How to Find IoT Devices Connected to Your Campus Network

Why is this important?

IoT devices on our campus networks may be vulnerable to malware and increase the risk for information security and privacy compromises. Yet, many of these devices show up on campus without the knowledge of central IT. So how can we find those devices that put us at risk? The Internet2 IoT Systems Risk Management Task Force found two tools, Censys and Shodan, to be easy enough for non-security experts to use to find IoT devices.

Internet2 IoT Systems Risk Management Task Force: April 2017

Types of Devices/ Vulnerabilities

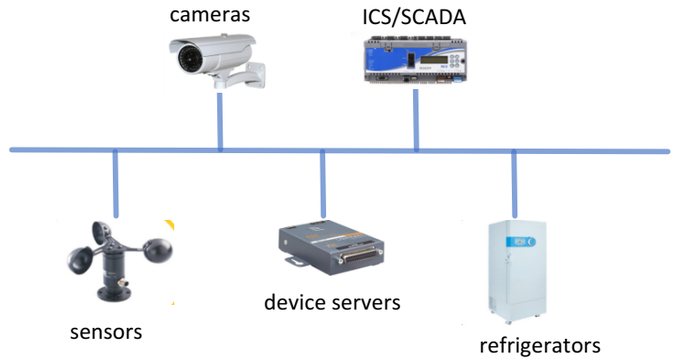


Image Sources: IndustryBuying; BACnet Interest Group Europe; Alibaba; Lantronix; MegaLab.

Bashlite and Mirai malware have created botnets that carried out DDoS attacks on DYN, OVH, and an unnamed US university. Other potential vulnerabilities include:

- Devices with weak or hardcoded passwords: IP cameras, light sensors, refrigerators
- Devices that connect through known high risk ports such as Telnet/port 23 using TCP/IP (no encryption): printers, cameras, device servers
- Devices that connect to components of building automation systems: SCADA and ICS components

Tools: Shodan and Censys

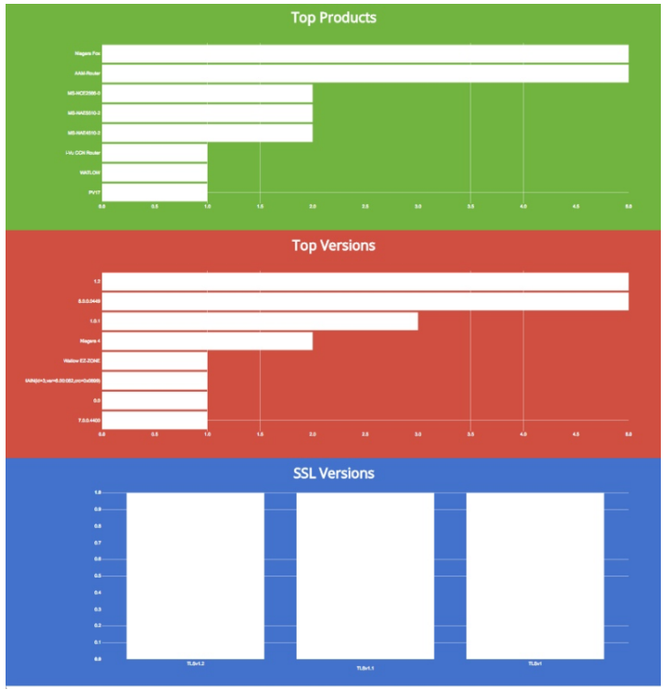
Shodan and Censys are search engines that find servers and other devices connected to the Internet that use Internet protocols specifically associated with industrial control systems and, increasingly, IoT devices & systems. They retrieve metadata about the devices such as geographic location, operating system, device name and serial number.

Join Us

Interested in joining the Internet2 Collaborative Innovation Community and IoT Working Group? Contact the Internet2 Chief Innovation Office at CINO@Internet2.edu

Reports

Both tools let you download reports in a variety of formats, like JSON, CSV, XML. You can also generate reports and have them emailed to you using Shodan.



WARNING: Consult your CISO office before sharing results and reports with external audiences.

What results mean

So you found IoT devices on your network connected to the Internet but does that mean they pose a risk?

- Is this a device that should be on a network segment behind a firewall? Is there a reason it is publicly available?
- Is it a device that enables remote access to configure key systems like building power or other operational technology?
- Could it be used as a jump point for bad actors?
- Is it a device on a watch list for password default or one that uses a protocol with known vulnerabilities, like Telnet?

If you find devices that meet some of these criteria, you may want to notify both device owners and your CISO office.

How to get started

WARNING: Consult your CISO office before proceeding since prior notice and authorization may be required.

Anyone can run basic searches in Shodan and Censys for free, although advanced searching and reporting features may have a cost. Create accounts at:

shodan.io
censys.io

Try searches with IoT keywords, such as “camera.” Also, Shodan has a specific filter for finding Industrial Control System devices: the ics category and Censys syntax includes the “scada” tag for Supervisory control and data acquisition components of industrial control systems.