El padre contactó con la Policía brasileña, que lo puso en contacto con The Exodus Road, una ONG que actúa contra la trata de personas. «Proporcionamos a las fuerzas de seguridad locales toda la información disponible sobre Ferreira para posibilitar su liberación», dice Cintia Meirelles de Azevedo, directora para Brasil de la organización. Hubo negociaciones con los operadores de la fábrica de estafas, supuestamente relacionados con la mafia china. De Azevedo confirma que Ferreira fue retenido en el complejo y forzado a las estafas.

Gracias a esa operación, fueron liberados más de 300 prisioneros, incluido Ferreira, que regresó a São Paulo, donde vive con sus dos hermanos y sus padres. «Birmania fue mi infierno», sentencia.

No está claro, sin embargo, que las autoridades hayan desarticulado la red criminal para la que Ferreira fue forzado a trabajar. Cuando una fábrica cierra en algún lugar, suele surgir en otra una nueva.

UN NEGOCIO REDONDO

Las ofertas de captación de los *scammers* aterrizan a menudo en plataformas como Facebook o Instagram. Los anuncios fraudulentos habrían «aumentado considerablemente» en los canales de redes sociales del consorcio Meta desde principios de 2025, informa el banco Trade Republic. Según sus propias declaraciones, el proveedor de servicios financieros reporta mensualmente entre diez mil y veinte mil nuncios fraudulentos a la empresa matriz de Facebook.

Meta no quiso responder a las preguntas de los periodistas. Un portavoz subraya que la compañía elimina todos los anuncios fraudulentos con ayuda de «tecnologías avanzadas y equipos de revisión capacitados» tan pronto como estos son descubiertos.

Con los anuncios publicitarios fraudulentos, Meta ganó el año pasado unos 16.000 millones de dólares. Así lo sugiere, al menos, una evaluación de documentos internos por parte de la agencia de noticias Reuters.

Pero el verdadero corazón de la estafa son las plataformas comerciales falsificadas: sitios web y *apps* que parecen tan profesionales que no todos reconocen el engaño de inmediato. Aquí no se realiza ningún comercio bursátil real, los saldos de cuentas y las ganancias los escriben los propios timadores.

Las autoridades registran en la actualidad una auténtica inundación de plataformas falsas en internet. Además, el uso de inteligencia artificial permite generar nuevas plataformas de fraude con poco esfuerzo, como en una cadena de montaje, lo que permite a los estafadores alcanzar a cada vez más víctimas potenciales.

La artimaña funciona así: los estafadores compran *apps* legítimas que ya están publicadas en Google Play Store y que originalmente ofrecían contenidos diferentes. Por ejemplo, la aplicación de timo STLSTE fue antes dos *apps* de música. Los estafadores cambiaron el logo, el nombre y todo el contenido para convertirlas en plataformas de estafa.

¿Por qué hacen esto? Porque estas aplicaciones ya tienen el visto bueno de Google. Al comprar una *app* legítima, evitan el proceso de verificación y parecen más confiables ante las víctimas. Siguiendo las huellas digitales de la estafa de STLSTE, los investigadores descubrieron una red de al menos 26 plataformas y *apps* fraudulentas conectadas entre sí. Muchas utilizaban herramientas de desarrollo y almacenamiento en la nube procedentes de China.

En la lucha contra estas redes delictivas, las autoridades tienen sus límites. Cuando se denuncia una *app* fraudulenta, Google tarda semanas en eliminarla de la Play Store. Y, cuando finalmente actúa, parece que lo hace a medias. En el caso de la red STLSTE, Google no eliminó todas las *apps* relacionadas de inmediato. Varias permanecieron disponibles para su descarga a pesar de las pruebas evidentes: tenían los mismos nombres de desarrollador y direcciones de correo electrónico idénticas. Mientras tanto, los estafadores siguen operando y captando nuevas víctimas.

GETTY IMAGES / D.R.

Google asegura «actuar de forma consecuente contra aplicaciones que infringen nuestras directrices», informa por escrito. La compañía habría bloqueado solo en 2024 la publicación de 2,36 millones de *apps* debido a infracciones y cerrado más de 158.000 cuentas de desarrolladores maliciosos. Además, a partir de 2026, todas las *apps* de Android deberán ser registradas por desarrolladores verificados.

Es una carrera entre las autoridades que investigan, cuyos medios son limitados, y estafadores bien organizados que siempre desarrollan nuevos métodos. Pero la pregunta decisiva permanece: ¿dónde acaba al final el dinero robado?

Mia, la víctima, revela que solo las pérdidas sufridas por los miembros de su grupo de chat ascienden a varios millones de euros. Si detrás de su caso están *scammers* de una de las fábricas del sudeste asiático, no se sabe. Como casi siempre, las autoridades no han podido identificar a ningún perpetrador. Pero esta vez han dejado huellas. El dinero de Mia no aterrizó en una cartera de criptomonedas anónima, sino en una cuenta bancaria, con IBAN y nombre.

UNA MADEJA INTERNACIONAL

Der Spiegel obtuvo justificantes de transferencias de varios perjudicados en la misma estafa. Muchos están supuestamente dirigidos a Easy Payment & Finance, una institución financiera con sede en Madrid que ofrece a clientes empresariales «servicios bancarios de marca blanca»; es decir, pone a su disposición su infraestructura bancaria. A los perjudicados se les hizo creer que con el registro de la *app* abrirían una «cuenta comercial» en dicha entidad. Los *scammers* promocionaban a Easy Payment & Finance como socio. La institución financiera no respondió a las preguntas de los reporteros. El Banco de España explica que Easy Payment & Finance es una «institución de pago debidamente autorizada y registrada». Sin embargo, no quiso pronunciarse más sobre casos individuales.

El rastro del dinero se pierde en una maraña de proveedores, cuentas virtuales y leyes internacionales. Para las víctimas, al final, apenas hay respuestas, ninguna justicia. Mia se ha dirigido a la supervisión bancaria española, incluso ha contactado con Interpol. Pero su dinero sigue desaparecido. Exactamente igual que Laura, la amable asistente. ●

© DER SPIEGEL

LOS ESTAFADORES COMPRAN 'APPS' QUE YA CUENTAN CON EL VISTO BUENO DE GOOGLE, LUEGO CAMBIAN SU LOGO Y TODO SU CONTENIDO. ASÍ LAS HACEN PASAR POR CONFIABLES