Se ha observado a un atacante con sede en Sudáfrica conocido como Automated Libra, empleando tácticas de omisión de CAPTCHA para crear cuentas de GitHub de forma programática como parte de una campaña de hacking denominada PURPLEURCHIN.

El grupo *«se dirige principalmente a las plataformas en la nube que ofrecen pruebas de tiempo limitado de los recursos de la nube para realizar sus operaciones de criptominería»,* dijeron los investigadores de Unit 41 de Palo Alto Networks, William Gamazo y Nathaniel Quist.

PURPLEURCHIN salió a la luz por primera vez en octubre de 2022 cuando Sysdig reveló que el adversario creó hasta 30 cuentas de GitHub, 2000 cuentas de Heroku y 900 cuentas de Buddy para escalar su operación.

Ahora, según Unit 42, el grupo de hackers en la nube creó de tres a cinco cuentas de GitHub cada minuto en el apogeo de su actividad en noviembre de 2022, configurando totalmente más de 130,000 cuentas falsas en Heroku, Togglebox y GitHub.

Se estima que se crearon más de 22,000 cuentas de GitHub entre septiembre y noviembre de 2022: tres en septiembre, 1652 en octubre y 20,725 en noviembre. También se identificaron un total de 100,723 cuentas únicas de Heroku.

La compañía de ciberseguridad también calificó el abuso de los recursos de la nube como una táctica de *«jugar y correr»* diseñada para evitar pagar la factura del proveedor de la plataforma mediante el uso de tarjetas de crédito falsificadas o robadas para crear cuentas premium.

Su análisis de 250 GB de datos muestra la señal más temprana de la criptocampaña hace al menos casi 3.5 años en agosto de 2019, además de descubrir el uso de más de 40 billeteras y siete criptomonedas diferentes.

La idea central que sustenta a PURPLEURCHIN es la explotación de los recursos computacionales asignados a cuentas gratuitas y premium en servicios en la nube para obtener ganancias monetarias a gran escala antes de perder el acceso por falta de pago de las cuotas.

Además de automatizar el proceso de creación de cuentas al aprovechar herramientas legítimas como xdotool e ImageMagick, también se descubrió que el atacante aprovecha la vulnerabilidad dentro de la verificación de CAPTCHA en GitHub para promover sus objetivos ilícitos.

Esto se logra usando el comando de conversión de ImageMagick para transformar las imágenes CAPTCHA en sus complementos RGB, seguido del uso del comando de identificación para extraer la asimetría del canal rojo y seleccionando el valor más pequeño.

Una vez que la creación de la cuenta es exiosa, Automated Libra procede a crear un repositorio de GitHub e implementa flujos de trabajo que hacen posible lanzar scripts y contenedores Bash externos para iniciar las funciones de criptominería.

Los hallazgos ilustran cómo se puede armar la campaña de hacking para maximizar los rendimientos al aumentar la cantidad de cuentas que se pueden crear por minuto en estas plataformas.

> *«Es importante tener en cuenta que Automated Libra diseña su infraestructura para aprovechar al máximo las herramientas de CD/CI»*, agregaron los investigadores.

> *«Esto es cada vez más fácil de lograr con el tiempo, ya que los VSP tradicionales están diversificando sus carteras de servicios para incluir servicios relacionados con la nube. La disponibilidad de estos servicios relacionados con la nube hace que sea más fácil para los actores de amenazas, porque no tienen que mantener la infraestructura para desplegar sus aplicaciones».*