La plataforma de alojamiento de código, GitHub, anunció de forma oficial este viernes una serie de actualizaciones de las políticas del sitio que profundizan sobre cómo la compañía trata el malware y el código de explotación cargado en su servicio.

> *«Permitimos explícitamente las tecnologías de seguridad de doble uso y contenidos relacionados con la investigación de vulnerabilidades, malware y exploit. Entendemos que muchos proyectos de investigación de seguridad en GitHub son de doble uso y ampliamente beneficiosos para la comunidad de seguridad. Asumimos la intención y el uso positivos de estos proyectos para promover e impulsar mejoras en todo el ecosistema»,* dijo la compañía.

Al afirmar que no se permitirá el uso de GitHub en apoyo directo a ataques ilegales o campañas de malware que causen daños técnicos, la compañía dijo que puede tomar medidas para interrumpir los ataques en curso que aprovechen la plataforma como un exploit o una red de entrega de contenido de malware (CDN).

Con ese fin, los usuarios se abstienen de cargar, publicar, alojar o trasmitir cualquier contenido que pueda utilizarse para entregar ejecutables maliciosos, o abusar de GitHub como una infraestructura de ataque, por ejemplo, organizando ataques de denegación de servicio (DoS) o administrando servidores de comando y control (C2).

> *«Daños técnicos significa el consumo excesivo de recursos, daño físico, tiempo de inactividad, denegación de servicio o pérdida de datos, sin un propósito de doble uso implícito o explícito antes de que ocurra el abuso»,* dijo GitHub.

En algunos escenarios en lo que existe un abuso activo y generalizado de contenido de doble uso, la compañía dijo que podría restringir el acceso a dicho contenido colocándolo detrás de las barreras de autenticación y, como último recurso, deshabilitar el acceso o eliminarlo por completo cuando haya otra restricción. GitHub también dijo que se pondría en contacto con

los propietarios de proyectos relevantes sobre los controles implementados cuando sea posible.

Los cambios entraron en vigencia luego de que la compañía, a fines de abril, comenzara a solicitar comentarios sobre su política de investigación de seguridad, malware y exploits en la plataforma con el objetivo de operar bajo un conjunto de términos más claros que eliminarían la ambigüedad que rodea a *«contenido activamente dañino y código en reposo»* en apoyo de la investigación de seguridad.

Al no eliminar los exploits a menos que el repositorio o el código en cuestión se incorpore directamente en una campaña activa, la revisión de las políticas de GitHub también es un resultado directo de las críticas generalizadas que siguieron a las consecuencias de un código de exploit de prueba de concepto (PoC) que se retiró de la plataforma en marzo de 2021.

El código, subido por un investigador de seguridad, se refería a un conjunto de fallas de seguridad conocidas como ProxyLogon, que Microsoft reveló que estaban siendo abusadas por grupos de hackers patrocinados por el estado chino, con el fin de violar los servidores de Exchange en todo el mundo. Ahora, GitHub dijo que eliminó el PoC de acuerdo con sus políticas de uso aceptable, citando que incluía código *«para una vulnerabilidad recientemente revelada que está siendo explotada activamente».*