Lazarus, el grupo patrocinado por el estado afiliado a Corea del Norte, está intentando nuevamente atacar a los investigadores de seguridad con puertas traseras y troyanos de acceso remoto utilizando una versión pirateada con troyanos del popular software de ingeniería inversa IDA Pro.

Los hallazgos fueron reportados por el investigador de seguridad de ESET, Anton Cherepanov, la semana pasada mediante Twitter.

IDA Pro es un desensamblador interactivo que está diseñado para traducir el lenguaje de la máquina (también conocido como ejecutables) al lenguaje ensamblador, lo que permite a los investigadores de seguridad analizar el funcionamiento interno de un programa (malicioso o de otro tipo) y funcionar como depurador para detectar errores.

> *«Los atacantes combinaron el software IDA Pro 7.5 original desarrollado por [Hex-Rays] con dos componentes maliciosos»*, dijo ESET.

Uno de estos componentes es un módulo interno llamado *«win_fw.dll»* que se ejecuta durante la instalación de la aplicación. Esta versión manipulada se orquesta luego para cargar un segundo componente llamado *«idahelper.dll»* desde la carpeta de complementos IDA en el sistema.

Tras la ejecución exitosa, el binario *«idahelper.dll»* se conecta a un servidor remoto en *«www[.]Devguardmap[.]org»* para recuperar cargas útiles posteriores. El dominio también se destaca por el hecho de que se vinculó previamente a una campaña similar respaldada por Corea del Norte dirigida a profesionales de la seguridad y divulgada por el Grupo de Análisis de Amenazas de Google a inicios de marzo.

La operación encubierta involucró a los adversarios que establecieron una compañía de seguridad falsa conocida como SecuriElite junto con una serie de cuentas de redes sociales en Twitter y LinkedIn en un intento de engañar a los investigadores desprevenidos para que visitaran el sitio web de la compañía con malware para desencadenar un exploit que

aprovechó un Zero Day en el navegador Internet Explorer. Microsoft finalmente abordó el problema en su actualización del martes de parches para marzo de 2021.

También conocido como APT38, Hidden Cobra y Zinc, el Grupo Lazarus es conocido por estar activo desde 2009 y vinculado a una serie de ataques para obtener ganancias financieras y recopilar información confidencial en los entornos comprometidos.

«El programa cibernético de Corea del Norte plantea una creciente amenaza de espionaje, robo y ataque», según la Evaluación Anual de Amenazas 2021 de la Oficina del Director de Inteligencia Nacional de Estados Unidos publicada a inicios de abril.

> *«Corea del Norte ha realizado robos cibernéticos contra instituciones financieras e intercambios de criptomonedas en todo el mundo, robando potencialmente cientos de millones de dólares, probablemente para financiar prioridades gubernamentales, como sus programas nucleares y misiles».*