Se ha detectado una reciente operación denominada LABRAT, motivada por intereses financieros, que ha aprovechado una vulnerabilidad crítica en GitLab, ya corregida, como parte de una campaña de cryptojacking y proxyjacking.

> *«El atacante ha empleado herramientas basadas en firmas no detectadas, malware sigiloso y avanzado multiplataforma, herramientas de control y comando (C2) que evaden los firewalls, y rootkits basados en el kernel para ocultar su presencia»,* reportó Sysdig en un informe.

> *«Además, el atacante ha utilizado un servicio legítimo, TryCloudflare, para enmascarar su red C2.»*

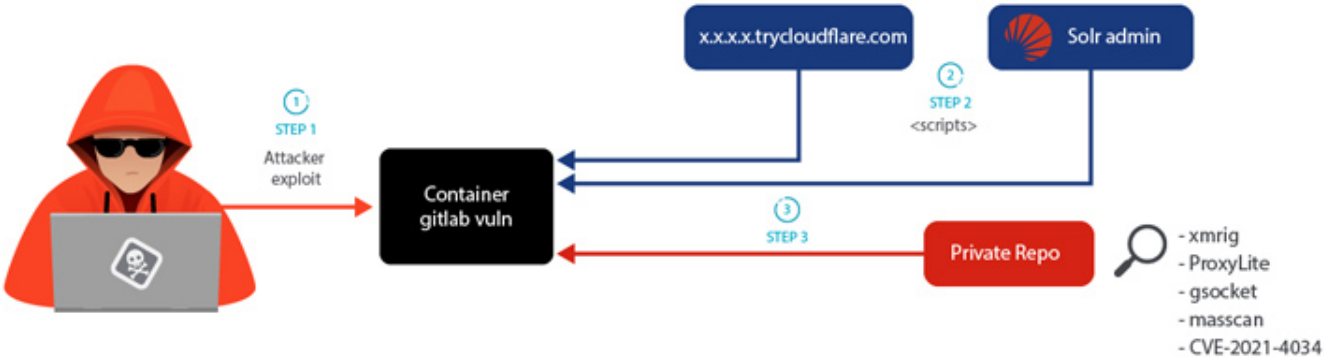
El proxyjacking permite al atacante alquilar el host comprometido en una red de proxy, posibilitando la monetización del ancho de banda no utilizado. Por otro lado, el cryptojacking se refiere a la explotación de recursos del sistema para minar criptomonedas.

Un aspecto significativo de esta campaña es la utilización de binarios compilados en Go y .NET para pasar inadvertidos, y LABRAT también facilita el acceso a puertas traseras en los sistemas infectados. Esto podría allanar el camino para ataques subsecuentes, robo de datos y ransomware.

Los ataques comienzan con la explotación de CVE-2021-22205 (puntuación CVSS: 10.0), una vulnerabilidad de ejecución remota de código que ha sido utilizada en la naturaleza por actores de origen indonesio en el pasado para desplegar mineros de criptomonedas.

Una intrusión exitosa es seguida por la obtención de un script dropper desde un servidor C2, el cual establece la persistencia, realiza movimientos laterales utilizando credenciales SSH encontradas en el sistema, y descarga binarios adicionales desde un repositorio privado de GitLab.

> *«Durante la operación LABRAT, TryCloudflare fue empleado para redirigir las conexiones a un servidor web protegido por contraseña que alojaba un script de shell malicioso. El uso de la infraestructura legítima de TryCloudFlare puede dificultar que los defensores identifiquen subdominios como maliciosos, especialmente si también se utiliza en operaciones normales»*, mencionó Miguel Hernández.



TryCloudflare es una herramienta gratuita que permite crear un túnel en Cloudflare sin agregar un sitio al DNS de Cloudflare. Genera un proceso que crea un subdominio aleatorio en trycloudflare.com, permitiendo la exposición de recursos internos en internet público.

Este desarrollo agrega al uso indebido de cloudflared para establecer canales de comunicación encubiertos desde hosts comprometidos y acceder a las redes de víctimas.

En una segunda variante del ataque, se informa que el adversario utilizó un servidor Solr en lugar de TryCloudflare para descargar un exploit para PwnKit (CVE-2021-4034) desde el mismo repositorio de GitLab para elevar privilegios, junto con otro archivo que ya no está disponible.

Algunas de las cargas útiles obtenidas por el script dropper incluyen una utilidad de código

abierto conocida como Global Socket (gsocket) para acceso remoto, y binarios para llevar a cabo cryptojacking y proxyjacking mediante servicios conocidos como IPRoyal y ProxyLite. El proceso de minería se oculta mediante un rootkit basado en el kernel llamado hiding-cryptominers-linux-rootkit.

Además, se proporciona un ejecutable basado en Go diseñado para asegurar persistencia y eliminar procesos mineros competidores u otras versiones anteriores para aprovechar al máximo los recursos de la máquina y maximizar ganancias.

> *«Dado que el objetivo de la operación LABRAT es financiero, el tiempo es dinero. Cuanto más tiempo pase desapercibida la intrusión, más dinero ganará el atacante y más costoso será para la víctima»,* Comentó Hernández