Los ingenieros y operadores industriales son el objetivo de una nueva campaña que aprovecha el software de descifrado de contraseñas para tomar el control de los controladores lógicos programables (PLC) y cooptar las máquinas a una red de bots.

El software *«explotó una vulnerabilidad en el firmware que le permitió recuperar la contraseña a pedido. Además, el software era un lanzador de malware, infectaba la máquina con el malware Sality y convertía al host en un par en la botnet peer-to-peer de Sality»,* dijo el investigador de seguridad de Dragos, Sam Hanson.

La compañía de seguridad cibernética industrial dijo que el exploit de recuperación de contraseña incrustado en el cuentagotas de malware está diseñado para recuperar la credencial asociada con Automation Direct DirectLOGIC 06 PLC.

El exploit, rastreado como CVE-2022-2003 (puntaje CVSS: 7.7), fue descrito como un caso de transmisión de datos confidenciales en texto sin cifrar, que podría conducir a la divulgación de información y cambios no autorizados. El problema se solucionó en la versión de firmware 2.72 lanzada el mes pasado.

Las infecciones culminan con la implementación del malware Sality para realizar tres tareas como la extracción de criptomonedas y el descifrado de contraseñas de forma distribuida, al mismo tiempo que se toman las medidas para permanecer sin ser detectados al terminar el software de seguridad que se ejecuta en las estaciones de trabajo comprometidas.

Además, el artefacto desenterrado por las funciones de Dragos arroja una carga útil de crypto-clipper, que roba criptomonedas durante una transacción al sustituir la dirección de la billetera original guardada en el portapapeles con la dirección de la billetera del atacante.

Automation Direct no es el único proveedor afectado, ya que las herramientas afirman abarcar varios PLC, interfaces hombre-máquina (HMI) y archivos de proyecto que abarcan

Omron, Siemens, ABB Codesys, Delta Automation, Fuji Electric, Mitsubishi Electric, Schneider Electric´s Pro-face, Vigor PLC, Weintek, Allen-Bradley de Rockwell Automation, Panasonic, Fatek, IDEC Corporation y LG.

> *«En general, parece que hay un ecosistema para este tipo de software. Existen varios sitios web y múltiples cuentas de redes sociales que promocionan sus 'crackers' de contraseñas»*, dijo Hanson, atribuyendo los ataques a un probable adversario motivado financieramente.

Esta no es la primera vez que el software troyanizado selecciona redes de tecnología operativa (OT). En octubre de 2021, Mandiant reveló cómo los binarios ejecutables portátiles legítimos se ven comprometidos por una variedad de malware como Sality, Virut y Ramnit, entre otros.