Un nuevo rootkit encubierto del kernel de Linux llamado Syslogk ha sido descubierto en desarrollo y encubre una carga útil maliciosa que puede ser comandada remotamente por un adversario utilizando un paquete de tráfico de red mágico.

> *«El rootkit Syslogk se basa en gran medida en Adore-Ng, pero incorpora nuevas funcionalidades que hacen que la aplicación en modo usuario y el rootkit del kernel sean difíciles de detectar»*, dijeron los investigadores de Avast, David Álvarez y Jan Neduchal.

Adore-Ng, un rootkit de código abierto disponible desde 2004, equipa al atacante con control total sobre un sistema comprometido. También facilita los procesos de ocultación, así como artefactos maliciosos personalizados, archivos e incluso el módulo del kernel, lo que dificulta su detección.

> *«El módulo comienza conectándose a varios sistemas de archivos. Desentierra el inodo para el sistema de archivos raíz y reemplaza el puntero de la función readdir() de ese inodo con uno propio. La versión de Adore funciona como la que reemplaza, excepto que oculta los archivos que pertenecen a un usuario e ID de grupo específicos»*, dijo LWN.net.

Además de sus capacidades para ocultar el tráfico de red de utilidades como netstat, dentor del rootkit hay una carga llamada *«PgSD93ql»*, que no es más que un troyano de puerta trasera compilado basado en C llamado Rekoobe y se activa al recibir un paquete mágico.

> *«Rekoobe es una pieza de código implantada en servidores legítimos. En este caso, está incrustado en un servidor SMTP falso, que genera un shell cuando recibe un comando especialmente diseñado»,* dijeron los investigadores.

Específicamente, Syslogk está diseñado para inspeccionar paquetes TCP que contienen el número de puerto de origen 59318 para iniciar el malware Rekoobe. Detener la carga útil, por otro lado, requiere que el paquete TCP cumpla con los siguientes criterios:

- El campo reservado del encabezado TCP se establece en 0x08
- El puerto de origen está entre 63400 y 63411 (incluido)
- Tanto el puerto de destino como la dirección de origen son los mismos que se usaron al enviar el paquete mágico para iniciar Rekoobe
- Contener una clave («D9sd87JMaij») que está codificada en el rootkit y ubicada en un desplazamiento variable del paquete mágico.

Por su parte, Rekoobe se hace pasar por un servidor SMTP aparentemente inocuo, pero en realidad se basa en un proyecto de código abierto llamado Tiny Shell e incorpora sigilosamente un comando de puerta trasera para generar un shell que permite la ejecución de comandos arbitrarios.

Syslogk se suma a una lista creciente de malware evasivo de Linux recientemente descubierto, como BPFDoor y Symbiote, que destaca cómo los ciberdelincuentes se dirigen cada vez más a los servidores Linux y la infraestructura de la nube para lanzar campañas de ransomware, ataques de cryptojacking y otras actividades ilícitas.

> *«Los rootkits son piezas peligrosas de malware. Los rootkits de kernel pueden ser difíciles de detectar y eliminar porque estas piezas de malware se ejecutan en una capa privilegiada»*, dijeron los investigadores.