Tres personas fueron acusadas este viernes por sus presuntos roles en el hackeo de Twitter ocurrido el pasado 15 de julio, según informó el Departamento de Justicia de Estados Unidos.

Mason Sheppard, alias «Chaewon», de 19 años de edad, de Bognor Regis, Reino Unido, fue acusado en una denuncia penal en el Distrito Norte de California por conspiración para cometer fraude electrónico, conspiración para cometer lavado de dinero y acceso intencional a una computadora protegida.

Nima Fazeli, alias «Rolex», de 22 años, de Orlando, Florida, fue acusada en una denuncia penal en el Distrito Norte de California por ayudar e instigar el acceso intencional de una computadora protegida.

El tercer acusado es un menor de edad. Con algunas excepciones que no se aplican a este caso, los procedimientos de menores en un tribunal federal están sellados para proteger la identidad del menor.

> *«De conformidad con la Ley Federal de Delincuencia Juvenil, el Departamento de Justicia ha remitido a la persona al Fiscal del Estado para el 13° Distrito Judicial en Tampa, Florida»,* dice el comunicado del Departamento de Justicia.
>
> *«Existe una falsa creencia dentro de la comunidad de hackers criminales de que los ataques como el hackeo de Twitter pueden perpetrarse anónimamente y sin consecuencias. El anuncio de la acusación de hoy demuestra que la euforia de la piratería nefasta en un entorno seguro por diversión o beneficio será de corta duración. La conducta criminal en Internet puede parecer sigilosa para las personas que la perpetran, pero no hay nada sigiloso al respecto. En particular, quiero decirle a los posibles delincuentes, violen la ley y los encontraremos»,* dijo el fiscal federal David L. Anderson para el Distrito Norte de California.
>
> *«Los piratas informáticos supuestamente comprometieron más de 100 cuentas de*

> *redes sociales y estafaron tanto a los usuarios de la cuenta como a otras personas que enviaron dinero en base a sus solicitudes fraudulentas. La rápida investigación de esta conducta es un testimonio de la experiencia de nuestros investigadores, nuestro compromiso de responder rápidamente a los ataques cibernéticos y las estrechas relaciones que hemos establecido con los socios de las fuerzas del orden en todo el mundo»,* dijo el Secretario de Justicia Auxiliar Interino, Brian C. Rabbit de la División Criminal del Departamento de Justicia.

> *«Al abrir una investigación sobre este ataque, nuestros investigadores trabajaron rápidamente para determinar quién era responsable y localizar a esas personas. Si bien las investigaciones sobre infracciones cibernéticas a veces pueden llevar años, nuestros investigadores pudieron detener a estos hackers en cuestión de semanas. Independientemente de cuánto tiempo nos lleve identificar a los hackers, seguiremos la evidencia hasta donde nos lleve, y en última instancia, responsabilizaremos a los responsables de las intrusiones cibernéticas por sus acciones. Los ciberdelincuentes no encontrarán refugio detrás de sus teclados»,* dijo el Agente Especial del FBI de San Francisco, John F. Bennett.

> *«El anuncio de hoy demuestra que los cibercriminales ya no pueden esconderse detrás del anonimato global percibido. El Servicio Secreto sigue comprometido a perseguir a los responsables del fraude cibernético y seguirá responsabilizando a los ciberdelincuentes por sus acciones. Esta investigación es un testimonio de las sólidas alianzas entre el Servicio Secreto, la Oficina del Fiscal de Estados Unidos, el FBI, el IRS, así como nuestros socios policiales estatales, locales e internacionales»*, dijo Thomas Edwards, Agente Especial a Cargo, Servicio Secreto de Estados Unidos, Oficina de Campo de San Francisco.

Según las quejas, el ataque de Twitter consistió en una combinación de infracciones técnicas e ingeniería social. El resultado del hackeo fue el compromiso de aproximadamente 130 cuentas de Twitter pertenecientes a políticos, celebridades y músicos.

Los hackers crearon una billetera Bitcoin fraudulenta, robaron el acceso a cuentas verificadas de Twitter, enviaron solicitudes de dichas cuentas con la falsa promesa de duplicar los depósitos de bitcoin realizados en la cuenta y luego robaron los bitcoin que las víctimas enviaron.

El caso sigue en investigación por la División de San Francisco del FBI, con asistencia de la Unidad de Investigación Cibernética del IRS, el Servicio Secreto de Estados Unidos, entre otras agencias.