La prevalencia de GitHub en entornos de tecnología de la información (TI) lo ha convertido en una opción atractiva para actores malintencionados que desean alojar y distribuir cargas maliciosas, así como fungir como resolutores de dead drop, puntos de comando y control, y puntos de exfiltración de datos.

> Según un informe compartido por Recorded Future, *«La utilización de los servicios de GitHub para infraestructura maliciosa permite a los adversarios mimetizarse con el tráfico de red legítimo, eludiendo a menudo las defensas de seguridad convencionales y complicando el rastreo de la infraestructura aguas arriba y la atribución del actor».*

La firma de ciberseguridad ha denominado a esta estrategia como «vivir de sitios confiables» (LOTS), una variante de las técnicas de «vivir de la tierra» (LotL) que suelen adoptar los actores maliciosos para ocultar sus actividades fraudulentas y pasar desapercibidos.

En cuanto a los métodos de abuso de GitHub, destaca la entrega de cargas útiles, donde algunos actores aprovechan sus funcionalidades para la obfuscación del comando y control (C2). En el último mes, ReversingLabs detalló varias instancias de paquetes de Python maliciosos que dependían de un gist secreto alojado en GitHub para recibir comandos malintencionados en los hosts comprometidos.

Aunque las implementaciones completas de C2 en GitHub son poco comunes en comparación con otros esquemas de infraestructura, su utilización por parte de actores malintencionados como resolutores de dead drop, donde la información de un repositorio de GitHub controlado por el actor se utiliza para obtener la URL real de C2, es mucho más frecuente, como se evidencia en el caso de malware como Drokbk y ShellBox.

También se observa raramente el mal uso de GitHub para la exfiltración de datos, probablemente debido a limitaciones de tamaño de archivo y almacenamiento, así como a preocupaciones sobre la detección.

Además de estos cuatro esquemas principales, las ofertas de la plataforma se utilizan de diversas maneras para cumplir con propósitos relacionados con la infraestructura. Por ejemplo, las GitHub Pages se han utilizado como hosts de phishing o redireccionadores de tráfico, y algunas campañas han empleado un repositorio de GitHub como canal de C2 de respaldo.

Este desarrollo refleja la tendencia general de que servicios de internet legítimos como Google Drive, Microsoft OneDrive, Dropbox, Notion, Firebase, Trello y Discord sean explotados por actores malintencionados. Esto incluye también otras plataformas de control de versiones y código fuente como GitLab, BitBucket y Codeberg.

> *«La detección de abusos en GitHub no tiene una solución universal. Se requiere una combinación de estrategias de detección, influenciadas por entornos específicos y factores como la disponibilidad de registros, la estructura organizativa, los patrones de uso del servicio y la tolerancia al riesgo, entre otros»,* afirmó la empresa.