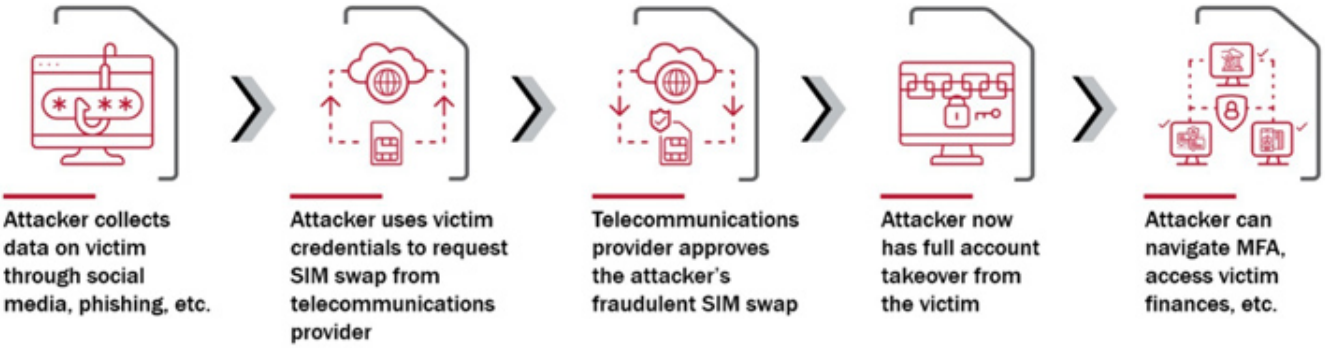
Dos adolescentes británicos han sido declarados culpables por un jurado en Londres por formar parte de la notoria banda transnacional LAPSUS$ y por orquestar una serie de audaces y destacados ataques cibernéticos contra grandes empresas tecnológicas, exigiendo un rescate a cambio de no filtrar la información que robaron.

Entre los acusados se encuentra Arion Kurtaj (también conocido como White, Breachbase, WhiteDoxbin y TeaPotUberHacker), un joven de 18 años de Oxford, y un menor de edad no identificado, quienes comenzaron a colaborar en julio de 2021 después de haberse conocido en línea, según informó la BBC esta semana.

Ambos acusados fueron inicialmente detenidos y liberados bajo investigación en enero de 2022, solo para ser nuevamente detenidos y acusados por la Policía de la Ciudad de Londres en abril de 2022. Kurtaj fue posteriormente puesto en libertad bajo fianza y se mudó a un hotel en Bicester después de que se revelara su identidad en un foro en línea de cibercriminales.

Sin embargo, continuó su racha de ciberataques, apuntando a empresas como Uber, Revolut y Rockstar Games, lo que resultó en su arresto nuevamente en septiembre. Otro supuesto miembro del grupo fue arrestado por las autoridades brasileñas en octubre de 2022.

Fundamental para llevar a cabo los esquemas de extorsión fue su capacidad para realizar cambios de tarjeta SIM y ataques de bombardeo para obtener acceso no autorizado a las redes corporativas después de una exhaustiva fase de manipulación psicológica.



La operación, motivada financieramente, también implicaba publicar mensajes en su canal de Telegram para reclutar colaboradores internos que pudieran proporcionar credenciales de Red Privada Virtual (VPN), Infraestructura de Escritorio Virtual (VDI) o Citrix a las organizaciones.

Un informe reciente del gobierno de Estados Unidos encontró que los actores ofrecían hasta $20,000 por semana por acceso a proveedores de telecomunicaciones para llevar a cabo los ataques de cambio de SIM. Este informe caracterizó a LAPSUS$ como única por su *«eficacia, rapidez, ingenio y audacia», así como por utilizar un «conjunto de técnicas efectivas».*

> *«Para llevar a cabo los cambios fraudulentos de SIM, LAPSUS$ obtenía información básica sobre sus víctimas, como su nombre, número de teléfono e información de red de propiedad exclusiva del cliente (CPNI)»*, afirmó el Cyber Safety Review Board (CSRB) del Departamento de Seguridad Nacional de EE. UU.

> *«LAPSUS$ obtenía esta información a través de diversas vías, como la emisión de solicitudes fraudulentas de divulgación de emergencia y el uso de técnicas de apoderamiento de cuentas para tomar control de las cuentas de empleados y contratistas de proveedores de telecomunicaciones».*

> *«A continuación, llevó a cabo intercambios fraudulentos de tarjetas SIM mediante las herramientas de gestión de clientes del proveedor de telecomunicaciones. Tras ejecutar estos intercambios de tarjetas SIM fraudulentos, LAPSUS$ se apoderó de cuentas en línea a través de procesos de inicio de sesión y recuperación de cuentas que enviaban enlaces de un solo uso o códigos de autenticación multifactor (MFA) a través de mensajes de texto o llamadas telefónicas.»*

Otros métodos para obtener acceso inicial variaron desde el uso de intermediarios de acceso inicial (IAB) hasta la explotación de deficiencias en la seguridad, después de lo cual los involucrados tomaron medidas para aumentar los privilegios, moverse dentro de la red, establecer un acceso permanente mediante software de escritorio remoto como AnyDesk y TeamViewer, y desactivar herramientas de monitoreo de seguridad.

Entre las empresas infiltradas por LAPSUS$ se encontraban BT, EE, Globant, LG, Microsoft, NVIDIA, Okta, Samsung, Ubisoft y Vodafone. Actualmente no está claro si alguna de las compañías afectadas pagó rescates. Se espera que se dicte la sentencia de los adolescentes en una fecha posterior.

> *«Este grupo se volvió conocido porque logró atacar con éxito a organizaciones bien protegidas utilizando ingeniería social altamente efectiva; se enfocó en cadenas de suministro al comprometer a proveedores de externalización de procesos comerciales (BPO) y proveedores de telecomunicaciones; y utilizó su canal público de Telegram para debatir sobre sus operaciones, objetivos y éxitos, e incluso para comunicarse y extorsionar a sus objetivos»,* declaró el CSRB.