España, entre los países con más usuarios atacados por los troyanos bancarios

Malware bancario: el peligro que no cesa

El *malware* bancario es uno de los grandes quebraderos de cabeza para los fabricantes de seguridad. Los troyanos bancarios, a los que se han unido las aplicaciones bancarias falsas, han sido, desde hace años, uno de los *malware* con más tirón entre los maleantes de la red. Diseñados para robar credenciales y datos bancarios, el incremento del uso de la banca *online* y de las aplicaciones bancarias móviles había disparado sus ataques. Un ascenso que continuó el pasado año, con el confinamiento y las medidas de distanciamiento posteriores, que hicieron crecer el número de usuarios. España, por la dimensión de su banca, la alta penetración de la telefonía y el uso creciente de las aplicaciones bancarias, es objetivo preferido de los maleantes.

Marilés de Pedro

España, en cabeza

Según un estudio de Kaspersky, España se situó el pasado año en tercer lugar en el ranking de países del mundo con mayor porcentaje de usuarios atacados por los troyanos bancarios. Un *malware* que se constituye en la principal amenaza para las plataformas móviles. Entre los más destacados en España, figura el ya "celebre" Ginp (que suplantó la aplicación de 7 entidades españolas) o también Mandrake, que acampó en 2019, a los que se sumaron nombres en 2020 como Cebruser o Knobot.

El incremento de usuarios que hace uso de la banca móvil es un excelente caldo de cultivo para que los *hackers* cocinen sus amenazas. Según el informe DESI de la Comisión Europea, seis de cada diez españoles utilizaron la banca digital en 2020, siendo la consulta de saldo, las transferencias y el pago de facturas las principales operaciones. Un dato, muy superior a algunos países de nuestro entorno, a pesar de que cuenten con una población superior a la española. "Los ciberdelincuentes han adaptado rápidamente sus herramientas y técnicas de *malware* para aprovecharse de esta evolución", explica Román Vargas, consultor de ciberseguridad en Cisco España.

La transformación digital de la banca ha provocado el cierre de una gran parte de las oficinas físicas y el fomento del uso de la banca *online* por parte de sus clientes. "Se han incorporado, además, nuevos clientes; todos ellos nativos digitales que entienden su comunicación externa y su conexión al comercio a través de las aplicaciones", explica Jorge Pages, ingeniero preventa de WatchGuard. "Crece el número de troyanos porque también lo ha hecho el número de clientes que pueden recibir esos troyanos; lo que confirma que es un enorme "negocio".

La dimensión y el peso que tiene la banca española, con su enorme presencia en Hispanoamérica y en otras zonas mundiales, ejerce también un enorme atractivo para los *hackers*. "Influye el tamaño de nuestros bancos y las regiones del mundo en las que operan. Son bancos que cuentan con más usuarios de habla hispana, además de tener presencia en mercados tan potentes como EEUU, Brasil o Turquía", recuerda Borja Pérez, *country manager* de Stormshield Iberia,

que puntualiza que, si son un objetivo, es por el exceso de confianza que tienen los usuarios. "Al integrar tantos clientes, esos usuarios se convierten en un objetivo muy atractivo".

> "El *malware* relacionado con el robo de datos bancarios es uno de los más rentables para los cibercriminales"

Una banca, que señala Sergio Martínez, director general de SonicWall en España y Portugal, invierte muchas decenas de millones de euros en ciberseguridad. "Esto puede hacernos pensar que estamos protegidos, pero no es así", opina. "El usuario es el eslabón débil de la cadena. La covid-19 nos ha convertido a todos en usuarios remotos de la banca y quizás no estamos tan preparados como creíamos para el uso de determinados servicios *online*".

La penetración en España de los teléfonos móviles, que alcanza cerca del 90 %, es otro de los factores que contribuye a que nuestro país se sitúe en este pódium. "El *malware* relacionado con el robo de datos bancarios es uno de los más rentables para los cibercriminales", recuerda Iván Mateos, *sales engineer* de Sophos Iberia. Un parque móvil que, como insiste Mario García, director general de Check Point en España y Portugal, apenas cuenta con medidas de seguridad para proteger los datos que almacena. "No es de extrañar, por tanto, que España ocupe uno de los primeros puestos entre los países más afectados por esta ciberamenaza".

¿De qué técnicas se valen?

Hay dos tipos principales de *malware* bancario: los troyanos y las aplicaciones bancarias falsas. Ambos persiguen el mismo objetivo: robar las credenciales para acceder a las cuentas de sus víctimas. Para lograrlo, utilizan el *phishing* y formularios de acceso falsos para robar las contraseñas. A veces también requieren controlar los dispositivos móviles de las víctimas para interceptar incluso los mensajes de confirmación SMS.

En el uso del *phishing*, los maleantes utilizan ganchos bastante convincentes en forma de comunicaciones oficiales, avisos de entrega de paquetes, burofaxes *online* y multas suplantando empresas de todo tipo y organismos oficiales, como Ministerios o incluso a la Guardia Civil. "Mediante un enlace o un fichero adjunto consiguen que la víctima ejecute un archivo malicioso que termina descargando y ejecutando en el sistema un troyano bancario encargado de robar las credenciales de acceso a la banca *online* cada vez que el usuario accede a través de su navegador", explica Josep Albors, responsable de concienciación e investigación de Eset España.

Otra de las técnicas más utilizada durante los últimos meses es el envío de mensajes SMS haciéndose pasar por empresas de transporte o, directamente, mostrando alertas falsas al visitar ciertas webs. "A continuación, se solicita la descarga de una aplicación fraudulenta que es la responsable de robar las credenciales bancarias y de interceptar los mensajes SMS enviados desde nuestra entidad bancaria como doble factor de autenticación para verificar la realización de transferencias de dinero", continúa Albors.

Otro camino es a través de una aplicación, aparentemente legal, que se exhibe en alguno de los populares *marketplaces*. Una aplicación, que cuenta con una funcionalidad legítima, pero que también tiene la capacidad de descargar e instalar aplicaciones adicionales cuando los atacantes le indiquen que lo haga. "Cuando aumenta la base de usuarios instalada, filtran los objetivos que consideran relevantes para recibir el *malware* bancario. Con las víctimas seleccionadas, indican a la aplicación que instale una actualización maliciosa que dibuja superposiciones sobre las aplicaciones con fines de *phishing*. Algunos troyanos bancarios también incluyen capacidades de acceso remoto para extender el robo de información más allá de las credenciales bancarias", explica Bogdan Botezatu, director de *threat research and reporting* en Bitdefender.

No falta, si se trata de ataques dirigidos a las empresas, el BEC (*Busines Email Compromise*). "Se suplanta la identidad de alguna persona relevante de una compañía, por ejemplo, el CEO, para efectuar ataques que puedan tener una implicación económica: desde solicitar una transferencia a una cuenta externa hasta robar credenciales de acceso a sistemas bancarios", explica José de la Cruz, director técnico de Trend Micro Iberia. Estos ataques, que consisten en un correo electrónico enviado en nombre de alguien relevante solicitando una transferencia u otra acción con trasfondo económico, pueden afectar también a la cadena de suministro de las compañías afectadas.

Mario Garcia recuerda que las técnicas utilizadas por los cibercriminales cada vez evolucionan más y son más efectivas. Los datos del indice global de amenazas de Check Point indican que Emotet, uno

¿Qué errores comenten los usuarios?

Como ya es tradicional, el eslabón más débil es el usuario. Pero, ¿qué errores comete? "El más habitual es usar la misma contraseña para los sistemas bancarios que la que utiliza para cientos de sitios similares (*blogs*, foros, *apps*, juegos...)", arranca Raúl Tejeda, *finance SE* en Fortinet. Por tanto, si se compromete una contraseña, lo más probable es que después esté comprometida la aplicación bancaria. "Lo recomendable es tener varias contraseñas e irlas cambiando a lo largo del tiempo, una práctica muy saludable pero poco practicada por los usuarios". El otro error común "es registrarse con el mismo correo electrónico en multitud de *newsletters*, juegos y aplicaciones de ocio de dudosa reputación".

Todavía existen muchos usuarios que no son capaces de identificar comunicaciones falsas procedentes de supuestas entidades bancarias y que caen en la trampa de un correo *phising*, un SMS fraudulento o cualquier otra amenaza, alerta Jorge Pages. Un problema que, lógicamente, está directamente relacionado con la falta de formación. "Sería recomendable que las entidades financieras definieran una estrategia de comunicación al usuario robusta en la que se abandonen canales inseguros como el correo electrónico y se le informe claramente de que estos canales nunca serán utilizados para solicitarles ningún tipo de acción o información", recomienda. "Además deberían potenciarse campañas de concienciación al ciudadano por parte de los gobiernos e incluir estos contenidos en los distintos currículums escolares".

Borja Pérez incide en la formación que deben recibir los equipos de marketing y comunicación por parte de la división de fraude y de ciberseguridad de las entidades bancarias para que "en las comunicaciones enviadas a los clientes no se les solicite o no se les pida realizar acciones como pulsar botones o abrir cierto tipo de enlaces".

En el caso del uso del dispositivo móvil, Iván Mateos recuerda que éste otorga al usuario una "falsa sensación de privacidad" que en muchas ocasiones le lleva a ser excesivamente confiado a la hora de utilizar las aplicaciones de un dispositivo, de conceder permisos o de acceder a su información confidencial. "Por otro lado, suele ser fácilmente engañado, por ejemplo, al recibir un SMS o un *email* con el aviso de un problema y en el que se les anima a solucionarlo simplemente haciendo *click* en un enlace".

La mayoría de las víctimas no revisa si el correo o el mensaje procede realmente de quién dice ser. "Tampoco se suele revisar si el fichero tiene el formato que debe tener (pulsando sobre ejecutables que supuestamente son archivos ofimáticos) y, además, se cae en la trampa de habilitar la ejecución del contenido a petición de los delincuentes cuando abren un archivo de Word o Excel que contienen macros maliciosas", explica Josep Albors.

de los troyanos bancarios más populares, ha sido el top *malware* que más ha afectado a las empresas españolas en el último trimestre del pasado año, llegando incluso a impactar a más del 15 % de las compañías.

Los troyanos bancarios son amenazas muy sofisticadas en términos de arquitectura y funcionalidad

Los troyanos bancarios son amenazas muy sofisticadas en términos de arquitectura y funcionalidad. "Han ido perfeccionando sus técnicas de *overlaying* para lograr que el *malware* superponga una pantalla de *phishing* al acceder a la aplicación en el dispositivo comprometido. Tienen un mayor alcance potencial que las aplicaciones falsas", apunta Román Vargas. El experto de Cisco señala que un ejemplo destacado es Trickbot, uno de los troyanos bancarios más sofisticados. Descubierto por primera vez en 2016, Trickbot es altamente modular. "Puede adaptarse a diferentes entornos con la ayuda de sus diversos módulos, como los dirigidos a atacar Windows 10 y a los sistemas de punto de venta (POS). Trickbot suele enviarse a través de un correo electrónico de *spam* que contiene un documento malicioso o una URL maliciosa. No sólo funciona como un troyano independiente, también se utiliza comúnmente como inyector de otros programas maliciosos como el *ransomware* Ryuk".

El director general de Sonicwall recuerda que no hay que olvidar a quién nos enfrentamos: organizaciones criminales opacas, con sede muchas veces en países de difícil acceso a la Interpol, como Nigeria, Rusia, Brasil, etc. "El *malware* es cada vez más evasivo y difícil de detectar, y estamos cada vez más expuestos".

A juicio de Jorge Pages, estas técnicas, en esencia, no han variado. "Quizás se hayan sofisticado y han podido ampliar sus objetivos, pero de base, siguen siendo las mismas rutinas", opina. El punto importante, puntualiza, es que el negocio del troyano se ha industrializado. "Se ha convertido en un SaaS: es un servicio que se puede contratar y que, además, ofrece garantías de éxito de las campañas". Pages distingue dos tipos de objetivos. Por un lado, el doméstico, que alcanza una dimensión más global. "Es un ataque refinado. No son burdos, sino que están bien escritos y preparados". Por otro, el corporativo, que se dirige al empleado. "Es un ataque dirigido", especifica. "Para ello, se ha tenido que llevar a cabo un estudio previo de la víctima y de su entorno".

Los mayores agujeros empresariales

La explosión del teletrabajo que ha extendido, aun más, el perímetro, ya "excedido", ha dejado en manos de los propios usuarios, alerta Sergio Martínez, la protección de su propio *endpoint*. "Esto está siendo fatal", denuncia. "Sin duda, el *endpoint* (y los credenciales

del usuario) son el punto débil a proteger". Según los datos que maneja el fabricante, el pasado 2020 cayó en un 40 % la cantidad de *malware* detectado mientras que crecían en un 19 % los intentos de intrusión y en más de un 20 % los ataques de *ransomware*. La construcción precipitada de accesos remotos, con políticas de acceso muy permisivas o sin autenticación multifactor, el control de usuarios, pero no de dispositivos; y la falta de mapeado de los usuarios *versus* los recursos a los que debe acceder, señalan otras áreas de riesgo, a juicio del director general de SonicWall.

Raúl Tejeda señala que los mayores agujeros están en aplicaciones no tan conocidas "como pueden ser *blogs*, entradas de personal externo, *contractors*, páginas de colaboración o páginas de preproducción". Además, recuerda que el vector del correo electrónico también afecta a los usuarios corporativos. "Aunque se pare el 90 % de los ataques, hay cientos, cada día, dirigidos a los dominios bancarios más conocidos".

El correo electrónico sigue siendo la principal puerta de entrada de *phising* y *malware* en el ámbito corporativo. De hecho, España presenta el porcentaje más alto de incidentes de seguridad en Europa como resultado de abrir un correo no deseado: un 54 % frente a la media europea que se sitúa en el 41 %. "Los correos maliciosos que ocultan estos troyanos suelen contener un sentido de "urgencia", como es el caso de facturas falsas que solicitan una comprobación rápida muchas veces suplantando identidades, para lograr que el usuario descargue el *malware* capaz de infectar teléfonos y PC", advierte el consultor de ciberseguridad en Cisco España.

Una puerta abierta que, como señala el *sales engineer* de Sophos Iberia, ya no depende tanto de los fallos en los sistemas de seguridad que pueda tener la empresa, si no de los propios trabajadores. "Es esencial que utilicen contraseñas robustas y, siempre que sea posible, sistemas de doble factor (2FA) para aumentar la seguridad de sus accesos. Así mismo, deben tener las mismas precauciones que cuando se encuentran fuera de la red empresarial, desconfiar de solicitudes y mensajes electrónicos sospechosos o no solicitados y trasladar al equipo de seguridad cualquier actividad sospechosa".

El negocio del troyano se ha industrializado. Se ha convertido en un SaaS: es un servicio que se puede contratar y que, además, ofrece garantías de éxito de las campañas

Ahora bien, los sistemas empresariales siempre deben ser robustos. "Una de las brechas que se encuentra con más frecuencia en la cadena de ciberseguridad de las empresas es la ausencia de políticas sólidas o de una cadena de aprobación para las transacciones", alerta el director de *threat research and reporting* en Bitdefender. Por ejemplo, los departamentos financieros que operan pagos regularmente solo deben hacerlo después de validar la existencia de contratos y solicitar la aprobación por escrito del responsable de los mismos. "Ha habido numerosos casos de fraude de suplantación del CEO que han creado graves daños en los últimos años".

¿Qué hacer?

La prevención se torna en la mejor estrategia. Mario García insiste en ella para paliar la falta de protección de los dispositivos móviles y el bajo nivel de formación en ciberseguridad. "En estos momentos en los que el trabajo en remoto ha reducido al máximo el contacto entre empleados, es fundamental segmentar la información para que sólo aquellos que realmente lo necesiten, puedan acceder a ella. Esto es fundamental a la hora de proteger las contraseñas de las cuentas bancarias y evitar ser víctima del conocido como timo del CEO".

La protección multicapa, en base a los niveles de exposición al riesgo, es esencial. "Aunque las técnicas usadas por los atacantes van cambiando, los vectores de ataque son muy estables, por lo que los refuerzos en protección se suelen dirigir hacia reforzar la identidad, conocer y parchear las vulnerabilidades y proteger los vectores principales de ataque: navegación y correo electrónico", recuerda Román Vargas. La migración hacia servicios SaaS ha provocado que la identidad sea cada vez más relevante, lo que explotan los atacantes. "La mayoría de las organizaciones está invirtiendo en reforzar el control de accesos mediante tecnologías de doble factor de autenticación de nueva generación, controlando no sólo la identidad del usuario sino también el tipo de terminal y su nivel de riesgo".

Con el auge del teletrabajo, el acceso a las redes internas de las empresas debe estar debidamente protegido. "La utilización de contraseñas robustas, apoyadas en soluciones de doble factor de autenticación, unido a soluciones VPN actualizadas, una segmentación de redes eficaz que evite movimientos laterales, copias de seguridad constantes y soluciones de seguridad que monitoricen cualquier ac-

ción sospechosa de la red (aunque sea ejecutada por herramientas legítimas del sistema) ayudan a mitigar buena parte de los incidentes", recomienda Josep Albors.

Sergio Martínez insiste en la protección del correo electrónico, que se constituye en el primer vector de entrada, en más del 70 % de los casos. "Es el primer punto donde se debe actuar, desplegando más capas que las propias proporcionadas por Microsoft o Google en sus servicios de correo en el *cloud* (Office 365 o G-Suite), ya que existe mucho *malware* preparado para saltarse las protecciones de estos fabricantes". Junto a ello, no olvida recordar que el entorno del puesto de trabajo debe contar con antivirus de nueva generación basados en el comportamiento, no en la firma. "Y, por supuesto, el análisis del tráfico que se recibe, encriptado en más del 70 %".

El ingeniero preventa de WatchGuard, además de la protección del correo fuera de su entorno y de la implementación de herramientas *antiphishing* y de servicios de APT; insiste en el uso de un EDR, "lo que impedirá que se pueda ejecutar el troyano cuando ha conseguido eludir todas soluciones de seguridad anteriores".

Del mismo modo, recomienda, se deben activar sistemas de autenticación multifactor (MFA), lo que dificulta el acceso a ciertos sitios. "Tenemos que mentalizarnos de que las contraseñas, no por ser largas, son más seguras. La contraseña por sí sola no protege, sino que hay que poner otro tipo de soluciones complementarias".

Zero Trust (confianza cero) es el mejor consejo que desde Sophos dan: desconfiar de correos desconocidos, inesperados o sospechosos; y si se trata de comunicaciones de entidades bancarias, no hay que ingresar credenciales ni acceder a páginas webs que soliciten cualquier trámite *online*. "Cuando accedamos a nuestra información personal, hay que cerrar todas las aplicaciones y evitar conectarse a conexiones *wifi* abiertas", aconseja Iván Mateos.

La formación es materia de obligado cumplimiento. José de la Cruz pide un refuerzo de la concienciación del usuario con planes de formación y evaluación continuos. Deben tener claros cuáles son los canales oficiales de comunicación tanto internos dentro de su orga-

nización como externos, con las distintas entidades financieras con las que trabajen. "Deben sospechar de cualquier comunicación, de contenido financiero, recibida a través del correo electrónico. Especialmente aquellas que soliciten algún tipo de acción".

Y 2021

De cara a este 2021, la previsión es que siga creciendo el número de ataques, tal y como sucedió el pasado año en el que se multiplicaron los ataques relacionados con la covid-19, como fue el caso de "falsos préstamos, falsas tarjetas de crédito, notificaciones falsas del banco sobre salud, PCR o servicios remotos falsos" enumera Raúl Tejeda.

Borja Pérez cree que es improbable ver ataques exitosos a la banca del estilo de Carbanak, una banda criminal que tomó el nombre de uno de sus *malware* (también propagó otros como Anunak o Cobalt), y que hace unos años se infiltraba en las redes de seguridad de los bancos en distintas partes del mundo y lograba controlar sus cajeros automáticos. Una mafia que en los 4 años que operó se calcula que robó alrededor de 10.000 millones de dólares. "Eso sí, no descartaría exfiltraciones de datos mediante ataques a la cadena de suministro, como los realizados infiltrándose en SolarWinds", prevé.

Como recuerda Josep Albors, 2021 ya ha arrancado con importantes campañas de propagación de troyanos bancarios dirigidas a usuarios de banca *online* españoles que operan desde su *smartphone*

> España presenta el porcentaje más alto de incidentes de seguridad en Europa como resultado de abrir un correo no deseado: un 54 % frente a la media europea que se sitúa en el 41 %

Android, como ya ocurrió a lo largo de 2020 en el que Eset detectó troyanos bancarios con origen en América Latina que tenían a los usuarios españoles entre sus objetivos favoritos. Concretamente, la marca detectó numerosas campañas protagonizadas principalmente por las familias Grandoreiro y Mekotio.

Otra de las tendencias que crecerá este año es lo que se denominan "navajas suizas" que identifica a aquellos atacantes que pueden adquirir servicios de *malware*, *ransomware*, troyanos bancarios, etc.; creados específicamente para atacar a las entidades que están en su punto de mira. Junto a esta tendencia, va a seguir aumentando el *phishing* personalizado (*spear-phishing*). "Estará tan depurado y tan completamente dirigido a la persona, que va a ser muy difícil de prever", alerta Jorge Pages.

¿Son seguras las aplicaciones bancarias?

No hay ningún banco que no cuente con su aplicación móvil que permite a los usuarios hacer cualquier tipo de transacción o de consulta de sus cuentas. La última novedad ha sido Bizum, que permite la realización de transferencias de manera inmediata. De su expansión es una muestra el caso de CaixaBank, por ejemplo, que cerró 2020 con más de 3 millones de clientes registrados en Bizum, lo que la convierte en la entidad líder en número de usuarios en España, con una cuota del 22,7 %.

El *finance SE* en Fortinet reconoce que no hay ningún sistema 100 % seguro, pero por defecto, todas las *apps* de banca móvil cumplen con un estándar de seguridad muy alto. "El mayor riesgo es, de nuevo, que la contraseña del usuario sea comprometida mediante *phishing* o porque esa misma contraseña se ha usado en otro sistema que ha sido atacado", vuelve a insistir.

Desde el pasado año las entidades financieras ya están aplicando la normativa europea PSD2, lo que ha permitido mejorar el nivel de seguridad tanto en el uso de las aplicaciones como en los pagos *online*. Sin embargo, muchas entidades siguen ofreciendo sistemas de pago y de acceso con medidas de seguridad ya obsoletas como tarjetas de coordenadas o contraseñas de acceso muy básicas. Borja Pérez reconoce que las entidades financieras han extendido el uso de herramientas como la autenticación en dos pasos (2FA). "Se deben proteger todos los dispositivos desde los que se utilicen estas aplicaciones, incluidos los móviles". Incluso, se recomienda un tercer factor en algunas operaciones que incluya *token*, SMS, hoja de coordenadas, reconocimiento facial, etc.

Jorge Pages se pregunta que, aunque las entidades bancarias hayan puesto todo tipo de sistemas de seguridad, hay que observar que estas aplicaciones funcionan en ecosistemas que no están exentos de vulnerabilidades. "Las aplicaciones son seguras y su operativa está estudiada para que lo sean, pero están envueltas en un entorno completamente hostil".

A juicio del consultor de ciberseguridad en Cisco España, el gran problema son los terminales comprometidos. "Los proveedores de aplicaciones móviles oficiales como Google Play y Apple App Store aplican medidas de protección avanzadas que impiden que muchas de las aplicaciones infectadas entren en sus tiendas o puedan instalarse en el dispositivo".