09/10/25

# La Guardia Civil desmantela una red de phishing bancario y detiene al principal desarrollador de kits de robo de credenciales en España

## Resumen

El desarrollador conocido como “GoogleXcoder” ofrecía un servicio completo de phishing a otros delincuentes diseñando y comercializando kits de phishing capaces de clonar páginas web de entidades bancarias y todo tipo de organismos estatales

La actividad delictiva de este cibercriminal era conocida y perseguida por otros cuerpos policiales nacionales e internacionales, así como numerosos organismos dedicados a la ciberseguridad

La investigación concluyó con 6 entradas y registros en diferentes localidades españolas y la detención del principal proveedor de kits de phising, además de la identificación de 6 personas relacionadas directamente con el uso de estos servicios

## Contenido

La Guardia Civil ha desarticulado una de las organizaciones criminales más activas en el ámbito del phishing en España, con la detención de un joven brasileño de 25 años considerado el principal proveedor de herramientas para el robo masivo de credenciales en el entorno hispanohablante.

Desde el año 2023, se han venido sucediendo a nivel nacional una serie de campañas de phishing, en las que los cibercriminales suplantaban tanto a los principales organismos públicos como a las entidades bancarias más importantes de España para engañar a las víctimas y obtener sus datos personales. Estas campañas de robo de credenciales han derivado en una cantidad importante de denuncias de personas afectadas, millones de euros sustraídos y el origen de una incipiente alarma social.

Debido a la gravedad de las circunstancias y a la proliferación agresiva de estas campañas de phishing, el Departamento contra el Cibercrimen de la Unidad Central Operativa (UCO) de la Guardia Civil, inició una investigación con el objetivo de alcanzar no solo a los ejecutores, sino al “cerebro” que diseñaba las herramientas utilizadas por numerosos grupos delictivos para estafar.

Los investigadores pusieron la pista sobre un desarrollador conocido como “GoogleXcoder”, que, bajo un modelo Crime as a Service (CaaS), ofrecía un servicio completo de phishing a otros delincuentes. En concreto, el investigado diseñaba y comercializaba kits de phishing capaces de clonar páginas web de entidades bancarias y todo tipo de organismos estatales. Sus servicios incluían personalización, soporte técnico y actualizaciones, consolidando una estructura criminal profesionalizada.

**Grupo de mensajería “Robarle todo a las abuelas”**

Los cibercriminales o “phishers” contactaban con GoogleXCoder por la aplicación de mensajería “Telegram”, contrataban sus servicios por cientos de euros al día y explotaban estas herramientas de forma abusiva. El resultado de un día: varias decenas de entidades suplantadas, miles de personas engañadas y millones de euros robados. Hasta tal punto llegaba la sensación de impunidad de estos autores, que uno de los grupos de mensajería utilizados por estos delincuentes para ejecutar las estafas se denominaba “Robarle todo a las abuelas”.

El individuo que se ocultaba tras este pseudónimo, era totalmente desconocido por las fuerzas y cuerpos de seguridad, no sólo a nivel nacional sino también internacional. Sin embargo, la localización de esta persona requirió un complejo trabajo operativo de investigación, ya que se trasladaba recurrentemente entre distintos domicilios de diferentes provincias de España, sirviéndose de líneas de teléfono y tarjetas de pago a nombre de identidades suplantadas para evitar su localización. Su actividad delictiva le permitía mantener una vida como “nómada digital” junto a su familia.

En el registro principal, en San Vicente de la Barquera (Cantabria), se detuvo de la persona que se ocultaba tras la identidad de “GoogleXCoder” y a la incautación de dispositivos electrónicos que contenían los kits de phishing de todas las entidades suplantadas, las cuentas personales del investigado, así como conversaciones con decenas de ciberestafadores.

El análisis forense de los dispositivos intervenidos, así como de las transacciones en criptomonedas, que se prolongó durante más de un año debido a su complejidad, permitieron reconstruir todo el entramado delictivo, logrando identificar a seis personas directamente relacionadas con el uso de estos servicios.

Como resultado de la investigación llevada a cabo por el Juzgado de Instrucción número 1 de San Vicente de la Barquera (Cantabria), la operación concluyó con seis entradas y registros en domicilios de distintas localidades (Valladolid, Zaragoza, Barcelona, Palma de Mallorca, San Fernando y La Línea de la Concepción), donde se intervinieron dispositivos electrónicos y se recuperaron fondos vinculados al dinero sustraído a las víctimas, almacenados en distintas plataformas digitales.

Actualmente, la investigación continúa abierta y no se descartan nuevas actuaciones. Los canales de Telegram han sido ya objeto de medidas de desactivación y se están analizando evidencias digitales intervenidas, que podrían dar lugar a nuevas identificaciones o detenciones.

Durante el desarrollo de la investigación se ha contado con la colaboración de la Policía Federal de Brasil y con la empresa de Ciberseguridad Group IB.

Para más información pueden contactar con la oficina de prensa de la Unidad Central Operativa en el teléfono 91 503 13 27.

## Imágenes