Investigadores de ciberseguridad han identificado una campaña «masiva» que se dirige a configuraciones de Git expuestas para robar credenciales, clonar repositorios privados e incluso extraer credenciales de servicios en la nube a partir del código fuente.

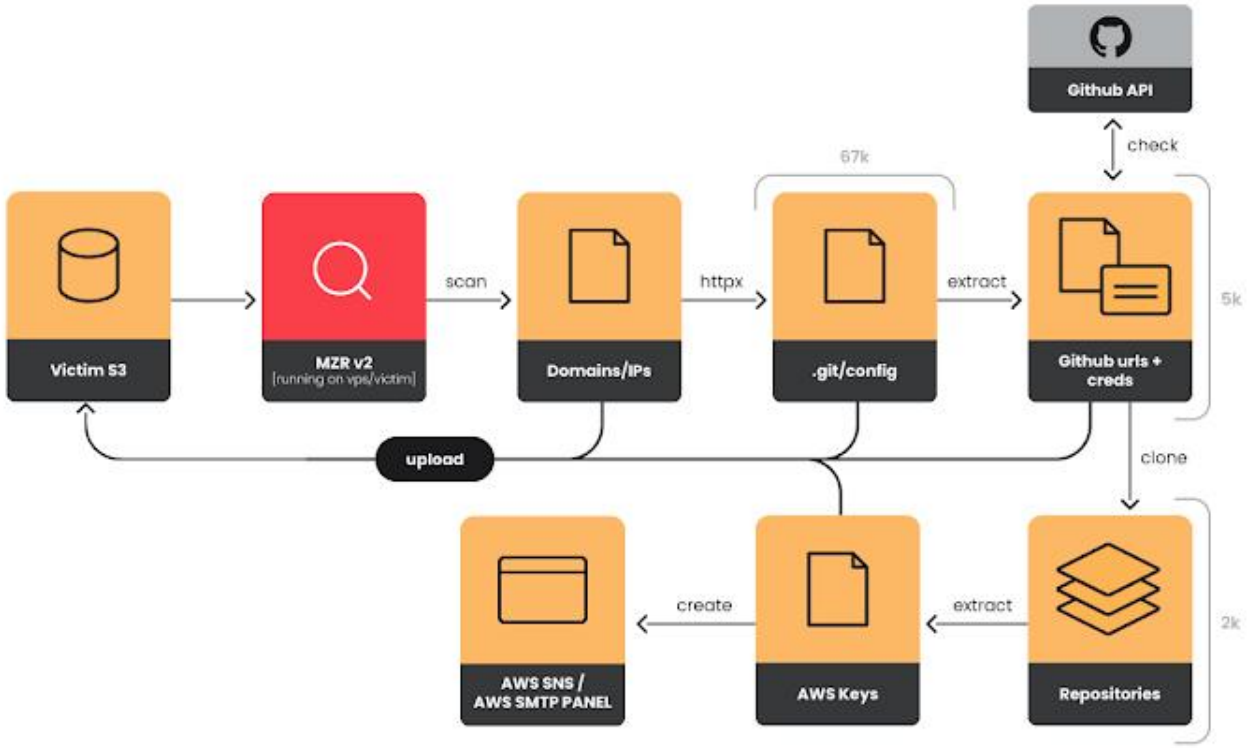
La operación, llamada EMERALDWHALE, se estima que ha recolectado más de 10,000 repositorios privados, almacenados en un bucket de Amazon S3 que pertenecía a una víctima anterior. Este bucket, que contenía al menos 15,000 credenciales robadas, ha sido desactivado por Amazon.

> *«Las credenciales robadas incluyen las de proveedores de servicios en la nube (CSP), proveedores de correo electrónico y otros servicios. El objetivo principal de este robo de credenciales parece ser el phishing y el envío de spam»*, señaló Sysdig en un informe.

Esta operación criminal, aunque no sofisticada, usa una variedad de herramientas privadas para robar credenciales, además de extraer archivos de configuración de Git, archivos .env de Laravel y datos web en bruto. Hasta el momento, no se ha atribuido esta actividad a ningún actor o grupo de amenazas específico.

Dirigiéndose a servidores con archivos de configuración de repositorios Git expuestos a través de amplios rangos de direcciones IP, el conjunto de herramientas de EMERALDWHALE permite identificar hosts relevantes y extraer y validar credenciales.

Los tokens obtenidos se utilizan para clonar repositorios públicos y privados, así como para extraer más credenciales incrustadas en el código fuente. La información recolectada finalmente se almacena en el bucket de S3.



Dos programas clave que el grupo de amenazas utiliza para alcanzar sus objetivos son MZR V2 y Seyzo-v2, los cuales se venden en mercados clandestinos y son capaces de aceptar listas de direcciones IP para escanear y explotar repositorios Git expuestos.

Estas listas generalmente se crean usando motores de búsqueda legítimos como Google Dorks y Shodan, además de herramientas de escaneo como MASSCAN.

El análisis de Sysdig también reveló que una lista de más de 67,000 URLs con la ruta «/.git/config» expuesta se está vendiendo en Telegram por $100, lo que sugiere un mercado activo para los archivos de configuración de Git.

> *«Además de los archivos de configuración de Git, EMERALDWHALE también ha atacado archivos de entorno de Laravel expuestos. Los archivos .env contienen una*

> *gran cantidad de credenciales, incluidas las de servicios en la nube y bases de datos»,* comentó Miguel Hernández, investigador de Sysdig.
>
> *«El mercado clandestino de credenciales está en auge, especialmente para los servicios en la nube. Este ataque demuestra que solo gestionar secretos no es suficiente para proteger un entorno».*