Se detectó una nueva campaña maliciosa que se aprovecha de los registros de eventos de Windows para ocultar fragmentos de shellcode por primera vez en la naturaleza.

> *«Permite que el troyano de última etapa 'sin archivos' se oculte a simple vista en el sistema de archivos»,* dijo el investigador de Kaspersky, Denis Legezo.

El proceso de infección sigilosa, que no se atribuye a un atacante conocido, comenzó en septiembre de 2021 cuando se atrajo a los objetivos previstos para que descargaran archivos .RAR comprimidos que contenían Cobalt Strike y Silent Break.

Los módulos de software de simulación del adversario se utilizan después como una plataforma de lanzamiento para inyectar código en los procesos del sistema Windows o en las aplicaciones confiables.

También es notable el uso de envoltorios antidetección como parte del conjunto de herramientas, lo que sugiere un intento por parte de los operadores de volar por debajo del radar.

Uno de los métodos clave es mantener el shellcode encriptado que contiene el malware de próxima etapa como piezas de 8 KB en los registros de eventos, una técnica nunca antes vista en los ataques del mundo real, que luego se combina y ejecuta.

La carga útil final es un conjunto de troyanos que emplean dos mecanismos de comunicación diferentes: HTTP con cifrado RC4 y sin cifrar con canalizaciones con nombre, que le permiten

ejecutar comandos arbitrarios, descargar archivos desde una URL, escalar privilegios y tomar capturas de pantalla.

Otro indicador de las tácticas de evasión del actor de amenazas es el uso de la información recopilada del reconocimiento inicial para desarrollar etapas sucesivas de la cadena de ataque, incluido el uso de un servidor remoto que imita el software legítimo utilizado por la víctima.

> *«El actor detrás de esta campaña es bastante capaz. El código es bastante único, sin similitudes con el malware conocido»,* dijo Legezo.

La divulgación se produce cuando los investigadores de Sysdig demostraron una forma de comprometer los contenedores de solo lectura con malware sin archivos que se ejecuta en la memoria aprovechando una falla crítica en los servidores Redis.