Project SHINE: 1,000,000 Internet-Connected SCADA and ICS Systems and Counting

SUBMITTED BY ERIC BYRES ON THU, 2013-09-19 21:00

Eric Byres: One of the statements I continue to hear as I talk to executives, managers and engineers is "None of our SCADA or ICS equipment is accessible from the Internet." So this week's blog contributor, Bob Radvanovsky, of www.infracritical.com, explains Project SHINE – his effort to determine if this statement is fact or fiction.

Shining a Light on a Big Problem

By Bob Radvanovsky

Project SHINE (SHINE meaning SHodan INtelligence Extraction) was developed to extract information about the existence of SCADA and ICS devices accessible from the Internet. We use an existing online search engine called SHODAN that scans the Internet looking for attached devices. Those devices can be computers, printers, switches, PLCs, SCADA RTUs, etc: **anything** with an IP address.

The SHODAN search engine works by searching for commonly used TCP/UDP port numbers (for more on port numbers read this blog), such as:

- 22 (SSH)
- 23 (Telnet)
- 21 (FTP)
- 80 (HTTP)
- 443 (HTTPS)
- and 161 (SNMP)

It sends connection requests to those devices and records the header information from the devices if they respond. And unless they are behind a firewall, most devices will respond, even if it is just to say "go away."

This header information often shows the type of software or device answering the request, what version it is, and if the device is patched (sometimes). This is all stored in an online accessible database. Think of it as Google for devices, rather than websites.

Of course it is the PLCs and RTUs that interest us, so we have created specific search terms related to SCADA and ICS products. So far we have just shy of 700 searchable terms and are adding more every week. When we find these terms in the SHODAN database, we are pretty sure that SHODAN has found a SCADA/ICS product.

SHODAN's massive database of header information is extremely useful for both the good guys and the bad guys. An adversary can conduct "indirect intelligence" gathering against a specific software application, hardware device, firmware, IP address, or some combination **without ever visiting the target's network location**.

All he or she has to do is query the database. To use the Google metaphor again, it is like spying on a person by simply looking at what is stored in Google. Likely there is so much material there that you never actually have to visit the person's website or Facebook page. So you can stay under the radar until you are ready to do something bad.

1,000,000 SCADA and control systems devices on the Internet?

Project SHINE development started mid-2008 and began ingesting raw data in mid-April 2012. It was initiated to determine a baseline of just how many SCADA/ICS devices and software products are directly connected to the Internet. At the time we started, many people said that the answer to our question would be "*very few, if any*."

To date, we have not reached a baseline (aka, "the bottom") in the total number of devices we discovered. The average number of **new** SCADA/ICS devices found every day is typically between 2000 and 8000. So far we have collected over 1,000,000 unique IP addresses that appear to belong to either SCADA and control systems devices or related software products.

These devices include the traditional SCADA/ICS equipment, such as RTUs, PLCs, IEDs/sensor equipment, SCADA/HMI servers, and DCS. Non-traditional SCADA/ICS devices include:

- medical devices
- traffic management systems
- automotive control
- traffic light control (includes red-light and speeding cameras)
- HVAC/environment control
- power regulators/UPSs
- security/access control (includes CCTV and webcams)
- serial port servers (many of which include Allen-Bradley DF1 capable protocols)
- data radios (point-to-point 2.4/5.8/7.8 GHz direct-connected radios)

Some of the more interesting control applications we have uncovered are off-road mining trucks and crematoriums. Why these are connected to the Internet is a mystery to us.

The manufacturers of the devices that we uncovered include (but are not limited to):

Allied Telesis	Delta Controls	LOGPAC	National Instruments	VxWorks
Alcea	Digi	Itron, Inc.	OMRON	Wago
ABB	Ecessa	Koyo	openSCADA	WindWeb
ADCON	Ericsson	KMC	Ourman	Wonderware
APC	Emerson	Komatsu	Phoenix Contact	
Allen-Bradley	EIG	Lennox	Phillips	
AKCP	EnergyICT	Leica	mGuard	
Barik	Falcon	Lancom	Schneider Electric	
Caterpillar Inc.	Force10	Lantronix	Siemens	
Cimetrics	Funkwerk	Moxa	RUGGEDCOM	
CIMON	GE	LonWorks	Rockwell Automation	
Control4	Genohm	LG	Powertech	
CODESYS	Hirschmann	Mitsubitshi	STULZ	
Clorius Controls	Honeywell	Motorola	SoftPLC	
Datawatt	Liebherr	Niagara	Telemecanique	

Quite a list...

We continue to find more manufacturers monthly and continue adding/ingesting raw data into our database. Most of these devices have been discovered using the commonly-known networking ports (web, telnet, and FTP are some of the more common ones; SNMP appears to be growing as well).

In many cases, a default web interface, usually with administrative privileges, is active on the SCADA or ICS device. Rarely is it ever disabled by the end user. We believe that there are two possible reasons for this.

1. The systems integrator is a contractor who doesn't have a full knowledge of the product being installed.

2. Owner of this system is unaware that there is a web interface that is enabled by default from the manufacturer.

Regardless of the reason, there are a lot of devices sitting on the Internet with unsecured web servers.

What Does it All Mean?

Essentially, the Internet is "public domain"; anything and everything attached to it can be seen, touched, accessed by anyone, anywhere, anytime. If SHODAN - and for that matter, Google, Yahoo, Bing, etc. - can "see" a SCADA/control systems device or software product, then so can the bad guys. An adversary wanting to damage a control system can have grave consequences to not only the companies that own and operate those devices and software products, but to their customers as well.

This applies to any control system, but service interruptions to the most important infrastructure sectors, such as Energy, Water and Transportation, can have grave consequences to our society. Asset owners are being encouraged to safeguard their critical infrastructure cyber assets, but this will be a long and arduous journey. We hope that through our SHINE project, we will encourage asset owners to be more proactive and to think about security before connecting a device/software product to the Internet.

The Future of Project SHINE

We intend to perform our own series of scans for SCADA/control systems through a new (undisclosed) method in the not-too-distant future. Additionally, we may make available SHINE data to be used as part of a compliance service for asset owners, but we are struggling with an appropriate business model. More to come...

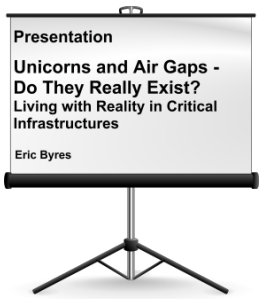
Eric Byres: Bob notes that SHINE has found over 1,000,000 "SCADA" devices sitting on the Internet. Of course none of these belong to any company we ever have talked to, do they? Or are control devices accidentally getting connected in ways engineers and managers aren't aware of?

Tell us what you are seeing at your company – are ICS devices sneaking onto the Internet?

Tofino Security thanks Bob Radvanovsky for this article.

Related Content to Download

Presentation - "Unicorns and Air Gaps - Do They Really Exist?"



Download this presentation and benefit from:

- Knowing the current status of air gaps and industrial control systems
- Understanding why air gaps are a challenge with today's infrastructure systems
- Seeing an oil and gas refinery example for dealing with multiple pathways

Related Links

- Webpage: SCADASEC Mailing List
- Webpage: Shodan HQ
- Webpage: Shodan Wikipedia
- Blog: SCADA Security Basics: Why are PLCs so Insecure?
- Blog: SCADA Security & Deep Packet Inspection – Part 1 of 2
- Blog: SCADA and ICS Cyber Security: Facing the Facts
- Blog: #1 ICS and SCADA Security Myth: Protection by Air Gap

Subscribe to the "Practical SCADA Security" news feed

Add new comment

Your name *

E-mail *

The content of this field is kept private and will not be shown publicly.

Subject

Comment *

- No HTML tags allowed.
- Web page addresses and e-mail addresses turn into links automatically.
- Lines and paragraphs break automatically.

More information about text formats

Verification *

Type the characters you see in the picture; if you can't read them, submit the form and a new image will be generated. Not case sensitive. Switch to audio verification.

Save Preview