Se ha detectado una reciente campaña engañosa que está tomando el control de cuentas en GitHub y efectuando código malicioso camuflado como contribuciones de Dependabot, con el objetivo de sustraer contraseñas de desarrolladores.

> Según un informe técnico de Checkmarx, *«el código malicioso extrae las secretas definidas en el proyecto de GitHub y modifica cualquier archivo JavaScript existente en el proyecto atacado con un código de malware para robar contraseñas de formularios web, afectando a cualquier usuario final que introduzca su contraseña en un formulario web».*

Este malware también está diseñado para capturar secretos y variables de GitHub y enviarlos a un servidor remoto utilizando una Acción de GitHub.

La compañía especializada en seguridad de la cadena de suministro de software señaló que se observaron compromisos atípicos en cientos de repositorios de GitHub, tanto públicos como privados, entre el 8 y el 11 de julio de 2023.

Se ha descubierto que las víctimas tuvieron sus tokens de acceso personal de GitHub sustraídos y utilizados por los actores de amenazas para realizar commits de código falsificados en los repositorios de los usuarios, haciéndose pasar por Dependabot.

Dependabot está diseñado para alertar a los usuarios sobre las vulnerabilidades de seguridad en las dependencias de un proyecto, generando automáticamente solicitudes de extracción para mantenerlas actualizadas.

Según la empresa, *«los atacantes accedieron a las cuentas utilizando tokens de acceso personal comprometidos, probablemente extraídos silenciosamente del entorno de desarrollo de la víctima»*. La mayoría de los usuarios comprometidos se encuentran en Indonesia.

No obstante, en este momento no está claro el método exacto mediante el cual se llevó a cabo este robo, aunque se sospecha que pudo haber involucrado la instalación inadvertida de

un paquete malicioso por parte de los desarrolladores.

Este incidente pone de manifiesto los continuos esfuerzos por parte de actores de amenazas para corromper los ecosistemas de código abierto y facilitar compromisos en la cadena de suministro.

Esto se refleja en una nueva campaña de exfiltración de datos que apunta tanto a npm como a PyPI y que utiliza hasta 39 paquetes falsos para recopilar información sensible de las máquinas y transmitir los detalles a un servidor remoto.

Los módulos, publicados durante varios días entre el 12 y el 24 de septiembre de 2023, demuestran un aumento progresivo en complejidad, alcance y técnicas de ocultación, según Phylum, una empresa de seguridad.

Además, Phylum también está rastreando lo que califican como una gran campaña de typosquat dirigida a npm, en la que se utilizan 125 paquetes que se hacen pasar por angular y react para enviar información de la máquina a un canal remoto de Discord.

Sin embargo, parece que esta actividad forma parte de un *«proyecto de investigación»*, ya que el autor afirma que lo hace para *«averiguar si alguno de los programas de recompensas por errores en los que participo se ve afectado por uno de los paquetes, con el fin de ser el primero en notificarlos y proteger su infraestructura».*

Phylum advierte que *«esto viola la Política de Uso Aceptable de npm, y este tipo de campañas ejercen presión sobre las personas encargadas de mantener estos ecosistemas limpios».*