Investigadores de seguridad cibernética revelaron una nueva amenaza de Linux completamente no detectada denominada OrBit, que señala una tendencia creciente de ataques de malware dirigidos al popular sistema operativo.

El malware recibe su nombre debido a uno de los nombres de archivo que se utiliza para almacenar de forma temporal la salida de los comandos ejecutados («/tmp/.orbit»), según la compañía de seguridad cibernética Intezer.

> *«Se puede instalar con capacidades de persistencia o como un implante volátil. El malware implementa técnicas de evasión avanzadas y gana persistencia en la máquina al conectar funciones clave, brinda a los actores de amenazas capacidades de acceso remoto por medio de SSH, recopila credenciales y registra comandos TTY»,* dijo la investigadores de seguridad, Nicole Fishbein.

OrBit es el cuarto malware de Linux que salio a la luz en un breve lapso de tres meses después de BPFDoor, Symbiote y Syslogk.

El malware también funciona de forma similar a Symbiote en el sentido de que está diseñado para infectar todos los procesos en ejecución de las máquinas comprometidas. Pero a diferencia de este último, que aprovecha la variable de entorno LD_PRELOAD para cargar el objeto compartido, OrBit emplea dos métodos distintos.

> *«La primera forma es agregando el objeto compartido al archivo de configuración que usa el cargador. La segunda forma es parcheando el binario del propio cargador para que cargue el objeto compartido malicioso»,* dijo Fishbein.

La cadena de ataque comienza con un archivo cuentagotas ELF que es responsable de extraer la carga («libdl.so») y agregarla a las bibliotecas compartidas que está cargando el enlazador dinámico.

La biblioteca compartida no autorizada está diseñada para enlazar funciones de tres bibliotecas: libc, libcap y Módulo de Autenticación Conectable (PAM), lo que hace que los procesos existentes y nuevos utilicen las funciones modificadas, lo que esencialmente le permite recopilar credenciales, ocultar la actividad de la red y configurar acceso remoto al host por medio de SSH, mientras permanece oculto.

Además, OrBit se basa en una gran cantidad de métodos que le permiten funcionar sin alertar de su presencia y establecer la persistencia de una forma que dificulta su eliminación de las máquinas infectadas.

Una vez activado, el objetivo final de la puerta trasera es robar información conectando las funciones de lectura y escritura para capturar los datos que escriben los procesos ejecutados en la máquina, incluidos los comandos bash y sh, cuyos resultados se almacenan en archivos específicos.

> *«Lo que hace que este malware sea especialmente interesante es el enlace casi hermético de las bibliotecas en la máquina de la víctima, lo que permite que el malware gane persistencia y evada la detección mientras roba información y configura la backdoor SSH»,* dijo Fishbein.

> *«Las amenazas que apuntan a Linux siguen evolucionando mientras se mantienen exitosamente bajo el rada de las herramientas de seguridad, ahora OrBit es un ejemplo más de cuán evasivo y persistente puede ser el nuevo malware».*