Una nueva investigación encontró que es posible que los hackers abusen de una función legítima en GitHub Codespaces para enviar malware a los sistemas de las víctimas.

GitHub Codespaces es un entorno de desarrollo configurable basado en la nube, que permite a los usuarios depurar, mantener y confirmar cambios con un código base determinado desde un navegador web o mediante una integración en Visual Studio Code.

También cuenta con una función de reenvío de puertos que hace posible acceder a una aplicación web que se ejecuta en un puerto particular dentro del espacio de código directamente desde el navegador en una máquina local para fines de prueba y depuración.

> *«También puede reenviar un puerto manualmente, etiquetar puertos reenviados, compartir puertos reenviados con miembros de su organización, compartir puertos reenviados públicamente y agregar puertos reenviados a la configuración del espacio de código»*, dice GitHub en su documentación.

Es importante tener en cuenta que cualquier puerto reenviado que se haga público también permitirá que cualquier parte con conocimiento de la URL y el número de puerto vea la aplicación en ejecución sin ninguna autenticación.

Además, GitHub Codespaces usa HTTP para el reenvío de puertos. Si el puerto visible públicamente se actualiza para usar HTTPS o se elimina y se vuelve a agregar, la visibilidad del puerto cambia de forma automática a privado.

La compañía de seguridad cibernética Trend Micro descubrió que dichos puertos reenviados compartidos públicamente podrían explotarse para crear un servidor de archivos malicioso usando una cuenta de GitHub.

> *«En el proceso, estos entornos abusados no se marcarán como maliciosos o sospechosos, incluso cuando presenten contenido malicioso (como secuencias de comandos, malware y ransomware, entre otros), y las organizaciones pueden considerar estos eventos como benignos o falsos positivos»,* dijeron los investigadores Nitesh Surana y Magno Logan.

En un exploit de prueba de concepto (PoC) demostrado por Trend Micro, un atacante podría crear un espacio de código y descargar malware desde un dominio controlado por un atacante al entorno, y configurar la visibilidad del puerto reenviado como público, transformando esencialmente la aplicación para que actúe como un servidor web que aloja cargas no autorizadas.

Aún más preocupante, el atacante puede aumentar este método para implementar malware y comprometer el entorno de la víctima, ya que cada dominio de espacio de código asociado con el puerto expuesto es único y es poco probable que las herramientas de seguridad lo marquen como un dominio malicioso.

> *«Al usar dichos scripts, los atacantes pueden abusar fácilmente de GitHub Codespaces para entregar contenido malicioso a un ritmo rápido al exponer los puertos públicamente en sus entornos de codesapace»,* dijeron los investigadores.

Aunque la técnica todavía no se observa en la naturaleza, los hallazgos son un recordatorio de cómo los hackers podrían armar las plataformas en la nube para su beneficio y llevar a cabo una serie de actividades maliciosas.

> *«Los servicios en la nube ofrecen ventajas tanto para los usuarios legítimos como para los atacantes. Las funciones que se ofrecen a los suscriptores legítimos también están disponibles para los atacantes, ya que aprovechan los recursos proporcionados por el proveedor de servicios en la nube»,* agregaron los

> investigadores.