La policía de Londres arrestó a siete adolescentes de entre 16 y 21 años de edad, por su supuesta conexión con el grupo de hackers y extorsionadores LAPSUS$, que está vinculada a una reciente ola de ataques contra NVIDIA, Samsung, Ubisoft, LG, Microsoft y Okta.

> *«La policía de la ciudad de Londres ha estado realizando una investigación con sus socios sobre los miembros de un grupo de piratería. Siete personas de entre 16 y 21 años fueron arrestadas en relación con nuestra investigación y todas han sido liberadas bajo investigación. Nuestras investigaciones continúan»,* dijo el inspector detective Michael O´Sullivan.

BBC News informó sobre esto, luego de que un informe de Bloomberg revelara que un adolescente de 16 años que vive en Oxford es el autor intelectual del grupo. No se sabe aún si el menor es uno de los arrestados. Se cree que dicho adolescente, bajo el alias en línea *White o Breachbase*, acumuló alrededor de 14 millones de dólares en Bitcoin por sus actos de ciberdelincuencia.

> *«Nunca había oído hablar de nada de esto hasta hace poco. Él nunca ha hablado de piratería informática, pero es muy bueno con las computadoras y pasa mucho tiempo en la computadora. Siembre pensé que estaba jugando»,* dijo el padre del adolescente.

Según el reportero de seguridad Brian Krebs, el líder del grupo compró Doxbin el año pasado, un portal para compartir información personal de objetivos, solo para ceder el control del sitio web a su antiguo propietario en enero de 2022, pero no antes de filtrar todo el conjunto de datos de Doxbin a Telegram.

Esto llevó a la comunidad de Doxbin a tomar represalias al divulgar la información personal sobre *«WhiteDoxbin»*, incluyendo la dirección de su casa y videos supuestamente filmados por la noche fuera de su casa en Reino Unido.

Ademas, el grupo de hackers reclutó activamente a personas con información privilegiada a través de plataformas de redes sociales como Reddit y Telegram desde al menos noviembre de 2021 antes de que apareciera en escena en diciembre de 2021.

También se cree que al menos un mimbro de LAPSUS$ estuvo involucrado en una violación de datos en Electronic Arts en julio pasado, con Unit 42 de Palo Alto Networks descubriendo evidencia de actividad de extorsión dirigida a clientes de teléfonos móviles del Reino Unido en agosto de 2021.

LAPSUS$, en un lapso de tres meses, aceleró su actividad maliciosa, alcanzando rápidamente prominencia en el mundo del crimen cibernético por sus objetivos de alto perfil y manteniendo una presencia activa en la aplicación de mensajería Telegram, donde acumuló 47 mil suscriptores.

Microsoft caracterizó al sindicato criminal como un grupo *«poco ortodoxo»* que *«no parece cubrir sus huellas»* y que utiliza una combinación única de oficio, que combina la ingeniería social basada en teléfonos y el pago a empleados de organizaciones objetivo para acceder a las credenciales.

En todo caso, el enfoque descarado de LAPSUS$ para atacar a las empresas sin tener en cuenta las medidas de seguridad operativas parece haberles costado muy caro, dejando huellas forenses que condujo a sus arrestos.

> *«Algunos de nuestros miembros tienen vacaciones hasta el 30/3/2022. Es posible que estemos tranquilos por algunos momentos. Gracias para que nos entienda, intentaremos filtrar cosas lo antes posible»,* fue el último mensaje del grupo este miércoles.