Investigadores de seguridad cibernética descubrieron un tipo completamente nuevo de malware para Linux, nombrado CDRThief, que se dirige a los softswitches de voz sobre IP (VoIP) en un intento de robar metadatos de llamadas telefónicas.

> *«El objetivo principal del malware es extraer varios datos privados de un conmutador de software comprometido, incluidos los registros de detalles de llamadas (CDR)»*, dijeron los investigadores de ESET.
>
> *«Para robar estos metadatos, el malware consulta las bases de datos MySQL internas que utiliza el softswitch. Por lo tanto, los atacantes demuestran un buen conocimiento de la arquitectura interna de la plataforma objetivo»*, agregaron.

Los softswitches son por lo general, servidores VoIP que permiten que las redes de telecomunicaciones proporcionen administración de tráfico de voz, fax, datos y video, y enrutamiento de llamadas.

La investigación de ESET descibrió que CDRThief tenía como objetivo una plataforma VoIP de Linux específica, a saber, los softswitches VOS2009 y 3000 de la empresa china Linknat, y tenía su funcionalidad maliciosa encriptada para evadir el análisis estático.

El malware comienza intentando localizar los archivos de configuración de softswitch de una lista de directorios predeterminados con el objetivo de acceder a las credenciales de la base de datos MySQL, que luego se descifran para consultar la base de datos.

Los investigadores de ESET dicen que los atacantes habrían tenido que aplicar ingeniería inversa a los binarios de la plataforma para analizar el proceso de cifrado y recuperar la clave AES utilizada para descifrar la contraseña de la base de datos, lo que sugiere el *«profundo conocimiento»* de los autores de la arquitectura VoIP.

Además de recopilar información básica sobre el sistema Linknat comprometido, CDRThief

extrae detalles de la base de datos (nombre de usuario, contraseña cifrada, dirección IP) y ejecuta consultas SQL directamente a la base de datos MySQL para capturar información relacionada con eventos del sistema, puertas de enlace VoIP y metadatos de llamadas.

> *«Los datos que se extraerán de las tablas e_syslog, e_gatewaymapping y e_cdr se comprimen y luego se cifran con una clave pública RSA-1024 codificada antes de la exfiltración. Por lo tanto, solo los autores u operadores de malware pueden descifrar los datos extraídos»,* dijo ESET.

Actualmente, el malware se está enfocando solo en recopilar información de la base de datos, pero ESET advierte que eso podría cambiar en cualquier momento si los atacantes deciden introducir funciones de robo de documentos más avanzadas en una versión actualizada.

> *«En el momento de redactar este informe, no sabemos cómo se implementa el malware en los dispositivos comprometidos. Especulamos que los atacantes podrían obtener acceso al dispositivo mediante un ataque de fuerza bruta o aprovechando una vulnerabilidad»,* dijo Anton Cherepanov de ESET.
>
> *«Parece razonable suponer que el malware se utiliza para el ciberespionaje. Otro objetivo posible para los atacantes que utilizan este malware es el fraude de VoIP. Dado que los atacantes obtienen información sobre la actividad de los softswitches de VoIP y sus puertas de enlace, esta información podría utilizarse para realizar el Fraude de Reparto de Ingresos Internacionales»*, agregó.