Investigadores de seguridad cibernética revelaron este jueves un nuevo tipo de backdoor modular que tiene como objetivo el software de gestión de restaurantes de punto de venta (PoS) de Oracle, en un intento de robar información de pago confidencial almacenada en los dispositivos.

La puerta trasera, denominada ModPipe, afecta a los sistemas POS 3700 de Oracle MICROS Restaurant Enterprise Series (RES), un paquete de software ampliamente utilizado en restaurantes y establecimientos hoteleros para manejar de forma eficiente POS, inventario y administración de mano de obra. La mayoría de los objetivos identificados se encuentran principalmente en Estados Unidos.

> *«Lo que distingue a la puerta trasera son sus módulos descargables y sus capacidades, ya que contiene un algoritmo personalizado diseñado para recopilar las contraseñas de la base de datos de POS RES 3700 descifrándolas de los valores del registro de Windows»,* dijeron los investigadores de ESET.
>
> *«Las credenciales extraídas permiten a los operadores de ModPipe acceder al contenido de la base de datos, incluidas varias definiciones y configuraciones, tablas de estado e información sobre transacciones POS»,* agregaron.

Cabe mencionar que los detalles como números de tarjetas de crédito y fechas de vencimiento, están protegidos detrás de las barreras de cifrado en RED 3700, lo que limita la cantidad de información valiosa viable para un uso indebido, aunque los investigadores aseguran que el actor detrás del ataque podría estar en posesión de un segundo módulo descargable para descifrar el contenido de la base de datos.

La infraestructura de ModPipe consta de un cuentagotas inicial que se utiliza para instalar un

cargador persistente, que luego desempaqueta y carga la carga útil de la siguiente etapa: el módulo de malware principal que se usa para establecer comunicaciones con otros módulos *«descargables»* y el servidor de comando y control (C2) a través de un módulo de red independiente.

El principal de los módulos descargables es *«GetMicInfo»*, un componente que puede interceptar y descifrar contraseñas de bases de datos mediante un algoritmo especial, que los investigadores de ESET teorizan que podría haberse implementado mediante ingeniería inversa de las bibliotecas criptográficas o haciendo uso de las especificaciones de implementación de cifrado obtenidas a raíz de una violación de datos en la división MICROS POS de Oracle en 2016.

Un segundo módulo llamado ModScan 2.20 está dedicado a recopilar información adicional sobre el sistema POS instalado, mientras que otro módulo con nombre Proclist recopila detalles acerca de los procesos que se están ejecutando actualmente.

> *«La arquitectura, los módulos y sus capacidades de ModPipe también indican que sus escritores tienen un amplio conocimiento del software RES 3700 POS específico. La competencia de los operadores podría provenir de múltiples escenarios, incluido el robo y la ingeniería inversa del producto de software propietario, el uso indebido de sus partes filtradas o la compra de código en un mercado clandestino»*, dijeron los investigadores.

Se recomienda a las empresas que utilizan el POS RES 3700 que actualicen a la última versión del software, así como el uso de dispositivos que ejecuten versiones actualizadas del sistema operativo adyacente.