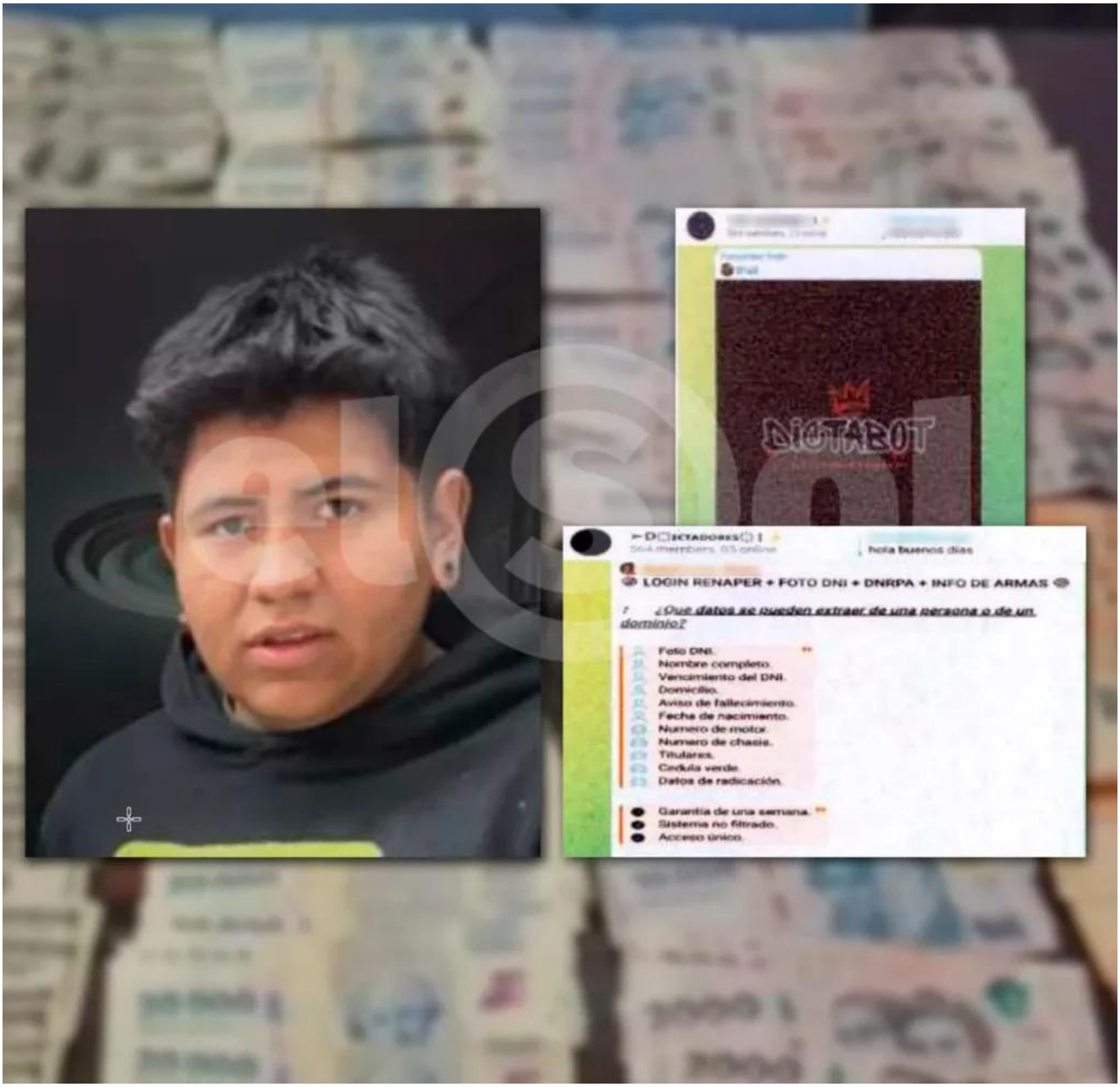
Quién es el joven mendocino que quedó preso en la megacausa nacional de los hackers “Dictadores”

25/10/2025



La habitación estaba a oscuras cuando los policías federales irrumpieron a las 6.35 del 15 de octubre a la casa del barrio Lihué, en el distrito Belgrano de Guaymallén. **Víctor Manuel**

Fabio Silva Santivañez, de apenas 20 años, dormía junto a sus dos hermanos menores en la modesta vivienda de la manzana 25. Lo que encontraron los efectivos en ese operativo no era el cuarto de un adolescente común: cuatro computadoras, tres teléfonos celulares de alta gama, un pendrive Kingston y 831 mil pesos en efectivo escondidos en el ropero de otra habitación, que podrían ser tranquilamente de sus papás.

Pero lo más revelador estaba en las pantallas: **los alias que lo conectaban con una de las organizaciones cibercriminales más sofisticadas que operó en Argentina** en los últimos años, tal como revelaron fuentes judiciales y policiales en charla con ***El Sol.***

El joven mendocino, conocido en el submundo digital como ***"NICEE",*** es considerado parte de una red criminal que desde los rincones más oscuros de Telegram coordinaba **hackeos masivos, comercializaba datos sensibles de millones de argentinos y hasta utilizaba menores de edad para sus operaciones.**

La banda, bautizada como ***"Dictadores",*** había logrado infiltrarse en las bases de datos más protegidas del Estado: el **RENAPER, PAMI, Mi Argentina y la Dirección Nacional del Registro de Propiedad Automotor,** viralizando información a cambio de dinero. También violentaron sistemas privados de Movistar, empresas de análisis crediticio como Nosis y plataformas financieras.

Todo coordinado desde una aplicación de mensajería que, en un principio, les garantizaba anonimato, mensajes autodestructibles cada 24 horas y cifrado de extremo a extremo. **Pero todo cambió cuando empezaron a trabajar los pesquisas policiales, con un agente encubierto**.

La operación *"Dictadores Digitales"* había comenzado seis meses antes, cuando el Departamento de Inteligencia Contra el Crimen Organizado detectó movimientos sospechosos.

Los detectives descubrieron un bot automatizado llamado *“Sherlock Alerts”:* bastaba ingresar un número de DNI para obtener instantáneamente información personal extraída ilegalmente de bases gubernamentales.

Detrás de esa herramienta había una estructura criminal descentralizada pero eficiente, donde cada miembro cumplía un rol específico sin jerarquías rígidas. *“Era como un mundo libre juvenil”,* sentenciaron las fuentes. Había administradores de canales, desarrolladores de software malicioso, vendedores de información y operadores técnicos especializados en distintas ramas del cibercrimen.

El creador de todo este ecosistema delictivo, agregaron las fuentes, fue **Tobías Silva, un joven de 20 años que operaba bajo el alias *“Tree Nix”.* Silva, nacido en noviembre de 2004 y sin registro de actividad laboral formal,** fue acusado de fundar no solo el grupo *“Dictadores”* sino también otra comunidad vinculada llamada *“Sherlock Group”.*

De la causa se desprende que “su genialidad criminal” radicaba en haber construido una red colaborativa donde los miembros compartían recursos, información y asistencia técnica, incluso organizando eventos para hackear objetivos específicos de forma coordinada.

Tobías Silva, señalado como el “cerebro” y creador de la organización de hackers.

Por lo que hablaron las fuentes judiciales a este diario, el mendocino **Silva Santivañez no era un simple miembro más**. El análisis forense inicial de sus comunicaciones reveló su participación activa en las actividades más lucrativas de la banda.

El 13 de julio, bajo la mirada del citado agente encubierto infiltrado en el grupo, realizó varias consultas a través de bots automatizados destinados a validar números de tarjetas de crédito mediante el comando *“/bin”*, una metodología clásica detectada en fraudes electrónicos con plásticos robados.

Los audios que el joven guaymallino compartió con descuido en los chats grupales terminaron por comprometerlo en el expediente. *“Fue la única vez que me molestaron cuando tuve un gasto de quince millones, porque eran cuentas de terceros que me transferían y yo después transfería a tres cuentas y listo, porque sacaba la plata en efectivo, compraba dólares”*, detalló en uno de ellos.

En otro audio, Silva Santivañez relataba cómo había sorteado los controles bancarios con documentación falsa. *“Me llegó un correo y tenía que justificar, y yo puse que eran herencias de mi abuela, que dejó unas cosas y las estaba vendiendo. Fue un abogado mío que me hizo, y un contador amigo que hicimos los papeles truchos y se los pasamos, y después no me molestaron más”,* se jactó el joven. Esas frases llegaron a la Justicia.

La investigación sobre sus movimientos financieros también fue materia de análisis. En su cuenta de **Fiwind Pay**, abierta en septiembre de 2023, se rastrearon transacciones sospechosas. En **Prex Argentina** movió más de 501 mil pesos entre abril y julio de 2024, con transferencias desde cuentas vinculadas incluso a empleados de la Contaduría General de la Provincia de Mendoza.

Pero era en **Mercado Pago** donde la actividad resultó masiva: **259 transferencias salientes y 218 ingresos en un solo año**, con montos que oscilaban entre los 200 mil y el millón de pesos. Entre los destinatarios frecuentes aparecían cuentas propias, familiares y curiosamente, una mujer universitaria (pidieron reserva de su identidad).

En su billetera **Brubank** se detectaron veinte transferencias a un nombre que al ser cruzado con bases de datos arrojó una dirección en José C. Paz, Buenos Aires, y vínculos laborales con el **Ministerio de Justicia y Seguridad**. La cuenta de **Lemon Cash** completaba el panorama: veinticinco transferencias a cuentas propias y, el dato más inquietante, varios movimientos de criptomonedas que evidenciaban un conocimiento sofisticado

de métodos para ocultar el origen de los fondos.

Lo que más impactó a los investigadores fue descubrir una modalidad criminal inédita en el país. **La organización captaba personas de bajos recursos a quienes les ofrecía comprar sus cuentas en diferentes plataformas para luego usarlas en el mercado legal**, blanqueando así operaciones ilegales.

También se identificó una variante del grooming con fines exclusivamente patrimoniales: los delincuentes se ganaban la confianza para obtener acceso a sus cuentas bancarias, tarjetas, correos electrónicos y perfiles en plataformas de juegos online.

La banda, agrega la pesquisa, operaba con ramificaciones en **Buenos Aires, Santa Fe, Córdoba y Mendoza**. Algunos de sus integrantes mantenían estrechos contactos con organizaciones narcocriminales de Rosario, a quienes les ofrecían información reservada para concretar extorsiones y desarrollar maniobras de lavado de activos.

Usaban técnicas diversas: phishing, ingeniería social, creación de sitios web falsos para capturar datos de tarjetas, generación de recetas médicas apócrifas, alteración de registros en organismos públicos y bases privadas, como informó la Policía Federal.

El citado 15 de octubre, **se desarrollaron 22 allanamientos simultáneos** en localidades de Libertad, Merlo, Berazategui, El Jagüel, Moreno, Tigre, Nordelta, Berisso, Marcos Paz, Temperley, Ezpeleta, Virrey del Pino, Olavarría, Mar del Plata y las provincias de Córdoba, Santa Fe y Mendoza.

Once personas quedaron detenidas en la megacausa, **entre ellos el joven guaymallino**. Además de los dispositivos electrónicos, se secuestraron dólares, euros, pesos colombianos, mexicanos, guaraníes paraguayos, libras esterlinas, vehículos, tarjetas y más de dos kilogramos de marihuana.

El allanamiento de la Federal en Guaymallén

En la casa del barrio Lihué, encontraron al joven junto a sus hermanos menores de 13 y 7 años. En su habitación, las dos notebooks Lenovo y Acer guardaban los secretos de sus incursiones digitales. Consultado en presencia de los testigos, **Santivañez aportó voluntariamente la clave de acceso de uno de los dispositivos.**

Los teléfonos celulares contaban su propia historia. En el iPhone blanco sin tarjeta SIM, los técnicos forenses visualizaron chats de Telegram bajo el alias *“@tokiolore”.* En el Motorola gris apareció su identidad más conocida: *“NICEE”*, el apodo con el que presuntamente operaba en el señalado submundo criminal. Ese mismo alias usaba en Instagram como *“vicxxc_.360”,* donde seguía curiosamente a *“tobbyssj”,* cuenta vinculada al fundador de la organización.

Cuando el Juzgado de Campana, que lidera la causa, fue informado telefónicamente de los hallazgos, no dudó: **ordenó el secuestro de todos los elementos vinculados y la detención en carácter de comunicado de Silva Santivañez**.

La Justicia federal lo imputó por asociación ilícita agravada por la intervención de menores. El agravante resultó demoledor. **La defensa intentó conseguir la excarcelación argumentando arraigo y falta de peligro de fuga, pero el pedido fue rechazado**. El juez de la causa consideró que la gravedad de los delitos, la sofisticación de la organización y el riesgo de entorpecimiento de la investigación justificaban mantenerlo tras las rejas.

Actualmente, mientras los peritos informáticos intentan descifrar el alcance real del daño causado y las bases de datos que fueron modificadas, Silva Santivañez espera que se resuelva su situación en una celda.

Fuente: El Sol – https://www.elsol.com.ar/policiales/quien-es-el-joven-mendocino-que-quedo-preso-en-la-megacausa-nacional-de-los-hackers-dictadores/