16 de mayo de 2022

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

El Departamento de los Estado de EE. UU., el Departamento del Tesoro de los EE. UU. y la Oficina Federal de Investigación (FBI) publican este aviso para la comunidad internacional, el sector privado y el público para advertirles de los intentos de los técnicos informáticos de la República Popular Democrática de Corea (RPDC, también conocida como Corea del Norte), de obtener empleo haciéndose pasar por no norcoreanos. Existen riesgos de reputación y posibles consecuencias legales, incluidas las sanciones de las autoridades de los EE. UU. y la Organización de las Naciones Unidas (ONU), para las personas físicas y las entidades que se involucren en el apoyo a las actividades de los técnicos informáticos de la RPDC y el procesamiento de las transacciones financieras vinculadas.

La RPDC envía a miles de técnicos informáticos altamente cualificados por todo el mundo para obtener ingresos con los que financiar sus programas de armas de destrucción masiva (ADM) y de misiles balísticos, lo que infringe las sanciones de los EE. UU. y la ONU. Estos técnicos informáticos se aprovechan de la demanda existente de conocimientos informáticos específicos, como el desarrollo de aplicaciones de software y móviles, para obtener contratos de empleo como autónomos de clientes de todo el mundo, incluidas Norteamérica, Europa y Asia del Este. En muchos casos, los técnicos informáticos de la RPDC se presentan como teletrabajadores residentes en los EE. UU. o no norcoreanos. Estos empleados pueden ocultar su identidad o ubicación subcontratando a personas que no sean norcoreanas. Si bien los técnicos informáticos de Corea del Norte suelen trabajar en sectores que no comportan ciberactividad maliciosa, han utilizado el acceso con privilegios obtenido por su condición de contratistas para habilitar las intrusiones cibernéticas maliciosas de la RPDC. Además, probablemente haya casos en los que los empleados estén sujetos a trabajo forzoso.

Este aviso proporciona información detallada sobre cómo trabajan los técnicos informáticos de la RPDC, sobre las señales de alerta para las empresas que den trabajo a desarrolladores autónomos y a las plataformas de trabajo para autónomos y de pago independientes para que identifiquen a los técnicos informáticos de la RPDC. Además, facilita medidas de mitigación generales para que las empresas se protejan mejor de accidentalmente contratar o propiciar las operaciones de los técnicos informáticos de la RPDC. Hay un Anexo que proporciona información adicional sobre los técnicos informáticos de la RPDC recopilada a partir de informes del Grupo de Expertos de la RPDC del Comité de Sanciones

1718 de la ONU. El FBI anima a las empresas estadounidenses a informar las actividades sospechosas, incluida cualquier actividad sospechosa de la que sea autor un técnico informático de la RPDC, a las oficinas locales.

TÉCNICOS INFORMÁTICOS DE LA RPDC: ANTECEDENTES

Los técnicos informáticos de la RPDC suministran un flujo de ingresos vital que ayuda a financiar las más altas prioridades económicas y de seguridad del régimen de la RPDC, como el programa de desarrollo de armas. El líder de la RPDC, Kim Jong Un, reconoce la importancia de los técnicos informáticos en su labor de servir de fuente significativa de divisas extranjeras e ingresos y apoya sus operaciones.

Hay miles de técnicos informáticos de la RPDC tanto en el extranjero como ubicados en la RPDC, y estos generan ingresos que envían al Gobierno norcoreano. Los técnicos informáticos de la RPDC se ubican, principalmente, en la República Popular China (RPC) y Rusia, pero también hay una cantidad menor en África y el Sudeste Asiático. Estos trabajadores informáticos suelen confiar en sus contactos en el extranjero para conseguir trabajos como autónomos para ellos y para interactuar de manera más directa con los clientes.

Todos los técnicos informáticos de la RPDC ganan dinero que utilizan para financiar el régimen del líder norcoreano, Kim Jon Un. La gran mayoría de ellos está subordinada a y trabaja en nombre de entidades que están directamente involucradas en los programas de armas de destrucción masiva (ADM) y de misiles balísticos de Corea del Norte prohibidos por la ONU, así como en el desarrollo de armas convencionales avanzadas y el comercio. Todo esto arroja como resultado que los ingresos que estos empleados generan van a parar a manos de la RPDC para desarrollar sus programas de ADM y misiles balísticos, infringiendo las sanciones de los EE. UU. y la ONU. La ONU y los Estados Unidos han previsto sanciones para muchas de estas entidades. Entre las entidades de la RPDC que envían técnicos informáticos se incluyen:

- **La 313 General Bureau of the Munitions Industry Department** (oficina general 313 del departamento de industria de municiones, MID), que gestiona la investigación, el desarrollo y la producción de armas —incluido armamento nuclear y misiles balísticos— y demás equipamiento militar de la RPDC. El MID está subordinado al Comité Central del Partido de los Trabajadores de Corea y, a través de la oficina general 313, despliega la mayoría de la mano de obra de la RPDC en el campo de la informática en el extranjero. Todos los bienes y los intereses en manos del Partido de los Trabajadores de Corea están bloqueados en virtud del Decreto 13722.

- **El Ministerio de Industria de Energía Atómica** es un actor vital en el desarrollo del armamento nuclear de la RPDC y está a cargo de las operaciones diarias del programa de armas nucleares de la RPDC. El Ministerio de Industria de Energía Atómica es designado en virtud del Decreto 13382.

- Las entidades militares están subordinadas al **Ministerio de Defensa y del Ejército Popular de Corea**. El Ejército Popular de Corea lo conforman ciudadanos especialmente designados y una lista de bienes cerrada.

- Se añaden otras entidades menos conocidas, como el **Ministerio de Comercio Exterior de la Comisión de Educación de la RPDC** y la **Pyongyang Information Technology Bureau of the Central Committee's Science and Education Department** (oficina de tecnologías de la información de Pyongyang del departamento de educación y ciencia del Comité Central). Todos los bienes y los intereses en manos del Gobierno de la RPDC están bloqueados en virtud del Decreto 13722.

Un técnico informático de Corea del Norte en el extranjero gana, como mínimo, diez veces más que un trabajador norcoreano convencional que trabaja en una fábrica o en un proyecto de construcción en el extranjero. Cada uno de los técnicos informáticos de la RPDC puede ganar más de 300 000 dólares al año en algunos casos y los equipos de técnicos informáticos pueden ganar más de 3 millones de dólares anualmente. Una parte significativa de sus ingresos brutos se usa para apoyar las prioridades del régimen de la RPDC, incluido el programa de ADM.

Las empresas IT de la RPDC y sus empleados, en general, se involucran en un amplio espectro de trabajos de desarrollo en el ámbito informático que varían en complejidad y dificultad, como, por ejemplo:

- aplicaciones web y móviles,
- creación de plataformas de cambio de divisas virtuales y monedas digitales,
- servicio técnico informático general,
- animación gráfica,
- programas de apuestas en línea,
- juegos para dispositivos móviles,
- aplicaciones de citas,
- aplicaciones relacionadas con la inteligencia artificial,
- desarrollo de firmware y hardware,
- programas de realidad virtual y de realidad aumentada,
- software de reconocimiento facial y biométrico,
- desarrollo y gestión de bases de datos.

Las aplicaciones y el software que desarrollan los técnicos informáticos de la RPDC abarcan una variedad de campos y sectores que incluyen negocios, salud y fitness, redes sociales, deportes, ocio y estilo de vida. Los técnicos informáticos de la RPDC suelen participar en proyectos que implican divisas virtuales. Algunos de los técnicos informáticos de la RPDC han diseñado intercambios de

divisas virtuales o creado herramientas y aplicaciones de análisis para operadores de divisas virtuales y comercializado sus productos para sus propios fines.

Durante décadas, la RPDC ha subrayado la importancia de formar a sus ciudadanos en matemáticas y ciencias. El énfasis para avanzar en ciencia y tecnología, lo que, históricamente, ha sido prioritario para el régimen de Kim, se refleja en la inversión de recursos y personal en los campos de investigación relacionados. La formación en informática y en el ámbito cibernético en la Corea del Norte actual se fundó en este empuje hacia el progreso y ha resultado en un currículo integrado y coordinado con el Partido de los Trabajadores, los centros de investigación y las fuerzas armadas.

- En los últimos años, con Kim Jong Un, el régimen ha hecho hincapié en la educación y la formación en las materias relacionadas con la informática y ha desarrollado programas de grado en informática en varias instituciones educativas de primer nivel de la RPDC, en especial, la Kim Il Sung University, la Kim Chaek University of Technology y la Pyongyang University of Science and Technology. Solo en estas universidades de excelente nivel, unos 30 000 estudiantes cursan materias relacionadas con las tecnologías de la comunicación y la información.

- Desde el 2019, se decía que 37 universidades contaban con 85 programas de estudios en los que se ofrecían asignaturas de ciencias avanzadas, tecnología, ingeniería y matemáticas (CTIM), incluida la seguridad de la información, y todas las provincias habían fundado, al menos, una escuela secundaria nueva para formar a los prometedores estudiantes.

- El sistema educativo de la RPDC fomenta una gran competitividad y solo se acepta a los estudiantes de primer nivel en los programas de tecnología y ciencia de la élite. Se los recluta a edades tempranas en escuelas secundarias como la Kumsong Academy y la Kumsong Middle School Number 1.

- Los técnicos informáticos de la RPDC reciben formación adicional en el extranjero y de sus propias organizaciones, frecuentemente a través de centros de investigación en informática regionales en el país para desarrollar aún más sus habilidades. Históricamente, los trabajadores informáticos de la RPDC han adquirido formación en el Este de África, el Sudeste Asiático y el Sur de Asia, de la que se benefician notablemente.

CÓMO OPERAN LOS TÉCNICOS INFORMÁTICOS DE LA RPDC

Los técnicos informáticos de la RPDC dirigen sus esfuerzos a conseguir contratos como autónomos de empresas ubicadas en países más ricos, incluidos los situados en Norteamérica, Europa y Asia del Este. En muchos casos, se presentan como teletrabajadores de nacionalidad surcoreana, china, japonesa o de Europa del Este residentes en los EE. UU.

En algunos casos, ocultan su identidad mediante acuerdos con terceras partes subcontratistas. Estos no son norcoreanos, sino técnicos informáticos autónomos que completan contratos para los informáticos de la RPDC. Los responsables de informática de la RPDC también han contratado a sus propios equipos de técnicos informáticos no norcoreanos, los cuales no suelen saber nada acerca de la identidad real de su empleador norcoreano o el hecho de que este sea una empresa de la RPDC. Los responsables de los técnicos informáticos de la RPDC utilizan a sus empleados externos para adquirir software e interactuar con los clientes en situaciones en las que, de no hacerse así, un técnico informático de la RPDC podría ser descubierto.

Si bien los técnicos informáticos de la RPDC suelen trabajar en proyectos informáticos no maliciosos como el desarrollo de intercambios de divisas virtuales o de un sitio web, han utilizado el acceso con privilegios obtenido por su condición de contratistas para habilitar las intrusiones cibernéticas maliciosas de Corea del Norte. Algunos de los técnicos informáticos de la RPDC radicados en el extranjero han provisto de apoyo logístico a los ciberagentes maliciosos ubicados en la RPDC, aunque es improbable que estos técnicos se involucren ellos mismos en ciberactividades maliciosas. Los técnicos informáticos de la RPDC pueden compartir el acceso a una infraestructura virtual, facilitar la venta de datos robados por los ciberagentes de la RPDC o contribuir a blanquear los capitales de la RPDC y con las transferencias de divisas virtuales.

Los técnicos informáticos de la RPDC también han ayudado a los funcionarios norcoreanos a obtener material relacionado con los programas de ADM y de misiles balísticos de la RPDC prohibidos.

Hay casos en los que los empleados están sujetos a la trata de personas, incluidos los trabajos forzosos. Existen informes fidedignos que demuestran que muchos de los empleados de la RPDC en el extranjero están sometidos a jornadas de trabajo excesivas, a la vigilancia constante y estrecha de los agentes de seguridad del Gobierno norcoreano, viven en condiciones insalubres y peligrosas y cuentan con poca libertad de movimiento. El Gobierno de Corea del Norte se queda con hasta el 90 % de los salarios de sus empleados en el extranjero, lo que genera unos ingresos anuales para este de cientos de millones de dólares.

Técnicos informáticos de la RPDC: habilidades y plataformas

Lo más frecuente es que los equipos de informáticos de la RPDC en el extranjero consigan trabajos como autónomos a través de diferentes plataformas en línea. Las empresas utilizan estas plataformas para anunciar proyectos a los que los desarrolladores informáticos autónomos pueden licitar. Con menor frecuencia, los equipos de informáticos de la RPDC encuentran ciudadanos locales no norcoreanos como directores de empresas que, en realidad, son controladas por norcoreanos. También ha habido casos en los que estos equipos figuran, en papel, como trabajadores para una empresa local legítima, pero desarrollan su propio negocio de manera independiente y, a cambio de ocultar su procedencia norcoreana, pagan una cuota a la empresa extranjera. Los equipos de informáticos de la RPDC suelen contar con miembros con dominio avanzado de lenguas extranjeras, como inglés o chino.

Los técnicos usan una amplia variedad de plataformas conocidas de empleo para autónomos específicas de la industria, plataformas y herramientas de desarrollo de software, aplicaciones de mensajería y sitios web de medios y redes sociales para conseguir contratos de proyectos de desarrollo de empresas de todo el mundo, además de utilizar plataformas y sitios web de pago digitales para recibir la remuneración por sus servicios. También usan el intercambio de divisas virtuales y las plataformas de comercio para gestionar los pagos digitales que reciben por los trabajos por contrato para blanquear y transferir el capital que obtienen.

Técnicos informáticos de la RPDC: cómo ocultar su identidad

Los técnicos informáticos de la RPDC ocultan su identidad, su ubicación y su nacionalidad en la red de forma deliberada, a menudo usando nombres no coreanos como alias. También usan redes privadas virtuales (VPN), servidores privados virtuales (VPS) o direcciones IP propias de terceros países para que parezca que se están conectando a Internet desde ubicaciones no sospechosas y así reducir las probabilidades de que se investiguen sus localizaciones y relaciones. Por norma general, confían en el anonimato que facilitan los acuerdos de teletrabajo, usan cuentas proxy para crear y mantener cuentas y prefieren servirse de intermediarios y de la comunicación a través de texto en lugar de las videoconferencias.

Los técnicos informáticos de la RPDC utilizan cuentas proxy en los sitios web para desarrolladores de software autónomos para licitar, conseguir adjudicaciones, trabajar y recibir pagos por los proyectos. Estas cuentas proxy pertenecen a terceros, algunos de los cuales venden la información de sus cuentas e identificaciones a los técnicos informáticos de la RPDC. En algunos casos, los técnicos informáticos de la RPDC les pagan cuotas a estos terceros para poder utilizar sus cuentas legítimas en estas plataformas. Los técnicos informáticos de la RPDC pueden rellenar los perfiles de las plataformas para autónomos con afiliaciones y experiencia profesional reales de la cuenta proxy.

A veces, estos técnicos involucran a trabajadores autónomos no norcoreanos en las plataformas para proponerles colaborar en proyectos de desarrollo. Un técnico informático de la RPDC saca ventaja de estas relaciones profesionales para conseguir acceso a nuevos contratos y cuentas de divisas virtuales utilizadas para realizar su trabajo en informática por encima de las infraestructuras virtuales europeas o estadounidenses sorteando las medidas de seguridad dirigidas a evitar el uso fraudulento. Al crear cuentas con la ayuda de otros trabajadores autónomos, los técnicos informáticos de la RPDC pueden asegurar ser ciudadanos de terceros países que necesitan documentos de identidad de los EE. UU. o de otros países occidentales y las cuentas de plataformas para autónomos para ganar más dinero.

Al ocultar su ubicación real, pueden infringir los términos de los contratos de servicio de las plataformas y los servicios en línea que utilizan para sus actividades. En la parte comercial de su oficio, también pueden usar diferentes dispositivos para cada una de sus cuentas, en particular para las de banca y, así, eludir la detección de prevención del fraude, el cumplimiento de las sanciones y las medidas antiblanqueo de dinero.

Habitualmente, los técnicos informáticos de la RPDC utilizan documentos falsos, modificados o falsificados, incluidos documentos de identidad, y firmas falsas, los cuales, o bien han hecho ellos mismos mediante software como Photoshop, o bien han pagado a una empresa de falsificaciones para modificarlos combinando la propia foto del trabajador o una falsa con los datos de una persona real. Los técnicos informáticos de la RPDC en general obtienen documentos falsos como, por ejemplo:

- licencias de conducir,
- tarjetas del seguro social,
- pasaportes,
- documentos nacionales de identidad,
- tarjetas de residencia de extranjeros,
- títulos de escuela secundaria y universidades,
- visas de trabajo, y
- tarjetas de crédito y extractos bancarios y de servicios públicos.

En algunos casos, estas identidades son robadas, mientras que, en otros, los técnicos informáticos de la RPDC le han pedido a un ciudadano extranjero que se cree una cuenta usando sus propios datos personales o la información a la que tengan acceso, después de lo cual el control de la cuenta se transfiere a los técnicos informáticos de la RPDC a cambio de una cuota. Esto le permite a los técnicos informáticos de la RPDC ocultar su identidad al licitar y completar proyectos para autónomos para clientes en Internet usando la infraestructura del titular real de la cuenta mediante acceso a escritorio remoto. Cada técnico informático suele usar múltiples identidades y cuentas, que también pueden compartir con técnicos informáticos del mismo equipo. Estas cuentas e identidades aparentan ser de países de todas las partes del mundo.

Pueden robar la información de la cuenta de un cliente de un banco de los EE. UU. o internacional para verificar su identidad en las plataformas para autónomos, con los proveedores de pagos y las empresas que dan trabajo a los técnicos informáticos de la RPDC. Al menos en un caso, los técnicos informáticos de la RPDC falsificaron cheques usando información robada de una cuenta bancaria. Las cuentas y los currículums asociados con las identidades proxy de los técnicos informáticos de la RPDC suelen incluir información sobre la formación y la experiencia laboral falsificada, pero realista y detallada, incluidos datos de contacto falsos de las instituciones educativas y las empresas anteriores.

También pueden completar las secciones de empleo de sus perfiles en línea de desarrolladores con nombres de pymes occidentales, con lo que los técnicos informáticos de la RPDC aparentan ser europeos o estadounidenses de confianza cuando licitan para proyectos. Pueden usar nombres de empleados reales y direcciones de correo electrónico que se asemejan a las del dominio real de la empresa occidental.

Además, los técnicos informáticos de la RPDC falsifican acuerdos de especificación de servicios laborales, facturas, documentación de contacto del cliente y otros documentos para emplearlos en las

plataformas para autónomos, probablemente para cumplir las medidas «conoce a tu cliente» y antiblanqueo de dinero (KYC y AM) o procedimientos similares con los que cuentan las plataformas para garantizar la legitimidad de la actividad del usuario. Estos documentos falsificados pueden tener datos de contacto mínimos para impedir la verificación.

Los técnicos informáticos de la RPDC también pueden intentar enmascarar su nacionalidad presentándose como ciudadanos surcoreanos o, simplemente, «coreanos».

También se sabe que los técnicos informáticos de la RPDC que consiguen puestos autónomos en una empresa de manera inconsciente por parte de esta, recomiendan después a la empresa a otros técnicos informáticos de la RPDC.

Currículum de un técnico informático de la RPDC

Los técnicos informáticos de la RPDC se promocionan con conocimientos en desarrollo de programas y sistemas, sistemas de gestión de bases de datos y el uso de una amplia variedad de recursos en la nube, herramientas, entornos y lenguajes comunes. Estos suelen incluir sólidos conocimientos en cierta cantidad de lenguajes de programación y de marcado. La mayoría de los proyectos de estos técnicos informáticos de la RPDC están relacionados con el desarrollo de aplicaciones web y móviles. También utilizan plataformas colaborativas, servicios de alojamiento de datos y de gestión del flujo de trabajo. Estos trabajadores suelen indicar que cuentan con experiencia con varias bases de datos y que son capaces de trabajar con los productos y servicios de análisis y en la nube de los principales proveedores. Además, los técnicos informáticos de la RPDC incorporan el pago digital y las plataformas de comercio electrónico en su trabajo.

Los técnicos informáticos de la RPDC crean sitios web con «portafolios» que, generalmente, tienen un diseño sencillo, en un esfuerzo de potenciar la credibilidad de sus imágenes artificiales de desarrolladores autónomos. Estos portafolios virtuales muestran el trabajo de las imágenes de los técnicos informáticos y suelen estar vinculados a las cuentas en línea de desarrolladores autónomos. Es probable que la información que aparece en estos sitios web, incluidos los datos de contacto y la ubicación, así como el historial académico y la experiencia profesional, sea falsa.

INDICADORES DE SEÑALES DE ALERTA

Las empresas que dan trabajo a los autónomos y las plataformas de pago independientes deben ser conscientes de que la siguiente actividad puede ser un indicador de la conducta propia de los técnicos informáticos de la RPDC que puedan estar usando sus plataformas.

- 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 ubican en países distintos;
- Los desarrolladores inician sesión en varias cuentas de la misma plataforma desde una única dirección IP;
- Los desarrolladores mantienen la sesión iniciada durante un día o más;
- El puerto del rúter u otros ajustes técnicos asociados al uso de software para conectarse a un escritorio remoto, como usar el puerto 3389 del rúter para acceder a la cuenta, en especial si el empleo de este software no es una práctica común en la empresa;
- Las cuentas del desarrollador utilizan una cuenta de cliente fraudulenta para aumentar la calificación de la cuenta del primero, pero ambas, la del cliente y la del desarrollador, indican la misma cuenta de PayPal para transferir o sacar dinero (se pagan a sí mismos con su propio dinero);
- Uso frecuente de plantillas de documentos para cosas como documentos de licitación y métodos de comunicación en el marco de un proyecto, en particular cuando se utilizan las mismas plantillas en diferentes cuentas de desarrollador;
- Varias cuentas de desarrolladores que reciben calificaciones altas de un cliente en un corto periodo de tiempo con documentación similar o idéntica que se usa para crear las cuentas de los desarrolladores o la cuenta del cliente;
- Muchas licitaciones para proyectos, pero un bajo número de aceptaciones en comparación a la cantidad de proyectos a los que el desarrollador ha licitado; y
- Transferencias de dinero frecuentes mediante plataformas de pago, especialmente a cuentas bancarias ubicadas en la República Popular China y, a veces, enviadas a través de una o más empresas para ocultar el destino último de los fondos.

Las empresas que dan trabajo a los autónomos deben ser conscientes de que la siguiente actividad puede ser un indicador de la conducta propia de los técnicos informáticos de la RPDC.

- Si el sitio web de desarrollo de software independiente o la cuenta de la plataforma de pago se ha suspendido o el trabajador contacta con el empleador pidiéndole usar una cuenta diferente, especialmente si está registrada con un nombre diferente;

- Uso de servicios digitales de pago, especialmente servicios vinculados a la República Popular China

- 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, las cuentas en las plataformas de pago y el análisis de su ubicación y horarios;

- Sitios web de portafolios, perfiles de medios sociales o de desarrolladores con unos diseños extrañamente sencillo;

- Mensajes directos o llamadas no solicitadas de personas que fingen ser ejecutivos de alto nivel de empresas desarrolladoras de software para solicitar servicios o promocionar sus habilidades;

- Solicitud de comunicarse con clientes y potenciales clientes a través de una plataforma diferente al sitio web de la plataforma para autónomos donde el cliente encontró al técnico informático;

- Un empleado propone enviar documentos o equipos relacionados con el trabajo, como puede ser una computadora portátil al desarrollador, y este pide que se envíe a una dirección que no aparece en los documentos de identificación del desarrollador. Se debe sospechar, especialmente, si el desarrollador afirma que no pueden recibir material en la dirección que consta en sus documentos de identificativos.

- Intentar recibir el pago en divisa virtual en un esfuerzo para evadir las medidas KYC y AML y el uso del sistema financiero habitual;

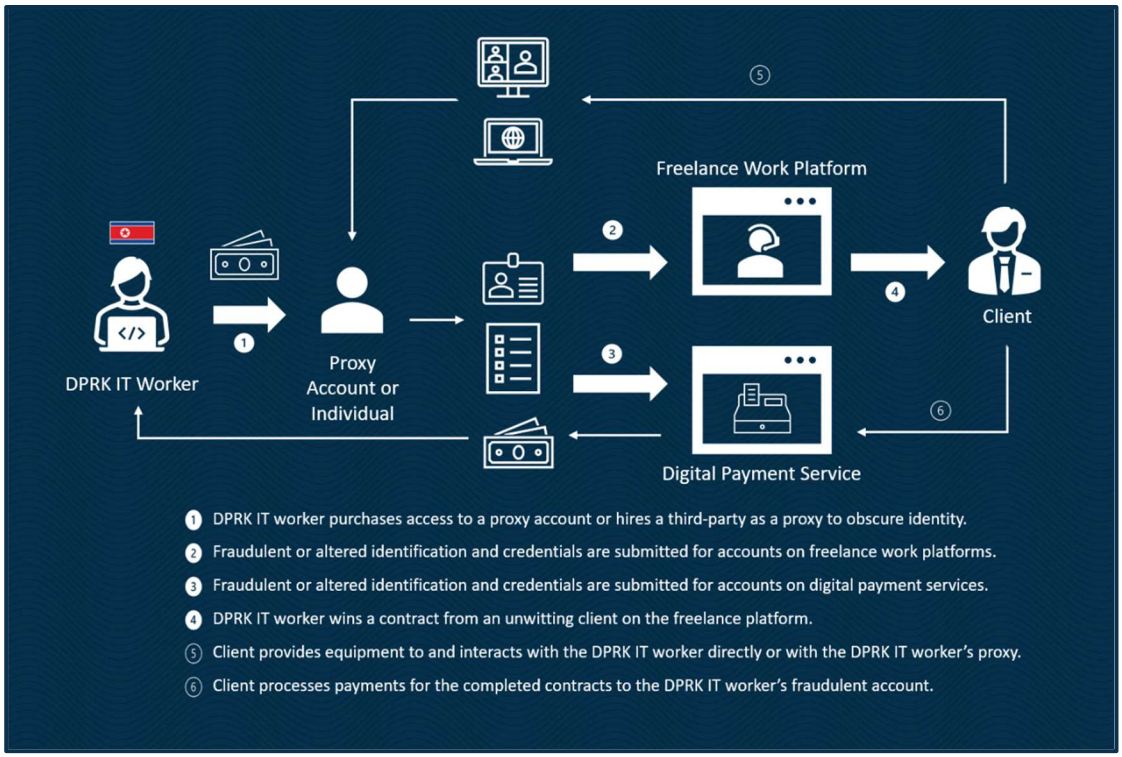
- Solicitar el pago de los contratos sin cumplir los parámetros de la producción o los requisitos de facturación;

- Falta de disponibilidad para trabajar durante el horario de oficina normal;

- Datos de contactos incorrecto o que cambian, en particular, el número de teléfono y las direcciones de correo electrónico;

- Información bibliográfica que parece no coincidir con el postulante;
- Problemas a la hora de completar tareas en un plazo adecuado o de responder a ellas;
- Imposibilidad de contactar con ellos en un periodo de tiempo adecuado, especialmente a través de formas de comunicación «inmediata»; y
- Pedirles a los compañeros que les faciliten algunos de sus datos personales para conseguir otros contratos.

Compendio de las operaciones de los técnicos informáticos de la RPDC



MEDIDAS POTENCIALES DE MITIGACIÓN

Para las empresas de las plataformas de trabajo para autónomos y de pago

- Verificar los documentos que se han recibido en el marco de los exámenes de propuestas y los procedimientos de contratación diligentemente, como examinar las facturas una a una y los contratos de trabajo contactando con los clientes enumerados a través de los datos de contacto indicados en las bases de datos empresariales y no los proporcionados en la documentación recibida;

- Examinar atentamente los documentos de identidad enviados para detectar fraudes y extendiendo el proceso a las autoridades locales en caso necesario para que se cumplan las leyes. Rechazar fotos de baja calidad enviadas para verificar la identidad;

- Comprobar la existencia de todos los sitios web facilitados para crear las cuentas: mejorar la investigación para detectar cualquier cuenta que haya utilizado sitios web inactivos para crear las cuentas.

- Como parte de los procesos iniciales de diligencia debida de contratación y las normas de renovación, solicitar el envío de un video para verificar la identidad o realizar una entrevista por videoconferencia para comprobarla;

- Utilizar frecuentemente funciones de control de puertos para detectar si se está accediendo a la plataforma de forma remota a través de un software para conectarse a un escritorio remoto, de una VPN o de VPS, en especial si el empleo de este software o de VPN para acceder a las cuentas no es una práctica común;

- Marcar automáticamente las cuentas del cliente y el desarrollador para una inspección adicional en el caso de que usen la misma documentación o similar para crear las cuentas o que utilicen las mismas cuentas de servicio de pago digital;

- Marcar automáticamente para una inspección adicional en el caso de que diferentes cuentas de desarrolladores usen las mismas plantillas de documentos, o parecidas, para licitar y para la comunicación en el marco del proyecto;

- Marcar automáticamente, para una inspección adicional, varias cuentas de desarrolladores que reciban calificaciones altas de un único cliente en un corto periodo de tiempo, especialmente si se empleó documentación similar o idéntica para crear las cuentas;

- Marcar automáticamente las cuentas de los desarrolladores con unas tarifas de licitación altas para una inspección adicional, así como aquellas cuentas con una cantidad de aceptaciones de licitaciones para proyectos baja en comparación con la cantidad de proyectos a los que se ha licitado. Además, marcar las cuentas con una cifra relativamente alta de licitaciones para proyectos en relación con la cantidad de inicios de sesión;

- No permitir ninguna actividad en una cuenta de reciente creación antes de una verificación completa de esta;

- Examinar con especial atención las cuentas nuevas; y

Para las empresas que dan trabajo a programadores y desarrolladores en plataformas para autónomos

- Realizar entrevistas por videoconferencia para comprobar la identidad de un potencial empleado externo;

- Llevar a cabo una verificación de los antecedentes previa a la contratación, una prueba de estupefacientes y un registro de huella dactilar o biométrico para comprobar la identidad y la supuesta ubicación. Evitar pagar en divisa virtual y solicitar la verificación de la información bancaria correspondiente en los demás documentos identificativos;

- Tener especial precaución al interactuar con desarrolladores autónomos a través de aplicaciones de colaboración a distancia, como las aplicaciones de escritorio remoto. Considerar deshabilitar las aplicaciones de colaboración a distancia en cualquier ordenador que se suministre a un desarrollador autónomo;

- Verificar el historial de educación superior y la experiencia profesional directamente con las instituciones educativas y las empresas enumeradas a través de los datos de contacto encontrados en un motor de búsqueda u otras bases de datos empresariales y no usando los datos obtenidos directamente del potencial empleado o recopilados en su perfil;

- 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 potencial candidato son consistentes entre sus perfiles en 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. Tener especial precaución con los sitios web de portafolios, perfiles de medios sociales o de desarrolladores con unos diseños sencillos;

- Tener especial precaución cuando un desarrollador solicita continuar la comunicación en una plataforma diferente a la del sitio web en la que la empresa encontró al técnico informático por primera vez;

- Si se deben enviar documentos o equipo relacionado con el trabajo, como una computadora portátil, a un desarrollador, hacerlo solo a la dirección indicada en los documentos de identificación y conseguir documentación adicional si el desarrollador pide que la computadora portátil o cualquier otro material se envíe a una dirección que no figure en sus documentos identificatorios. Se debe sospechar si el desarrollador no puede recibir material en la dirección que consta en sus documentos identificatorios; y

- Estar atento ante transacciones de pequeño tamaño y sin autorización efectuadas por técnicos informáticos contratados que puedan ser fraudulentas. En un caso, los técnicos informáticos de la RPDC contratados como desarrolladores por una empresa de los EE. UU. realizaron un cargo fraudulento a esta última y robaron más de 50 000 dólares en 30 pequeñas cuotas en cuestión de meses. La empresa estadounidense no se percató de que los desarrolladores eran norcoreanos ni del robo en marcha debido a las pequeñas sumas.

CONSECUENCIAS DE INVOLUCRARSE EN COMPORTAMIENTOS PROHIBIDOS O SANCIONABLES

Las personas físicas y las entidades que se involucren o que apoyen las actividades relacionadas con los técnicos informáticos de la RPDC, incluido procesar transacciones financieras vinculadas, deben ser conscientes de las potenciales consecuencias legales de involucrarse en comportamientos prohibidos o sancionables.

Las resoluciones 2321, 2371 y 2397 del Consejo de Seguridad de la ONU subrayan que los ingresos que los trabajadores de Corea del Norte generan en el extranjero financian los programas de armamento nuclear y misiles balísticos de la RPDC. La resolución 2375 del Consejo de Seguridad de la ONU prohíbe a los Estados miembros conceder nuevos permisos de trabajo o renovar los expirados a los ciudadanos de la RPDC en sus jurisdicciones en relación con el acceso a sus territorios, a menos que las haya aprobado el Comité 1718 del Consejo de Seguridad de la ONU previamente. La resolución 2397 del Consejo de Seguridad de la ONU solicita a todos los Estados miembros que repatrien a los ciudadanos norcoreanos que reciben ingresos en sus jurisdicciones antes del 22 de diciembre de 2019, sin importar cuándo o si se concedieron permisos de trabajo a estos ciudadanos de la RPDC.

La Oficina de Control de Activos Extranjeros del Departamento del Tesoro (OFAC) es competente para imponer sanciones económicas a cualquier persona de la que se determine, entre otras cosas:

- Haberse involucrado en actividades significativas en nombre del Gobierno de la RPDC o del Partido de los Trabajadores de Corea que entrañen un peligro para la ciberseguridad;
- Haber trabajado en nombre de la RPDC en la industria informática;
- En ciertos casos, haberse involucrado en otras actividades que hayan posibilitado ciberoperaciones maliciosas;
- Haberse involucrado en, al menos, una importación o exportación a la RPDC de cualquier bien, servicio o tecnología;
- Haber vendido, suministrado, transferido o adquirido software, directamente o indirectamente, a o de la RPDC o cualquier persona que actúe para o en nombre del Gobierno de Corea del Norte o del Partido de los Trabajadores de Corea, en cuya operación, cualquier ingreso o bien recibido pueda beneficiar al Gobierno de la RPDC o al Partido de los Trabajadores de Corea; o
- Haber ayudado materialmente, patrocinado o proporcionado apoyo tecnológico, material o económico, bienes o servicios a o en apoyo del Gobierno de la RPDC o el Partido de los Trabajadores de Corea.

Por ejemplo, en 2018, los Estados Unidos aplicó sanciones a la empresa tecnológica con sede en China, Yanbian Silverstar Network Technology Co., Ltd. Esta empresa era, teóricamente, una empresa china de la industria informática, pero, en realidad, estaba gestionada y controlada por norcoreanos. La mencionada empresa, además, creó una sociedad fantasma con sede en Rusia, Volasys Silver Star, con el fin de eludir los requisitos de identificación en los foros de trabajo para autónomos.

Además, el Secretario del Tesoro, tras consultar con el Secretario de Estado, determina si una institución financiera extranjera ha comerciado o facilitado, deliberadamente, operaciones comerciales relevantes con la RPDC o ha realizado o facilitado intencionadamente una transacción significativa en nombre de una persona designada en virtud de un decreto de Corea del Norte o de conformidad con el Decreto 13382 (Personas que facilitan o apoyan la proliferación de armas de destrucción masiva) en conjunto con la actividad vinculada a la RPDC. Esa institución podría, entre otras restricciones potenciales, perder el permiso para mantener una cuenta bancaria corresponsal o empleada para pagos en los Estados Unidos.

La OFAC investiga las infracciones aparentes de sus sanciones, reglamentos y cumple la función de autoridad ejecutiva, como se describe en la Economic Sanctions Enforcement Guidelines [Directrices para la Aplicación de Sanciones económicas], título 31 del Código de Reglamentos Federales, parte 501, apéndice A. Las personas que infrinjan el Reglamento de Sanciones a Corea del Norte, título 31 del Código de Reglamentos Federales, parte 510, pueden enfrentarse a sanciones económicas civiles hasta las penas máximas previstas aplicables o hasta el doble del valor de la transacción subyacente.

Además, la Ley estadounidense para contrarrestar a adversarios a través de sanciones (CAATSA; Ley Pública 115-44) Art. 321(b) (Título 22 del Código de los Estados Unidos, Art. 9241a), que modificó la Ley de Sanciones y Mejoras de Políticas de Corea del Norte de 2016 (Título 22 del Código de los Estados Unidos, Art. 9241 y siguientes), estableció una presunción refutable de que bienes, mercancías, mercaderías y productos significativos extraídos, producidos o manufacturados, totalmente o en parte, por ciudadanos norcoreanos en cualquier parte del mundo son bienes procedentes de mano de obra forzosa que se prohíben importar en virtud de la Ley de Aranceles de 1930 (Título 19 del Código de los Estados Unidos, Art. 1307). Esto implica que esos bienes no tienen autorización para entrar en ningún puerto de los Estados Unidos y pueden estar sujetos a detención, incautación y confiscación. Las violaciones pueden dar lugar a sanciones civiles, además de procesamiento penal. Sin embargo, en virtud de la CAATSA, estos bienes pueden importarse a los Estados Unidos si el Comisario de Aduanas y Protección de Fronteras de los EE. UU. (CBP) determina mediante pruebas claras y convincentes que los bienes no se han producido usando mano de obra de presos, forzosa o mano de obra en condiciones de esclavitud. La prohibición de importar bienes producidos mediante mano de obra de presos, forzosa o mano de obra en condiciones de esclavitud bajo pena (incluidas la mano de obra infantil forzosa o en condiciones de esclavitud) se estableció conforme a la Ley de Aranceles de 1930 y ha permanecido vigente durante casi 90 años.

El Departamento de Justicia es responsable de la investigación y la ejecución de las leyes federales aplicables, incluida la Ley de Poderes Económicos en Caso de Emergencia Internacional (IEEPA),

título 50 del Código de los Estados Unidos, Art. 1701 y siguientes y la Ley de Secreto Bancario (BSA), título 31 del Código de los Estados Unidos, Art. 5318 y 5322. De conformidad con la IEEPA, es un delito infringir, intentar infringir, conspirar para infringir o causar una infracción intencionada de cualquier autorización, orden, reglamento o prohibición emitida por la IEEPA para incluir cualquier decreto relacionada con la RPDC (p. ej.: Decretos 13722 y 13810), Decreto 13382 y el Reglamento de Sanciones de Corea del Norte, 31 C.F.R. parte 510. Las personas que infrinjan intencionadamente la IEEPA se enfrentan a penas de prisión de hasta 20 años, penas económicas de hasta 1 millón de dólares o un total del doble de las ganancias brutas, la sanción económica mayor de los dos, y la confiscación potencial de todos los fondos involucrados en las transacciones en cuestión. La BSA exige a las instituciones financieras, entre otras cosas, mantener programas efectivos antiblanqueo de dinero y archivar determinados informes en la FinCEN (Control de delitos financieros). Las personas que infrinjan la BSA pueden enfrentarse a penas de prisión de hasta 5 años, penas económicas de hasta 250 000 dólares y la confiscación potencial de los bienes involucrados en las violaciones en cuestión. Las sociedades y demás entidades que infrinjan la IEEPA, la BSA y las demás leyes federales aplicables también pueden ser procesadas penalmente. El Departamento de Justicia también colabora con socios extranjeros para compartir pruebas y apoyar las investigaciones y los procedimientos penales en los Estados Unidos y en el extranjero.

En virtud del título 31 del Código de los Estados Unidos art. 5318(k), el Secretario del Tesoro o el fiscal general pueden citar a juicio a una institución financiera extranjera que mantenga una cuenta bancaria corresponsal en los Estados Unidos con informes almacenados en el extranjero. Si el Secretario de Estado o el fiscal general facilita una notificación por escrito a una institución financiera de los EE. UU. de que una institución financiera extranjera no se ha presentado a la mencionada citación judicial, la institución financiera de los EE. UU. debe suspender la relación bancaria corresponsal en un plazo de diez días hábiles. Un incumplimiento de esta orden puede llevar a la institución financiera de los EE. UU. a sanciones civiles diarias.

RECOMPENSAS POR LA JUSTICIA RPDC

Si cuenta con información sobre actividades ilícitas de la RPDC en el ciberespacio, incluidas operaciones pasadas o en marcha, proporcionar esa información a través del programa Recompensas por la Justicia del Departamento de Estado podría hacerlo apto para recibir una compensación de hasta 5 millones de dólares. Para obtener más información, visite https://rewardsforjustice.net/index/?north-korea=north-korea.

APÉNDICE

Grupo de expertos de las Naciones Unidas que informa sobre los técnicos informáticos de la RPDC

En lo relativo a la RPDC, al Comité de Sanciones 1718 del Consejo de Seguridad de la ONU lo apoya un Grupo de Expertos que recopila, examina y analiza la información procedentes de los Estados miembros de la ONU, las instituciones relevantes de la ONY y otras partes para la implementación de las medidas descritas en las Resoluciones del Consejo de Seguridad de la ONU relacionadas con Corea del Norte. El Grupo de Expertos también recomienda sobre cómo mejorar la implementación de las sanciones proporcionando tanto un informe de mitad de periodo como otro final al Comité 1718. Esto informes se pueden consultar en https://www.un.org/securitycouncil/es/sanctions/1718/panel_experts/reports

El Grupo de Expertos ha investigado múltiples casos de técnicos informáticos de la RPDC, como los subordinados al departamento de industria de municiones (MID) señalados por la ONU y presentado la información sobre estas investigaciones en los informes semestrales del Grupo de Expertos, incluidos los siguientes:

La primera información del Grupo de Expertos sobre los técnicos informáticos de la RPDC en el informe de mitad de periodo de 2019 observaba que el MID, que había sido señalado por su papel supervisor en el desarrollo de los programas nuclear y de misiles balísticos de Corea del Norte, estaba sirviéndose de sus sociedades comerciales subordinadas para destinar al extranjero a técnicos informáticos de la RPDC, como programadores y desarrolladores de software, con el fin de adquirir divisas extranjeras. En ese momento, los técnicos informáticos norcoreanos ubicados en Europa, Asia, África y Medio Oriente estaban utilizando sitios web extranjeros para conseguir trabajo como autónomos mientras que ocultaban su identidad. Además del trabajo no malicioso en el campo de la informática, los técnicos informáticos de la RPDC realizaban tareas ilícitas que incluían el robo de activos, como divisas virtuales, para ayudar a los ciberagentes de Corea del Norte a eludir las sanciones económicas.

El Grupo de Expertos continuó con su investigación sobre los técnicos informáticos de la RPDC en su informe final de 2020, y descubrió que la mayoría de los informáticos de Corea del Norte eran contratados por empresas subordinadas al MID. Hacia 2019, se sospechaba que el MID había desplegado, al menos, 1000 técnicos informáticos en el extranjero con el fin de generar ingresos usando, frecuentemente, entidades subordinadas o sociedades fantasma. Sin embargo, debido a sus técnicas para ocultar información, la cifra verdadera de técnicos informáticos en el extranjero y en la RPDC no era clara. El Grupo de Expertos observó que los técnicos informáticos de la RPDC emplean varios métodos para conseguir trabajo para informáticos autónomos sin revelar su identidad, dentro de lo que se incluye crear cuentas en plataformas para desarrolladores autónomos con clientes de todo el mundo que no eran conscientes de lo que hacían, especialmente, clientes en China, Rusia, Ucrania, Serbia, Canadá y los Estados Unidos. El Grupo de Expertos investigó con mayor detalle varios casos

específicos de equipos de técnicos informáticos y empresas vinculadas a la RPDC en China, Nepal y Vietnam.

El Grupo de Expertos investigó a cierta cantidad de equipos de técnicos informáticos de la RPDC en China y Rusia y enumeró sus investigaciones en su informe de mitad de periodo de 2020. El Grupo de Expertos observó que cientos de técnicos informáticos de la RPDC subordinados al MID estaban operando en China en 2019 y 2020, obteniendo accesos ilícitos a cuentas de plataformas para autónomos a nombre de terceros de otros países. Además, el Grupo de Expertos también descubrió que múltiples grupos de técnicos informáticos de la RODC subordinados al MID estaban operando en Rusia en 2019 y 2020, usando identidades extranjeras falsas para conseguir acceso a las plataformas para informáticos autónomos, a los sitios web de divisas virtuales y de pago.

Según el informe final de 2021 del Grupo de Expertos, los técnicos informáticos de la RPDC pueden eludir los esfuerzos diligentes debidos de los empleados y los protocolos KYC y AML sirviéndose de técnicas de ocultación similares a las que utiliza Corea del Norte para acceder al sistema financiero internacional, dentro de lo que se incluye proporcionar identificación falsa, usar servicios VPN y crear sociedades fantasma. El Grupo de Expertos también observó que la mayoría de las cuentas ligadas a la RPDC operan desde localidades chinas. Con el fin de evitar ser investigados, los usuarios de estas cuentas quieren «salir de la plataforma» tras contactar con clientes potenciales en busca de contratar servicios en informática. Los usuarios vinculados a Corea del Norte también dirigen sus esfuerzos a las plataformas de trabajo para informáticos autónomos con niveles de seguridad más bajos o procedimientos de diligencia debida menos exigentes. El Grupo de Expertos destacó, específicamente, los peligros a los que se enfrentan las plataformas de trabajo para informáticos autónomos en el ejercicio de cumplir sus obligaciones y posibilitar, accidentalmente, a la RPDC el acceso a los sistemas de pago internacionales, y recomienda a los Estados miembros de la ONU que colaboren con las empresas independientes del sector de la informática para fomentar y mejorar las capacidades y las aptitudes para implementar el cumplimiento de las sanciones.