Un estudio reciente ha identificado más de 145,000 Sistemas de Control Industrial (ICS, por sus siglas en inglés) accesibles a través de Internet en 175 países, siendo Estados Unidos responsable de más de un tercio de estas conexiones expuestas.

El informe, realizado por la empresa Censys, especializada en gestión de superficies de ataque, reveló que el 38 % de estos dispositivos están ubicados en América del Norte, el 35.4 % en Europa, el 22.9 % en Asia, el 1.7 % en Oceanía, el 1.2 % en Sudamérica y el 0.5 % en África.

Entre los países con mayor cantidad de servicios ICS expuestos destacan Estados Unidos (con más de 48,000 dispositivos), Turquía, Corea del Sur, Italia, Canadá, España, China, Alemania, Francia, Reino Unido, Japón, Suecia, Taiwán, Polonia y Lituania.

Los datos se basan en la exposición de varios protocolos ICS ampliamente utilizados, como Modbus, IEC 60870-5-104, CODESYS, OPC UA, entre otros.

Un detalle importante señalado en el informe es que las vulnerabilidades varían según la región: en Europa son más frecuentes los protocolos Modbus, S7 e IEC 60870-5-104, mientras que en América del Norte predominan Fox, BACnet, ATG y C-more. Algunos servicios ICS, como EIP, FINS y WDBRPC, son comunes en ambas regiones.

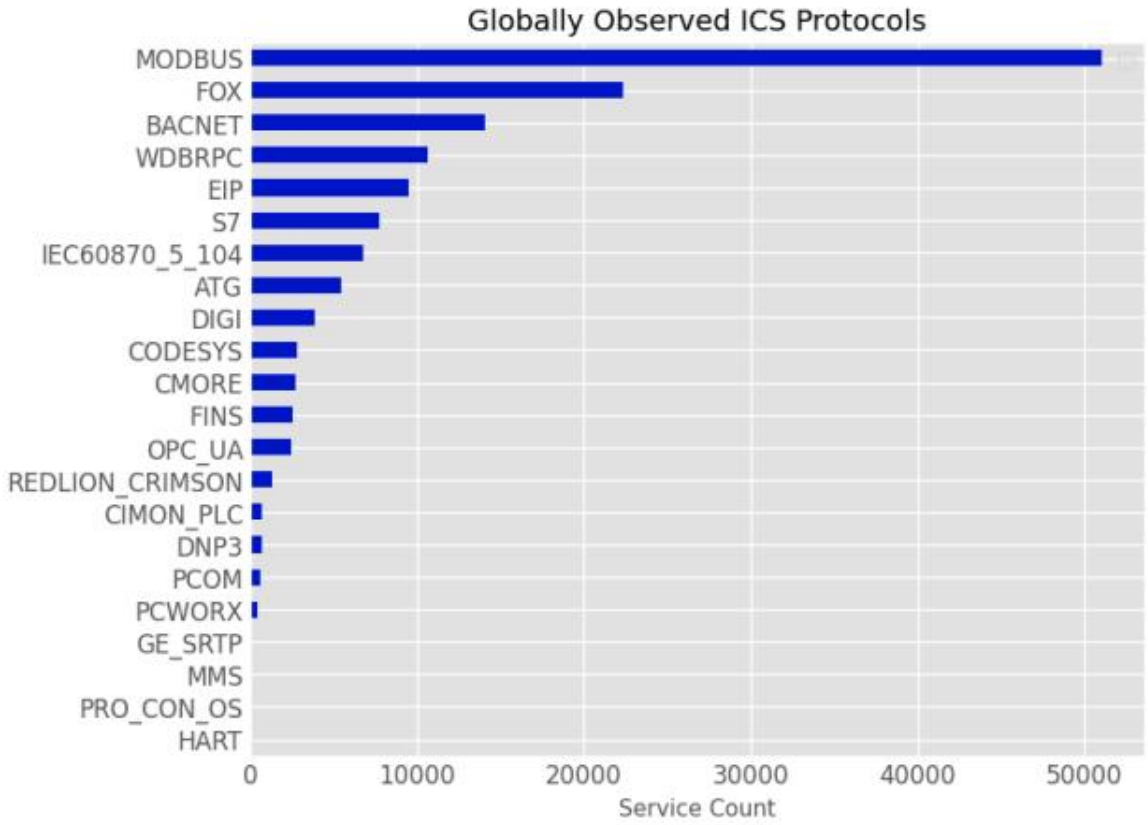
Por otro lado, el 34 % de las interfaces hombre-máquina (HMIs) C-more están vinculadas a sistemas de agua y aguas residuales, mientras que el 23 % se relacionan con actividades agrícolas.

> *«Muchos de estos protocolos fueron desarrollados en la década de 1970 y aún son esenciales para los procesos industriales, pero no han experimentado las mejoras de seguridad que otros sectores han adoptado»,* señaló Zakir Durumeric, cofundador y científico principal de Censys.
>
> *«La protección de los dispositivos ICS es crucial para garantizar la seguridad de la*

> *infraestructura crítica de un país. Es necesario entender cómo estos sistemas están expuestos y las vulnerabilidades que enfrentan»,* agregó.

Aunque los ataques cibernéticos dirigidos específicamente a sistemas ICS han sido escasos, con solo nueve tipos de malware identificados hasta ahora, ha habido un aumento reciente en estas amenazas, especialmente tras el conflicto entre Rusia y Ucrania.

En julio, Dragos informó que una empresa energética ucraniana fue blanco de un ataque con un malware llamado FrostyGoop, diseñado para utilizar el protocolo Modbus TCP con el fin de interrumpir las redes de tecnología operativa (OT).



Conocido también como BUSTLEBERM, este software malicioso, desarrollado en Golang como herramienta de línea de comandos para Windows, puede provocar fallos en dispositivos expuestos públicamente, causando interrupciones o ataques de denegación de servicio (DoS).

> *«Aunque este malware fue usado contra dispositivos de control ENCO, también puede dirigirse a cualquier equipo que opere con Modbus TCP»,* explicaron Asher Davila y Chris Navarrete, investigadores de Palo Alto Networks Unit 42, en un reciente informe.
>
> *«Los parámetros necesarios para que FrostyGoop establezca una conexión Modbus TCP y envíe comandos pueden configurarse mediante argumentos de línea de comandos o a través de un archivo JSON independiente»*, detallaron.

De acuerdo con datos de telemetría de la empresa, 1,088,175 dispositivos Modbus TCP estuvieron accesibles en Internet durante un período de un mes entre el 2 de septiembre y el 2 de octubre de 2024.

Los actores maliciosos también han dirigido su atención hacia otras infraestructuras críticas, como las entidades encargadas del suministro de agua. En un incidente ocurrido en EE. UU. el año pasado, la Autoridad Municipal de Agua de Aliquippa, en Pensilvania, sufrió una violación de seguridad al aprovecharse de los controladores lógicos programables (PLC) de Unitronics expuestos a internet, para alterar los sistemas con un mensaje en contra de Israel.

Censys descubrió que los interfaces hombre-máquina (HMI), utilizados para supervisar e interactuar con los sistemas de control industrial (ICS), también están siendo cada vez más accesibles a través de la red para permitir el acceso remoto. La mayoría de los HMIs expuestos se encuentran en EE. UU., seguidos de países como Alemania, Canadá, Francia, Austria, Italia, Reino Unido, Australia, España y Polonia.

Lo curioso es que la mayoría de los HMIs e ICS encontrados están en proveedores de servicios de Internet móviles o de nivel empresarial, como Verizon, Deutsche Telekom, Magenta Telekom y Turkcell, entre otros, ofreciendo poca información sobre quién realmente está usando el sistema.

> *«Los HMIs frecuentemente incluyen logotipos de la empresa o nombres de plantas, lo que puede ayudar a identificar al propietario y al sector. Por el contrario, los protocolos ICS rara vez proporcionan esta información, lo que dificulta enormemente la identificación y notificación a los propietarios sobre las exposiciones. Será necesaria la colaboración de las principales compañías de telecomunicaciones que alojan estos servicios para abordar este problema»,* comentó Censys.

El hecho de que las redes ICS y OT presenten una gran superficie de ataque para los actores maliciosos hace imprescindible que las organizaciones tomen medidas para identificar y proteger los dispositivos OT e ICS expuestos, actualizar las credenciales predeterminadas y vigilar las redes en busca de actividades sospechosas.

El riesgo para estos entornos se ve incrementado por un aumento en los malware de botnets — Aisuru, Kaiten, Gafgyt, Kaden y LOLFME — que explotan las credenciales predeterminadas de OT no solo para llevar a cabo ataques de denegación de servicio distribuido (DDoS), sino también para eliminar los datos almacenados en ellos.

Este aviso se presenta pocas semanas después de que Forescout revelara que las estaciones de trabajo de Digital Imaging and Communications in Medicine (DICOM) y los Sistemas de Archivo y Comunicación de Imágenes (PACS), los controladores de bombas y los sistemas de información médica están entre los dispositivos más vulnerables en las organizaciones de atención sanitaria (HDO).

DICOM es uno de los servicios más utilizados por los dispositivos del Internet de las Cosas Médicas (IoMT) y uno de los más expuestos a internet, señaló la firma de ciberseguridad, con

una notable cantidad de instancias ubicadas en EE. UU., India, Alemania, Brasil, Irán y China.

> *«Las organizaciones de salud seguirán enfrentando dificultades con dispositivos médicos que operan con sistemas antiguos o no estándar»*, afirmó Daniel dos Santos, jefe de investigación de seguridad de Forescout.
>
> *«Un solo punto débil puede abrir la puerta a información sensible de pacientes. Por eso, la identificación y clasificación de activos, el mapeo del flujo de comunicaciones en las redes, la segmentación de redes y el monitoreo constante son clave para proteger las redes de atención médica en expansión.»*