HOJA INFORMATIVA:

ORIENTACIÓN SOBRE LOS TÉCNICOS INFORMÁTICOS DE LA REPÚBLICA POPULAR DEMOCRÁTICA DE COREA

16 de mayo de 2022

El Gobierno de los EE. UU. publica este **aviso** como un recurso completo para la comunidad internacional, el sector privado y el público para que comprendan y se protejan mejor del reclutamiento, la contratación y la facilitación accidentales de los técnicos informáticos (IT) de la República Popular Democrática de Corea (RPDC, también conocida como Corea del Norte). Este aviso proporciona información detallada sobre cómo operan los técnicos informáticos de la RPDC e identifica señales de alerta y medidas de diligencia debidas para ayudar a las empresas a no contratar desarrolladores autónomos de la RPDC, y a las plataformas de pago digitales independientes a identificar a los técnicos informáticos de la RPDC que se aprovechan de sus servicios. Contratar o apoyar las actividades de los técnicos informáticos de la RPDC conlleva muchos riesgos, que van desde el robo de propiedades intelectuales, datos y fondos, hasta daños en la reputación y consecuencias legales, incluidas las sanciones de las autoridades de los EE. UU. y la Organización de las Naciones Unidas (ONU).

La RPDC ha enviado a miles de técnicos informáticos altamente cualificados por todo el mundo, obteniendo ingresos con los que financia sus programas de armamento, lo que infringe las sanciones de los EE. UU. y la ONU. Estos empleados:

- Se aprovechan de todo el ecosistema de las plataformas de trabajo para autónomos para conseguir encubiertamente contratos de desarrollo en informática de empresas de todo el mundo que necesitan estos servicios, así como se aprovechan de muchas plataformas de medios sociales para comunicarse con los clientes, y de las plataformas de pago para recibir remuneración por su trabajo.
- Desarrollan aplicaciones y software que abarcan sectores en el que están incluidos, pero no se limitan a, negocios, criptomonedas, salud y fitness, redes sociales, deportes, ocio y estilo de vida.
- En muchas ocasiones, falsifican su identidad y se presentan como extranjeros (no norcoreanos) o teletrabajadores residentes en los EE. UU., para lo que usan redes privadas virtuales (VPN), servidores privados virtuales (VPS), direcciones IP adquiridas de terceros países, cuentas proxy y documentos de identidad falsificados o robados.
- Además, utilizan el acceso con privilegios obtenido por su condición de contratistas con fines ilícitos, dentro de lo que se incluye habilitar intrusiones cibernéticas maliciosas de otros agentes de la RPDC.

Algunas señales de alerta de actividad potencial de técnicos informáticos de la RPDC incluyen:

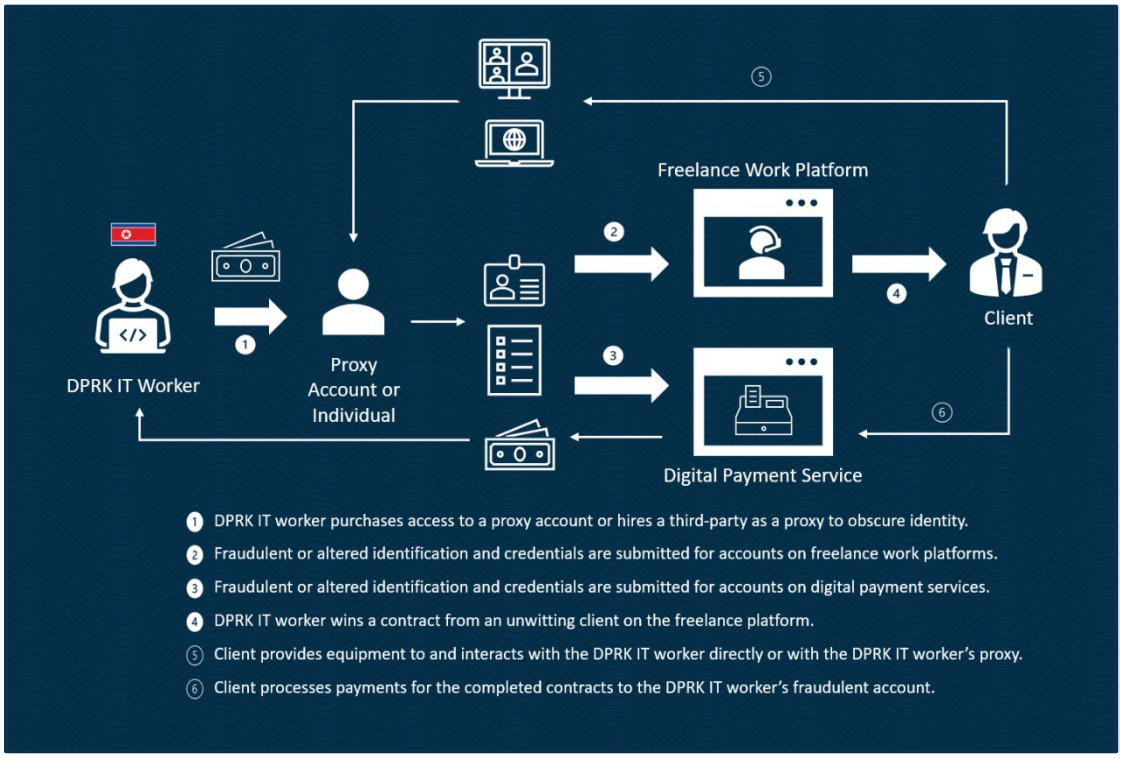
- Múltiples inicios de sesión en una misma cuenta desde diferentes direcciones IP en un periodo de tiempo relativamente corto, especialmente si las direcciones IP se asocian con distintos países.
- Transferencias de dinero frecuentes a través de plataformas de pago, particularmente a cuentas bancarias localizadas en la República Popular China (RPC), o solicitudes de pago en criptomonedas.

- Inconsistencias en la escritura del nombre, la nacionalidad, la supuesta localidad desde donde trabajan, los datos de contacto, el historial académico, la experiencia profesional y demás datos entre sus perfiles en las diferentes plataformas de trabajo para autónomos, los perfiles de los medios sociales, los sitios web externos con portafolio, los perfiles en las plataformas de pago y el análisis de su ubicación y horarios; y
- No estar disponible para trabajar durante el horario normal de oficina y tener dificultad para contactar con el trabajador en un plazo adecuado, especialmente a través de las formas de comunicación «inmediata».

Las medidas de diligencia debidas que el sector privado puede tener en cuenta para evitar la contratación accidental o inconsciente de técnicos informáticos de la RPDC incluyen:

- Verificar los documentos que se han recibido en el marco de los exámenes de propuestas o solicitudes de trabajo directamente con las empresas y las instituciones educativas mencionadas en ellos (sin utilizar los datos de contacto proporcionados en la documentación que se ha recibido).
- Examinar atentamente los documentos de identidad enviados para detectar fraudes.
- Realizar una entrevista por videoconferencia para comprobar la identidad de un posible trabajador externo.
- Llevar a cabo una verificación de los antecedentes previa a la contratación o un registro de huella dactilar o biométrico para comprobar la identidad y la supuesta ubicación.
- Evitar pagar en criptomonedas y solicitar verificación de la información bancaria correspondiente a otros documentos identificativos.
- Comprobar que la escritura del nombre, la nacionalidad, la supuesta localidad desde donde trabaja, los datos de contacto, el historial académico, la experiencia profesional y demás datos de un posible candidato coinciden en los perfiles de las diferentes plataformas de trabajo para autónomos, los perfiles de los medios sociales, los sitios web externos con portafolio, las cuentas en las plataformas de pago y el análisis de su ubicación y horarios.
- Se debe sospechar si el desarrollador no puede recibir material en la dirección que consta en sus documentos de identificación.

Resumen de las operaciones de los técnicos informáticos de la RPDC



Para obtener más información, consulte ***DPRK Cyber Advisory*** *(Aviso cibernético sobre la RPDC), visite el* ***Treasury resource center*** *(centro de recursos del Tesoro) o contáctese con la* ***oficina local del FBI****. Si cuenta con información sobre actividades ilícitas de la RPDC en el ciberespacio, incluidas operaciones pasadas o en marcha, podría ser elegible para recibir una compensación de hasta 5 millones de dólares si proporciona esa información a través del programa* ***Recompensas por la Justicia*** *del Departamento de Estado.*