pardo, su directora de gestión operativa. "Cuando ocurren casos de riesgo operativo, eso genera pánico en la gente".

Aunque este "pánico financiero" nunca se ha dado de una manera considerable debido a un crimen informático, los bancos prefieren callar. Ya en el año 2000 el experto en seguridad informática Michael Higgins le contaba a la revista *Forbes* sobre cómo los bancos americanos reportaban sus pérdidas por hackeos, que podían ascender a cientos de millones de dólares, como "errores de contabilidad" para evitar la mala publicidad y no perder la confianza de los cuentahabientes. Esto no solo pasa en Estados Unidos. En Colombia, donde las entidades privadas no tienen la obligación legal de reportar estos delitos, fuentes relacionadas con el sector bancario confirmaron que, en ciertas ocasiones, los bancos prefieren callar este tipo de actos, bien sea para evitar la mala prensa o para no saturar el sistema judicial con investigaciones que no llegarán a ningún lado. "Realmente, la probabilidad de encontrar a los culpables de estos crímenes es muy baja", fue la opinión de Fabio Herrera al respecto.

No es como si las sumas que se roban estos cibercriminales sean suficientes para desestabilizar la banca. Eso aseguran las fuentes. ¿Cien millones, mil millones de pesos? Difícilmente harán quebrar a las instituciones bancarias más poderosas del país, cuyo valor combinado es de más de 22.000 millones de dólares. Pero como es mejor prevenir que lamentar, la Superintendencia Financiera obliga a los bancos a cumplir con ciertos estándares de seguridad (norma ISO 27000).

El problema es que ninguna defensa es suficiente cuando el ladrón tiene las llaves de la bóveda, cuando tiene acceso a los sistemas de los bancos sin necesidad de hackear nada. Es lo que pasa casi siempre. Tomemos por ejemplo a Nilton Galeano, un criminal sin talento. Digo esto porque, de alguna manera, durante su gran debut en el mundo criminal, logró hacerlo todo mal: uno no olvida borrar sus rastros digitales; uno no comete el robo usando el correo y la cuenta de usuario que está registrado a su nombre; y uno no transfiere el dinero robado a la cuenta de banco propia, a la del hermano y a la de la esposa –exesposa, pues el juez le preguntó en su juicio "¿estado civil?", y Nilton respondió a secas "en proceso de divorcio", y con razón–. Hizo el equivalente digital a haber asesinado a alguien y luego estornudar diez veces sobre el cadáver. Aun así, este "novato" de cincuenta años solo tuvo que conspirar con un par de empleados del banco para tener acceso al sistema. Sin usar ni *malware*, ni *backdoors*, ni *exploits*, ni *spyware*, ni ningún otro término raro en inglés, Nilton hurtó 3.365 millones de pesos de varias cuentas usando el sistema de pagos por internet de BBVA.

Cuando lo atraparon, unos cuantos días después, su defensa en la corte fue sencilla: "Yo no lo hice porque no sabría cómo".

–Señor Nilton, usted ha manifestado que no es diestro en el tema de computación –le señaló el fiscal durante el juicio.

–No, señor –respondió Nilton–. Manejo solo lo básico, básico. Manejo los discos flexibles, de esos grandotes. ¡Y ahora estos muchachos manejan unas cosas a la velocidad del sonido!

★

En los viejos tiempos, robar a lo grande era algo más o menos así:

César Agudelo[4] se dio cuenta de que los estaban robando de golpe. Literalmente. A las seis de la mañana, el 15 de agosto de 2009 en una calle de Cali, un vehículo embistió al carro de valores de la compañía de seguridad G4S en el que iban él y dos de sus compañeros. La buseta arremetió desde un costado, golpeándolos en la parte delantera y cerrándoles el paso. No se habían detenido del todo cuando César reparó, desde el asiento del pasajero, que por la calle se acercaban varias personas armadas; las puertas de la buseta se abrieron y descendió otro grupo de hombres, cargando revólveres desgastados y fusiles AK-47, que empezaron a rodear el camión. "Nos van a robar", pensó César, mientras informaba por radio lo que pasaba, con la esperanza de que llegara apoyo pronto. Los ladrones abrieron fuego contra el carro, pero el blindaje clase 5 y los vidrios de 7 cm de grosor resistieron. "¡Hijueputas, ya los tenemos!", gritaban los criminales mientras disparaban. "¡Bájense!".

Fue entonces cuando sacaron los bidones. Varios hombres se encaramaron al carro

[4] No es su verdadero nombre.

SWORDFISH (2001), de Dominic Sena

"HACE UNOS AÑOS SE VULNERARON UN PAR DE CAJEROS AUTOMÁTICOS. LES HABÍAN INSTALADO UN VIRUS. LAS PERSONAS QUE ALIMENTABAN EL CAJERO LE HABÍAN INSTALADO UNA MEMORIA USB. LA DEJABAN UN MES Y A LA SIGUIENTE ALIMENTACIÓN DEL CAJERO LA RETIRABAN".

THE GIRL WITH THE DRAGON TATTOO (2011), de David Fincher.

"TAMPOCO HUBO TRANSFERENCIAS DE DINERO, SINO ALGO UN POCO MÁS INGENIOSO", CUENTA EL SUBINTENDENTE LÓPEZ. "POR EJEMPLO, A UNA CUENTA QUE TENÍA $10.000, LE COLOCARON TRES CEROS MÁS, O QUIZÁ CUATRO".

y empezaron a regar su contenido. Gasolina. Encendieron el combustible y empezó a arder, a filtrarse por las ranuras de las puertas. Entre las quemaduras y el pánico y la asfixia, cada uno de los tres tripulantes toma una decisión: el hombre que va en la bóveda (que se estima llevaba unos mil millones de pesos) abre las puertas para escapar al fuego; el conductor reacciona y pone marcha atrás, a ciegas, estrellando el camión contra un muro de ladrillo y bloqueando el acceso a la bóveda; y César, asustado, abre la puerta del pasajero y salta fuera del vehículo, rodando en el asfalto.

–Cuando salí, uno de los criminales empezó a dispararme con un AK-47 –me contó César–. Yo lo que hago es defenderme en el piso, dando vueltas, sintiendo las esquirlas rebotar a mi alrededor. Una bala me alcanzó a rozar en la pierna.

–¿Y luego qué pasó?

–El tipo estaba tan ensañado conmigo que se descuidó. Entonces un compañero mío que llegó al lugar lo alineó y le disparó. Los tipos llevaban chalecos antibala, pero igual arrancó a correr. Yo quedé ahí, aturdido.

–¡*Wow*! –dije, sin hacer ningún esfuerzo por disimular mi fascinación.

Los ladrones se retiraron en mitad de una balacera contra el personal de apoyo de G4S y las fuerzas de la policía que acababan de llegar. No pudieron robar nada. Nunca los capturaron.

¡Esos eran robos! Se necesitaban tanto preparación como cojones para lograr algo así. Sin la gente adecuada, sin las armas, explosivos, chalecos, dispositivos de comunicación, carros para la fuga y hasta sobornos para conseguir la información por adelantado, eran planes condenados a fallar. Eran crímenes mórbidos y fascinantes, la clase de historias que, inconsciente pero expectante, la gente siempre busca en los periódicos. Pero ya pueden irse despidiendo de relatos como este. Esos son ladrones del pasado, cada día más escasos. Las historias de ahora cambiaron las balas por líneas de código, los bangs por clics. En vez del cinematográfico asalto a un carro de valores, tenemos casos como el del banco colombiano con el que empieza este artículo. Los responsables gastaron más de siete mil millones de pesos en un día y desaparecieron gran parte de ese dinero en cuentas en el extranjero.

Entonces, ¿cómo lo hicieron?

Respuesta: de la manera más fácil y aburrida posible.

Para robar uno de los bancos más grandes del país solo tuvieron que sobornar a alguien: un trabajador de la firma que proveía servicios tecnológicos al banco. Ya con las llaves del sistema no tuvieron que hackear nada, solo abrirse caminos entre las cuentas de usuario hasta conseguir los permisos para controlar el dinero de las cuentas.

"Tampoco hubo transferencias de dinero, sino algo un poco más ingenioso", cuenta el subintendente López. "Por ejemplo, a una cuenta que tenía $10.000, le colocaron tres ceros más, o quizá cuatro. En algunos casos, para las cuentas que no pertenecían a gente que moviera mucho dinero, tomaron la precaución de colocar solo $9'900.000, para no ser detectados por controles que los bancos hacen, estipulados por el SARLAFT (Sistema de Administración del Riesgo de Lavado de Activos y de la Financiación del Terrorismo), que controlan las transacciones superiores a diez millones de pesos". Los criminales hicieron esto en 356 cuentas, pertenecientes a particulares o fundaciones –algunas reales, otras inventadas por ellos mismos–, todas de gente reclutada para la estafa.

Estuvieron planeando el robo durante un año. Un año de conseguir los accesos a los computadores de la red del banco para mover los dineros, de convencer a funcionarios de sumarse a la estafa, de reclutar personas que prestaran sus cuentas para el fraude –a veces las amenazaban o se aprovechaban de personas con problemas mentales– y de montar fundaciones de papel con cuentas en el banco que pudieran insuflar. En enero todo estaba listo. En menos de 48 horas inyectaron 160.000 millones de pesos en las cuentas. Sabían que tenían que retirar el dinero antes de que los libros digitales contables del banco se sincronizaran y delataran sus movimientos. Así es como terminan por realizarse gran cantidad de retiros sospechosos en Cúcuta, Cali, Medellín, Calarcá y Bogotá en la tarde del 18 de enero de 2014. Gastaron dinero que se había creado casi por arte de magia, que nació de poner un cero de más en una computadora, y lo convirtieron en billetes, joyas, motos y marranos.

–Al final, todo fue posible por lo que los ingenieros llaman un error en la capa 8 –dice el subintendente López.

–¿Cuál es la capa 8?

–El usuario.

Una manzana podrida entre la gente que trabajaba con el banco le costó a ese banco 7.500 millones. No hay antivirus para eso. Es una vulnerabilidad que han sabido explotar los criminales, desde las bandas internacionales hasta los "genios informáticos" como Nilton Galeano, y que ha traído el robo bancario en Colombia al siglo XXI. Es un crimen tan fácil y aburrido como presionar ENTER, pero mucho más lucrativo de lo que podrá lograr cualquier ladrón armado con un AK-47. ■