Un malware de Linux nunca antes visto fue denominado *«navaja suiza»* por su arquitectura modular y su capacidad para instalar rootkits.

Esta amenaza de Linux no detectada antes, llamada Lightning Framework por Intezer, está equipada con una gran cantidad de características, lo que la convierte en uno de los marcos más complejos desarrollados para atacar los sistemas Linux.

> *«El framework tiene capacidades pasivas y activas para la comunicación con el actor de amenazas, incluida la apertura de SSH en una máquina infectada y una configuración de comando y control maleable polimórfica»,* dijo el investigador de Intezer, Ryan Robinson.

El elemento central del malware es un descargador («kbioset») y un módulo central («kkdmflush»), el primero de los cuales está diseñado para recuperar al menos siete complementos distintos de un servidor remoto que posteriormente son invocados por el componente central.

Además, el descargador también es responsable de establecer la persistencia del módulo principal del marco. *«La función principal del módulo de descarga es buscar los otros componentes y ejecutar el módulo central»*, dijo Robinson.

El módulo central, por su parte, establece contacto con el servidor de comando y control (C2) para obtener los comandos necesarios para ejecutar los complementos, al mismo tiempo que se encarga de ocultar su propia presencia en la máquina comprometida.

Algunos de los comandos notables recibidos del servidor permiten que el malware tome huellas dactilares de la máquina, ejecute comandos de shell, cargue archivos en el servidor C2, escriba datos arbitrarios en el archivo e incluso se actualice y se elimine del host infectado.

Además, configura la persistencia mediante la creación de un script de inicialización que se

ejecuta al arrancar el sistema, lo que permite que el descargador se inicie de forma automática.

> *«El Lightning Framework es un malware interesante, ya que no es común ver un marco tan grande desarrollado para apuntar a Linux»,* dijo Robinson.

El descubrimiento de Lightning Framework los convierte en la quinta cepa de malware de Linux descubierta en un corto período de tres meses después de BFPDoor, Symbiote, Syslogk y OrBit.