Accessible ICS Report

A scan report on exposed ICS devices in your network or constituency

@shadowserver

contact@shadowserver.org

SHADOWSERVER.ORG

Presentation Aims & Objectives

- Introduce the Accessible ICS Report
- Highlight a sample Accessible ICS report
- Describe key features of the report
- Demonstrate how a National CERT or network owner can action an Accessible ICS Report
- Offer general guidance on how to protect against ICS attacks
- Provide a key list of Shadowserver online resources to enable report subscription and use

SHADOWSERVER

Industrial Control Systems (ICS)

- Industrial Control Systems is a general term that encompasses several types of control systems and associated instrumentation used for industrial process control (from Wikipedia)
- Examples include supervisory and control acquisition systems (SCADA), distributed control systems (DCS), programmable logic controllers (PLCs), industrial switches, interface-converters and gateways
- Used for operations in multiple service sectors such as transport, power plants, utilities, and many other facilities
- Long list of both industrial standard and proprietary protocols used

Industrial Control Systems (ICS)

- Many ICS devices also have standard Web or other networking protocols enabled, not just native ones

- Multiple types of ICS device that have a public facing internet connection are at risk, with many having vulnerabilities documented in the past, allowing for exploitation similar to the IT world:
  - Remote Code Execution
  - Privilege Escalation
  - DoS

- Ever increasing ICS device populations, poorly understood and often proprietary protocols, weak security controls make these public facing ICS an attractive attack vector

- There is typically no need for any of these devices to be exposed to the public Internet. They constitute an unnecessary attack surfaces and should be removed from the public Internet immediately (unless a honeypot)

SHADOWSERVER

Accessible ICS Report Summary

- https://www.shadowserver.org/what-we-do/network-reporting/accessible-ics-report/

- Report contains responses for many different “native” ICS protocols that Shadowserver is scanning for, all lumped together in one report (instead of having a separate report for every protocol)

- Report is available as a file in CSV format

- The report filename contains `scan_ics`

- All timestamps are in UTC

- Reports can be sent as e-mail attachments, or downloaded via HTTP or obtained via a RESTful API

- For more documentation on API access, please visit the below URLs and send a request for access to contact@shadowserver.org

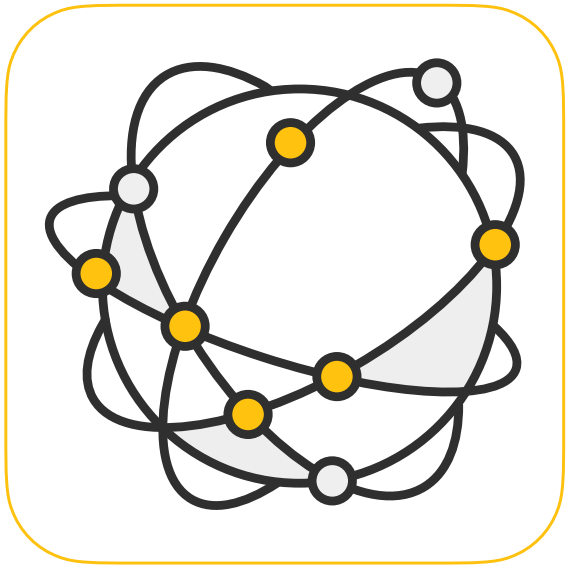
https://www.shadowserver.org/what-we-do/network-reporting/api-documentation/

https://www.shadowserver.org/what-we-do/network-reporting/api-reports-query/

SHADOWSERVER

ICS Protocols Scanned (2022-04-26)

- BACnet (port 47808/udp)
- CODESYS (port 1200/tcp, port 2455/tcp)
- Crimson V3 (port 789/tcp)
- DNP3 (port 20000/tcp)
- EtherNet/IP (port 44818/tcp)
- GE-SRTP (port 18245/tcp)
- HART (port 5094/tcp)
- IEC 60870-5-104 (port 2404/tcp)
- MELSEC-Q (port 5007/tcp)
- Modbus (port 502/tcp)
- OMRON FINS (port 9600/udp)
- OPC UA Binary (port 4840/tcp)
- PC Worx (port 1962/tcp)
- ProConOS (port 20547/tcp)
- Siemens S7 (port 102/tcp)
- Tridium Niagara Fox (port 1911/tcp)



SHADOWSERVER

Accessible ICS Report Summary

Accessible ICS Report

LAST UPDATED: 2022-04-20

This report contains a list of devices that are responding to various specialized ICS (Industrial System) protocols, such as **Modbus** or the **Siemens S7 protocol.**

As of 2022-04-15 we scan for the following protocols:

- BACnet (port 47808/udp)
- CODESYS (port 1200/tcp, port 2455/tcp)
- Crimson V3 (port 789/tcp)
- DNP3 (port 20000/tcp)
- EtherNet/IP (port 44818/tcp)
- HART (port 5094/tcp)
- IEC 60870-5-104 (port 2404/tcp)
- MELSEC-Q (port 5007/tcp)
- Modbus (port 502/tcp)
- OMRON FINS (port 9600/udp)
- OPC UA Binary (port 4840/tcp)
- PC Worx (port 1962/tcp)
- ProConOS (port 20547/tcp)
- Siemens S7 (port 102/tcp)

https://www.shadowserver.org/what-we-do/network-reporting/accessible-ics-report/

FIELDS

timestamp	Timestamp when the IP was seen in UTC+0
ip	IP of the detected device
protocol	Protocol of the response
port	Port response was received from
hostname	Hostname of the device (may be from reverse DNS)
tag	Tag, set to specific ICS protocol, such as Modbus or S7
asn	AS of the detected device
geo	Country of the detected device
region	Region of the detected device
city	City of the detected device
naics	North American Industry Classification System Code
sic	Standard Industrial Classification System Code

SAMPLE

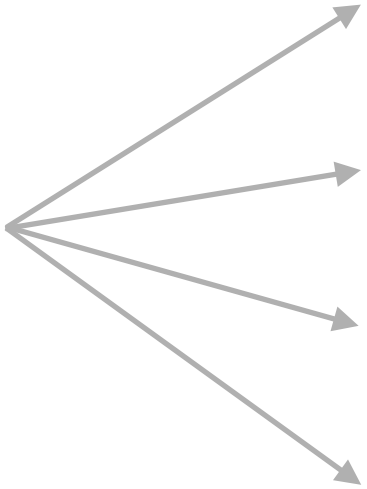
```
timestamp,ip,protocol,port,hostname,tag,asn,geo,region,city,naics,sic,sector,device_vend
"2010-02-10 00:00:00",192.168.0.1,tcp,502,node01.example.com,modbus,64512,ZZ,Region,City
"2010-02-10 00:00:01",192.168.0.2,tcp,502,node02.example.com,modbus,64512,ZZ,Region,City
"2010-02-10 00:00:02",192.168.0.3,tcp,502,node03.example.com,modbus,64512,ZZ,Region,City
```

SHADOWSERVER

Action an Accessible ICS Report

timestamp	protocol	src_ip	port	hotsname	tag	asn	Region	sic	Vendor
06/04/2022 00:02	tcp	65.18..X.X	502	node01.example.com	modbus	15600	nidau	XXX	Schneider Electric

Key event fields



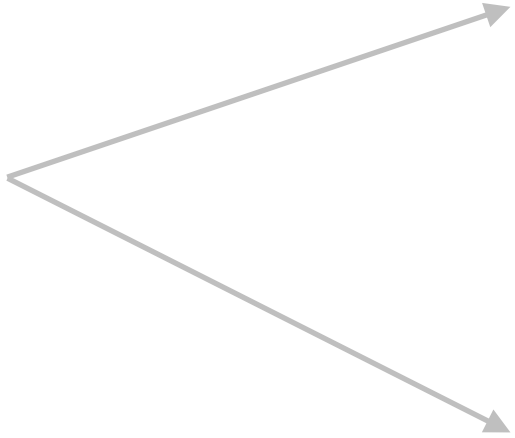
timestamp	Timestamp when the IP was seen in UTC+0
ip	IP of the detected device
protocol	Protocol of the response
port	Port response was received from
hostname	Hostname of the device (may be from reverse DNS)
tag	Tag, set to specific ICS protocol, such as Modbus or S7
asn	AS of the detected device
geo	Country of the detected device
region	Region of the detected device
city	City of the detected device
naics	North American Industry Classification System Code
sic	Standard Industrial Classification System Code
sector	Sector of the IP in question
deivce_vendor	Vendor name of device

SHADOWSERVER

Action an Accessible ICS Report

timestamp	protocol	src_ip	port	hotsname	tag	asn	Region	sic	Vendor
06/04/2022 00:02	tcp	65.18..X.X	502	node01.example.com	modbus	15600	nidau	XXX	Schneider Electric

IP WHOIS 65.18.X.X



```
inetnum:        65.18.128.0 - 65.18.159.255
netname:        FTTH-NET-BRAS-1
descr:          FTTH Network
descr:          Quickline AG
descr:          Nidau, Switzerland
country:        CH
admin-c:        LSAN1-RIPE
tech-c:         LSAN1-RIPE
status:         ASSIGNED PA
mnt-by:         CH-LAN-MNT
created:        2018-07-30T11:46:17Z
last-modified:  2018-07-30T11:46:17Z
source:         RIPE # Filtered

role:           Quickline AG
address:        Dr. Schneider-Strasse 16
address:        CH-2560 Nidau
address:        Switzerland
phone:          +41 32 559 99 99
fax-no:         +41 32 559 99 90
admin-c:        MJ393-RIPE
admin-c:        RM738-ORG
admin-c:        MB42573-RIPE
admin-c:        MK23361-RIPE
tech-c:         MJ393-RIPE
tech-c:         RM738-ORG
tech-c:         MB42573-RIPE
tech-c:         MK23361-RIPE
nic-hdl:        LSAN1-RIPE
mnt-by:         CH-LAN-MNT
created:        2002-07-08T13:45:40Z
last-modified:  2020-04-02T07:09:35Z
source:         RIPE # Filtered
abuse-mailbox:  abuse@qlgroup.ch
```

SHADOWSERVER

Verifying our results

- False positives are normally unlikely in this scan. We only report IPs that have responded to specific native ICS protocol queries. However:
  - It is possible in some cases that due to multiple interfaces or routing anomalies we see a different IP responding to our scans (than the IP we were actually querying)
  - In some cases attackers that monitor our scans spoof UDP packets in response, thus leading to false positives (applies only to UDP scans).
  - It is possible that due to a delay in reporting, a device was taken offline by the time you received the report

- If you would like to verify a result by scanning, in many cases you can use an *nmap* scripts for the task. See: https://nmap.org/nsedoc/scripts/

- If you are unable to find a way to verify a result, please contact us

- You may also be running an ICS honeypot … in this case, you can probably ignore our report!

SHADOWSERVER

ICS - PROTECT

- As a rule, ICS devices should never be publicly accessible on the Internet!
- Make sure you at least firewall them to block access from the Internet
- However, the topic of securing ICS devices is more complicated than that
- Some recommended reading to start!:
  - Securing Industrial Control Systems by CISA :

https://www.cisa.gov/publication/securing-industrial-control-systems

  - NIST Special Publication 800-82 :

https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-82r2.pdf

  - SANS Introduction to ICS Security :

https://www.sans.org/blog/introduction-to-ics-security/

SHADOWSERVER

Summary & Key Report Pages

Reports overview

- https://www.shadowserver.org/what-we-do/network-reporting/get-reports/
- https://www.shadowserver.org/what-we-do/network-reporting/
- https://www.shadowserver.org/what-we-do/network-reporting/accessible-ics-report/

Report Updates

- https://www.shadowserver.org/news-insights/
- Twitter @shadowserver
- Mailing list access send request to contact@shadowserver.org and request access to public@shadowserver.org
- Or subscribe directly at https://mail.shadowserver.org/mailman/listinfo/public

Reports API

- Request access to **contact@shadowserver.org**
- https://www.shadowserver.org/what-we-do/network-reporting/api-documentation/
- https://www.shadowserver.org/what-we-do/network-reporting/api-reports-query/

SHADOWSERVER

SHADOWSERVER

Lighting the way to a more secure Internet

@shadowserver

contact@shadowserver.org

SHADOWSERVER.ORG