Investigadores en ciberseguridad han identificado lo que consideran el noveno malware dirigido a Sistemas de Control Industrial (ICS) utilizado en un ataque cibernético que afectó a una empresa de energía en la ciudad ucraniana de Lviv en enero pasado.

La firma de ciberseguridad industrial Dragos ha nombrado al malware como FrostyGoop, describiéndolo como la primera cepa de malware en usar directamente comunicaciones Modbus TCP para sabotear redes de tecnología operativa (OT). Fue descubierto por la compañía en abril de 2024.

«FrostyGoop es un malware específico para ICS escrito en Golang que puede interactuar directamente con Sistemas de Control Industrial (ICS) utilizando Modbus TCP a través del puerto 502», explicaron los investigadores Kyle O'Meara, Magpie (Mark) Graham y Carolyn Ahlers en un informe técnico.

Se cree que el malware, diseñado principalmente para atacar sistemas Windows, ha sido utilizado para comprometer controladores ENCO con el puerto TCP 502 expuesto a Internet. No se ha asociado con ningún actor de amenaza o grupo de actividad previamente conocido.

FrostyGoop tiene la capacidad de leer y escribir en registros de dispositivos ICS que contienen datos de entrada, salida y configuración. También acepta argumentos opcionales de ejecución desde la línea de comandos, usa archivos de configuración en formato JSON para especificar direcciones IP objetivo y comandos Modbus, y registra la salida en una consola y/o archivo JSON.

Se informa que el incidente que afectó a la empresa de energía municipal resultó en la pérdida de servicios de calefacción para más de 600 edificios de apartamentos durante casi 48 horas.

«Los atacantes enviaron comandos Modbus a los controladores ENCO, provocando mediciones incorrectas y fallos en el sistema», dijeron los investigadores en una llamada de conferencia, señalando que el acceso inicial probablemente se logró explotando una vulnerabilidad en los enrutadores Mikrotik en abril de 2023.

> *«Los atacantes enviaron comandos Modbus a los controladores ENCO, causando mediciones inexactas y malfunciones del sistema. La remediación tomó casi dos días.»*

Aunque FrostyGoop emplea extensamente el protocolo Modbus para comunicaciones cliente/servidor, no es el único. En 2022, Dragos y Mandiant detallaron otro malware ICS llamado PIPEDREAM (también conocido como INCONTROLLER) que utilizaba varios protocolos de red industrial como OPC UA, Modbus y CODESYS para la interacción.

También es el noveno malware enfocado en ICS después de Stuxnet, Havex, Industroyer (también conocido como CrashOverride), Triton (también conocido como Trisis), BlackEnergy2, Industroyer2 y COSMICENERGY.

La capacidad del malware para leer o modificar datos en dispositivos ICS utilizando Modbus tiene graves consecuencias para las operaciones industriales y la seguridad pública, dijo Dragos, añadiendo que más de 46,000 dispositivos ICS expuestos a Internet se comunican a través de este protocolo ampliamente utilizado.

> *«El ataque específico a los ICS utilizando Modbus TCP a través del puerto 502 y la capacidad de interactuar directamente con varios dispositivos ICS representan una seria amenaza para la infraestructura crítica en múltiples sectores»,* dijeron los investigadores.

> *«Las organizaciones deben priorizar la implementación de marcos de ciberseguridad integrales para proteger la infraestructura crítica de amenazas similares en el futuro.»*