censys

EXECUTIVE SUMMARY

The 2024 State of the Internet Report

Key Findings on Industrial Control System Exposures

Industrial control systems (ICS) exposed to the Internet have long been a concern among security researchers, as these systems are foundational to industrial processes. Though cyber attacks on ICS can be catastrophic in nature, systems themselves are more rarely compromised, given the specialized knowledge typically required to launch attacks against them.

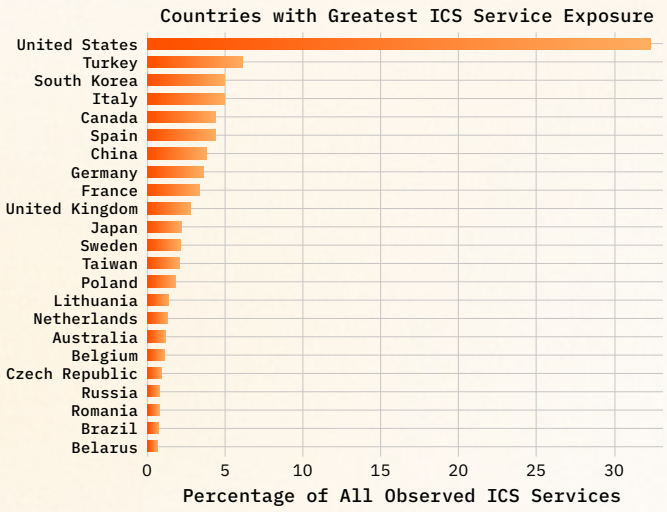
However, threat actors have recently shifted to simpler tactics: targeting human machine interfaces (HMIs). HMIs are graphical interfaces that ICS operators can use to interact with systems and machinery. As we observed, many are connected to the public Internet to support remote operator access. However, their relative ease of use and frequent lack of authentication also present opportunities for threat actors.

In the third annual *State of the Internet Report*, the Censys Research Team uses our global scanning perspective to learn more about the state of ICS exposures, including the prevalence of exposed protocols and HMIs, and the implications these exposures may have on critical infrastructure security.

What You Should Know

1 The U.S. Alone Is Responsible for Over One-Third of Global ICS Service Exposures

Censys researchers observed over 145,000 exposed ICS services across 175 countries. Of these services, 38% were in North America, 35% were in Europe, and 22% were in Asia. It's clear that U.S. operators in particular have ample opportunity to reduce ICS exposure. However, when exposures are observed as a ratio of all IP addresses associated with a country, the countries with the highest proportion of ICS exposures are actually focused in Lithuania, Belarus, and Turkey.

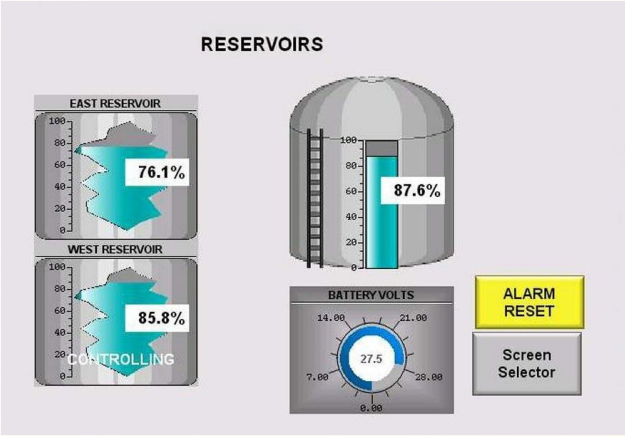


2 ICS Attack Surfaces Are Regionally Unique

ICS protocol exposures vary depending where you're looking. Modbus is the most commonly observed ICS protocol globally, and boasts a wide variety of applications across sectors like facility management, telecommunications, and manufacturing. Of all protocols observed, Modbus, S7, and IEC 60870-5-104 are more widely observed in Europe, but Fox, BACnet, ATG, and C-More are more commonly found in North America. If attempting to identify potential exposure across your own systems, checking these protocols may serve as a good starting point.

3 HMI Exposures Affect Water, Wastewater, and Agricultural Processes

We know that HMIs are attractive and increasingly popular targets for threat actors. For this reason, Censys examined the exposure of over 20 types of HMI software, and identified nearly 7,700 hosts across 80 countries running HMIs. When analyzing C-More HMIs, which are HMIs that run a proprietary protocol enabled by default with weak or no authentication, Censys observed that **34% were water and wastewater related**, while 23% are associated with agricultural processes. While these numbers reflect global data, it should be noted that similar to ICS service exposures, C-More exposures are most prominent in North America.



A C-More HMI monitoring reservoir and tank levels.

4 Many Hosts Running HMIs Are Also Running Prohibited Products

Censys researchers discovered nearly 200 hosts running HMIs that were *also* running products from vendors explicitly prohibited by the U.S. National Defense Authorization Act (NDAA) Section 889. While not all of these hosts are critical infrastructure, government-operated, or even located in the U.S., this serves as a reminder that operators should be mindful of what products and software they allow to run alongside industrial processes.

5 Most Observed ICS Services and HMIs Run on Mobile or Business-Grade ISPs

Given the often remote nature of industrial facilities, not all operators have the ability to leverage a wired Internet connection to run systems. 5G or LTE routers, typically provided by mobile service providers, are a common solution to this connectivity issue. However, lack of useful metadata (e.g., DNS) for hosts on these networks can make it nearly impossible to determine a system's owner or intended purpose. This further complicates the ability for researchers like those at Censys to learn more about exposures and notify owners.

How to Take Action

Given the extent of exposures observed, there's opportunity for organizations around the world to remediate current exposures and mitigate future risk. In the U.S., CISA provides guidance for securing and defending ICS environments. In addition to that guidance, Censys offers the following suggestions for defenders and operators based on our observations:

- **Know Your Attack Surface**
  Perform a comprehensive asset inventory and understand your public Internet attack surface. It's impossible to defend systems you don't know about, and it's useful to understand what your external perimeter looks like from a threat actor's perspective. Attack Surface Management solutions can help provide this visibility.
- **Avoid Public Internet Connection**
  If possible, avoid connecting any ICS service or HMI directly to the public Internet. Protecting these assets with a VPN or a firewall is ideal, but for services that offer it, authentication should be enabled at minimum.
- **Always Ensure Strong Credentials**
  Avoid using weak or default credentials, as these are trivial for threat actors to guess or crack.

Interested in Learning More?

Download the full *2024 State of the Internet Report* for a complete analysis of our findings!

Download the Report →

Censys is the leading Internet Intelligence Platform™ for Threat Hunting and Attack Surface Management, known for discovering assets six times faster than its closest competitor. Censys offers the most comprehensive, accurate, and up-to-date map of the internet available with daily refreshes of billions of services and the world's largest certificate database empowering our customers to proactively discover, prioritize and remediate threats. Established by the creators of ZMap and trusted by the U.S. Government, along with over 50% of the Fortune 500, Censys' mission is to be the one place to understand everything on the internet.

hello@censys.com www.censys.com