VEDERE LABS

Industroyer2 e INCONTROLLER

Nuevos hallazgos y cómo Forescout protege contra el malware específico de ICS más reciente

28 de julio de 2022

1. Resumen ejecutivo

En nuestro nuevo informe sobre amenazas, Vedere Labs de Forescout presenta el análisis técnico público más detallado de Industroyer2 e INCONTROLLER (también conocido como PIPEDREAM), los ejemplos más recientes de malware específico de ICS que fueron revelados al público casi simultáneamente el 12 y el 13 de abril.

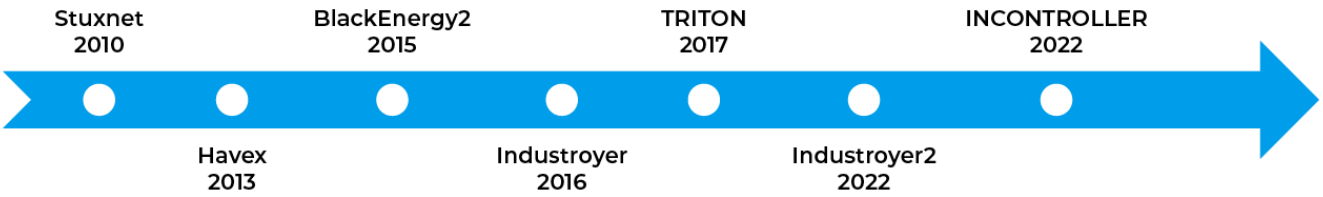
Aunque ya ha habido informes anteriores sobre las dos familias de malware analizadas en esta investigación, le presentamos aquí las siguientes nuevas contribuciones:

- Un análisis de una funcionalidad en Industroyer2 para descubrir la dirección común de ASDU del objetivo. A pesar de no ser utilizado dada la configuración preprogramada de nuestra muestra, podría haber sido una herramienta utilizada en etapas de reconocimiento anteriores para recopilar información sobre el objetivo.
- Un análisis de la similitud de la implementación de IEC-104 en Industroyer que revela que es muy probablemente una versión modificada de una implementación disponible públicamente.
- La descripción pública más detallada hasta ahora de Lazycargo, una parte de INCONTROLLER que se hizo pública recientemente y que se utiliza para ejecutar otras partes del malware.

Este informe también contiene una lista de indicadores de áreas comprometidas y de mitigaciones recomendadas.

2. La evolución del malware de ICS

El malware específico de ICS sigue siendo muy poco frecuente en comparación con el malware básico, como el ransomware o los troyanos bancarios. Industroyer2 e INCONTROLLER siguen ejemplos conocidos anteriores de malware dirigidos a sistemas de control industrial como Stuxnet, Havex, BlackEnergy2, Industroyer y TRITON como se indica en la línea de tiempo de la imagen a continuación.



Industroyer2 aprovecha los limpiadores específicos del sistema operativo y un módulo dedicado para comunicarse a través del protocolo industrial IEC-104. INCONTROLLER es un completo kit de herramientas que contiene módulos para enviar instrucciones o recuperar datos de dispositivos ICS mediante protocolos de red industriales, como OPC UA, Modbus, CODESYS, Machine Expert Discovery y Omron FINS. Asimismo, Industroyer2 tiene una configuración muy específica, mientras que INCONTROLLER es mucho más reutilizable entre diferentes objetivos

Tanto Industroyer2 como INCONTROLLER fueron detectados antes de que causaran interrupciones físicas. Se cree que Industroyer2 fue desarrollado y desplegado por la APT Sandworm , vinculada a la GRU rusa, que se considera responsable de los ataques originales a la red eléctrica ucraniana en 2015 y 2016. El incidente de Industroyer2 es resultado de la actividad reciente contra la APT en 2022, como la interrupción de la botnet de

Cyclops Blink. Todavía no hay indicios concluyentes sobre los actores detrás de INCONTROLLER, sus motivos o propósitos.

Ambos nuevos malwares muestran que el abuso de capacidades nativas, a menudo inseguras por diseño del equipo de tecnología operativa, continúa siendo el *modus operandi* preferido de los atacantes del mundo real. Vedere Labs recientemente expuso un conjunto de 56 vulnerabilidades inseguras por diseño en equipos de tecnología operativa llamadas OT:ICEFALL en las que se incluían los controladores Omron que fueron atacados por INCONTROLLER. La aparición de nuevas vulnerabilidades y nuevo malware que aprovecha la naturaleza insegura por diseño de los equipos de tecnología operativa justifica la necesidad de tener una sólida supervisión de red dirigida a esta tecnología, además de contar con capacidad de inspección profunda de paquetes.

3. Mitigaciones

Los clientes de Forescout eyeInspect pueden seguir las recomendaciones siguientes para asegurarse de que están protegidos contra Industroyer2 e INCONTROLLER.

1. Recomendaciones generales

- Seguir la publicación de contenido adicional, como scripts e IoC en el portal de tecnología operativa o a través de sus representantes de Forescout.
- Supervisar la exposición de la red para sistemas de control y HMI.
- Supervisar con precisión las conexiones a dispositivos que no cumplan las normas documentadas para estos y su entorno, prestando especial atención a las conexiones HTTP y Telnet a estos dispositivos.
- Supervisar los intentos de conexión Telnet no autorizados, incluyendo el uso de credenciales predeterminadas.
- Detectar el uso de ICMP y en especial los posibles barridos con ping a través de los indicadores IMCP de la Biblioteca de Amenazas Industriales destinados a detectar posibles exploraciones de puertos y descubrimientos.
- Se pueden aplicar configuraciones adicionales en eyeInspect para llevar a cabo la detección de intrusiones en nodos conocidos. Existen algunos métodos disponibles, como la creación de una lista negra de protocolos y una lista blanca de comunicaciones con reglas de tráfico.
- El script Threat Detection Add-Ons (complementos de detección de amenazas) contiene comprobaciones adicionales para el movimiento lateral y la manipulación de cuentas de usuario y esto puede revelar intentos de obtener derechos administrativos.
- Supervisar estrechamente los protocolos de los que abusa el nuevo malware para poder detectar indicios de anomalías: IEC-104 (2404/TCP), OPC UA (4840/TCP, 4843/TCP), Modbus (502/TCP), Machine Expert Discovery (27126/UDP, 27127/UDP), CODESYS (1740-1743/UDP, 11740-11743/TCP, 1105/TCP) y Omron FINS (9600/TCP, 9600/UDP). A continuación presentamos recomendaciones específicas para cada protocolo en eyeInspect.

Para más información y análisis técnicos lea el informe completo aquí.


VEDERE LABS