Anuncio de Servicio Público

OFICINA FEDERAL DE INVESTIGACIONES

Número de alerta: I-051624-PSA
16 de mayo de 2024

La República Popular Democrática de Corea se aprovecha de personas basadas en EE.UU. para defraudar a empresas estadounidenses y generar ingresos

La Oficina Federal de Investigaciones (FBI) advierte al sector público y privado de la amenaza que representa para las empresas estadounidenses los trabajadores de tecnologías de información (TI) procedentes de la Republica Popular Democrática de Corea (Corea del Norte). Corea del Norte está evadiendo las sanciones de EE.UU. y de la ONU al enfocarse en empresas privadas para generar ilícitamente ingresos sustanciales para el régimen. Los trabajadores informáticos norcoreanos utilizan diversas técnicas para ofuscar sus identidades, entre ellas el aprovechamiento de personas radicadas en EE.UU., tanto a sabiendas o no para conseguir empleos fraudulentos y tener acceso a las redes de empresas estadounidenses con el fin de generar estos ingresos.

Estas personas, a sabiendas o no, basadas en EE.UU. proporcionan a las empresas una ubicación en Estados Unidos para el envío de dispositivos, que le permite a los trabajadores informáticos norcoreanos eludir los controles que las empresas puedan tener establecidos para impedir la contratación de trabajadores extranjeros ilícitos así como controles para impedir el acceso no autorizado a las redes de las empresas por parte de los trabajadores informáticos norcoreanos, por medio de la instalación no autorizada de software de acceso remoto. Las actividades de los trabajadores informáticos norcoreanos violan ilegalmente las sanciones de EE.UU. y la ONU y amenazan la seguridad de las empresas objetivo. Las empresas que subcontratan la manutención de su trabajo de TI a proveedores terceros pueden enfrentarse a vulnerabilidades adicionales, puesto que estas empresas están alejadas del proceso de contratación directa.

Los facilitadores basados en EE.UU. han proporcionado los siguientes servicios específicos a trabajadores informáticos norcoreanos:

- Una conexión a internet con base en EE.UU. habilitada a través de ordenadores portátiles de empresas estadounidenses recibidos en su nombre por facilitadores en los Estados Unidos;
- La configuración de infraestructura basada en EE.UU., incluyendo la habilitación de la conexión remota de escritorios a ordenadores portátiles de empresas estadounidenses por medio de protocolos o la descarga e instalación de software de conexión de escritorios remotamente;
- Reenvió de ordenadores portátiles de empresas estadounidenses a trabajadores informáticos norcoreanos en el extranjero;
- Creación de cuentas financieras para los trabajadores de TI norcoreanos. Algunos facilitadores radicados en EE.UU. reciben parte de los ingresos obtenidos por medio de estratagemas para el empleo de trabajadores de TI norcoreanos;
- Creación de cuentas en sitios populares de búsqueda de empleo para el uso de los trabajadores de TI norcoreanos;

- Asistencia en la compra y financiación de servicios en la web tales como, modelos de inteligencia artificial y programas de comprobación de antecedentes para uso de los trabajadores de TI norcoreanos;
- Asistencia a entrevistas y reuniones virtuales en nombre de trabajadores de TI norcoreanos; y
- La creación de empresas pantalla con sede en EE.UU., incluyendo empresas que pretenden ofrecer trabajadores técnicos contratados a corto plazo.

CONSEJOS PARA PROTEGER SU EMPRESA:

- Implemente procesos de verificación de identidad durante la contratación, la incorporación y el empleo de cualquier trabajador remoto.
- Eduque al personal de Recursos Humanos, a los responsables de contratación y a los equipos de desarrollo sobre esta amenaza.
- Monitorear los cambios de dirección de los solicitantes, especialmente después de la contratación, pero antes de que los ordenadores portátiles sean entregados a la dirección proporcionada por el solicitante.
- Observe el tráfico anormal en la red incluyendo, las conexiones remotas a dispositivos, y supervise los entornos para detectar la presencia de protocolos de escritorio remoto o software prohibido.
- Observe las incoherencias en las entrevistas, especialmente si los candidatos son incapaces de responder a preguntas sobre donde están localizados o a detalles importantes sobre su pasado.
- Observe un aumento del ruido durante las entrevistas o sonidos como si el solicitante estuviera rodeado de otras personas que realizan un trabajo similar.
- Verifique la información de identificación de todos los trabajadores a distancia en E-Verify.gov.
- Anote los errores derivados en el proceso de contratación de la comprobación de E-Verify y solicite una verificación en persona u otros medios de verificación confiables.
- Asegúrese de que las empresas de contratación de terceros lleven a cabo prácticas de contratación sólidas para cubrir los puestos de trabajo, hacen auditorías rutinarias sobre las prácticas de contratación y señalan los cambios de dirección o de plataformas de pago.

CONSEJOS PARA PROTEGERSE:

- Tenga cuidado con las ofertas aparentemente aleatorias en sitios de búsqueda de empleo y plataformas de redes sociales para puestos a distancia, cuentas compartidas y puestos de asistente virtual.
- Manténgase alerta con respecto a las ofertas de trabajo que impliquen la recepción de paquetes a cambio de parte de los ingresos derivados de trabajos afiliados a equipos entregados.
- Si recibe un formulario W-4, 1099-NEC, u otro formulario del IRS por un trabajo que usted no tenia, póngase en contacto con la empresa que se lo proporcionó, así como con el FBI.

- Considere la posibilidad de bloquear su identidad a través de E-Verify.gov para evitar que sea utilizado en fraudes de identidad relacionados con el empleo.

DENUNCIAS

Si usted es una empresa que ha sido víctima de la estafa de trabajadores TI norcoreanos o sospecha que usted o su empresa han sido contactados por un trabajador informático norcoreano, el FBI recomienda tomar las siguientes medidas:

- Informe inmediatamente al Centro de Denuncias de Delitos en el Internet del FBI (IC3) en www.IC3.gov.
- Evalué la actividad en la red del empleado sospechoso y su dispositivo asignado y utilice software de detección de intrusos para capturar la actividad en el dispositivo sospechoso.

REFERENCIA

En 2022 y 2023, Estados Unidos, junto con socios extranjeros, emitió avisos públicos relacionados con los trabajadores informáticos norcoreanos que describían su forma de operar y se proporcionaba indicadores de alerta junto con medidas de debida diligencia para que las empresas evitaran contratar a trabajadores informáticos norcoreanos. La República de Corea y el Gobierno de Japón también han alertado al público sobre los trabajadores informáticos norcoreanos.