Project RUGGEDTRAX
SCADA/ICS Analysis

Findings Report

Based on intelligence gathered from an
ICS device placed directly onto the Internet
14 Oct 2014 through 27 Dec 2014

28 Nov
2015

This following findings report contains specific details of devices that are directly connected to the Internet that may be utilized for mission critical operations associated to one (or more) critical infrastructure sectors (and their respective industries). Information contained within this report should only be used for awareness purposes.

LEGAL DISCLAIMER

Project RUGGTEDTRAX is a research project designed to observe and gather data used to provide some proof of any threats and risk associated with SCADA and industrial control system devices that appear to be directly connected to the Internet. The project is but one of several projects to raise public awareness of such devices that may impact one (or more) critical infrastructure sectors (and their respective industries), while demonstrating providing quantifiable proof of any impacts to these devices that are publicly accessible through the Internet.

Contact Information

For more information about Project RUGGEDTRAX, please send correspondence to:

Project RUGGEDTRAX Inquiries
projectruggedtrax@infracritical.com

Introduction

This project is subset to Project SHINE (SHodan Intelligence Extraction), providing one example of what would happen if a device was to be directly connected to the Internet.

At no point in time was this project intended to identify any shortcomings of the manufacturer's efforts in remediating any of the known vulnerabilities, nor was it intended to place any blame or negligence towards the manufacturer in any manner whatsoever. The choosing of the specific device was to provide a simplified example which could be easily demonstrated as a form of substantiation of our position provided through Project SHINE. It should be noted that the device utilized, has an out-of-date version of its firmware that is subject to one or more known vulnerabilities that currently exist. The manufacturer has taken steps previously to remediate those versions of firmware by providing updated versions; it is strongly suggested that any asset owners running this specific version of firmware update/upgrade to the latest version as a precautionary effort.

Objective

The objective of this project is to provide some form of substantiation that directly connecting an ICS device onto the Internet could have consequences. As such, the premise of this project was to:

(1) Obtain current ICS equipment through public sources (eBay), and deploy this equipment as actual cyber assets controlling perceived critical infrastructure environments;

(2) Ascertain any pertinent threat or attack vectors, as well as scope and magnitude of any attacks against the perceived critical infrastructure environments;

(3) Record network access attempts, and analyze captured network packets for any patterns; and,

(4) Report redacted findings for public awareness to governments and media outlets.

Device Specifications

The equipment chosen is a serial-to-Ethernet converter that has capabilities of controlling two (2) ICS devices utilizing either the MODBUS/TCP or DNP3 network protocols.

The manufacturer is Siemens RuggedCom, and the device model is RS910, which is a 2-port serial-to-Ethernet converter that is DIN rail-mounted; a hardware diagram is shown below:

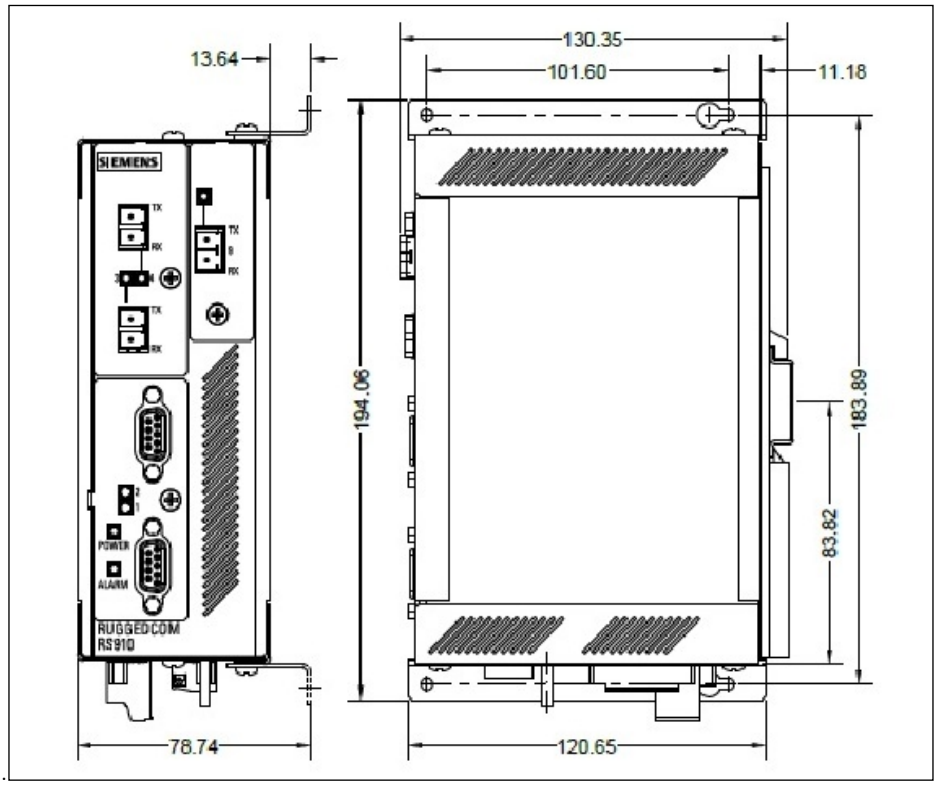


Figure 1.

The device is running the firmware release level of version 3.8.0. This version of the firmware is susceptible to several publicly known vulnerabilities, including the factory backdoor vulnerability, in which an adversary may bypass security controls by executing an application to obtain administrative privileges through a generated factory account and password. This feature was previously available as a method of accessing the device should an asset owner administrator lose their administrative privileged access to any Siemens RuggedCom device, and has since been remediated by Siemens RuggedCom.

Device Configuration

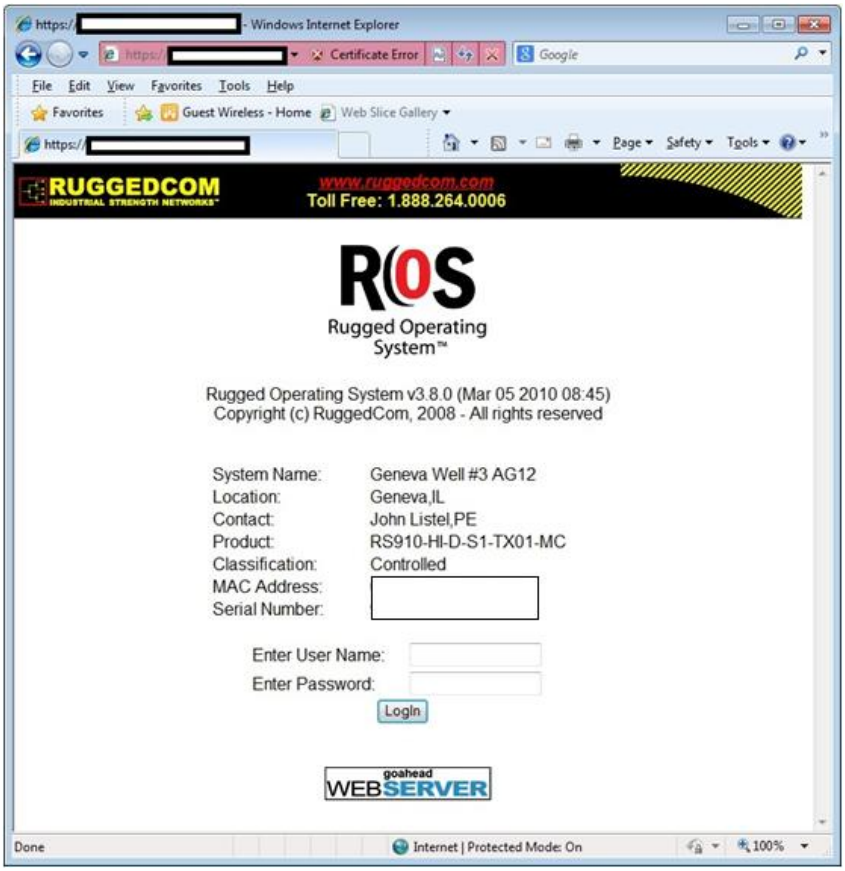
The device can communicate using the following protocols: TELNET, Trivial FTP (TFTP), Remote Shell (RSH), Secure Shell (SSH), SNMP, HTTP/HTTPS, MODBUS/TCP and DNP3. After resetting the device to factory defaults, all protocols are enabled and available.

The following protocols were disabled: TELNET, TFTP, RSH, SNMP, and MODBUS/TCP.

The protocols HTTP/HTTPS and SSH are always required (outside of serial console), with minimal connectivity of at least ONE (1) allowed connection. **NOTE: The DNP3 protocol cannot be disabled.**

The device was portrayed and configured as a water pump to a wellhead for a local municipality. In this case, the local government is Geneva, Illinois.

The contact name is fictitious; any resemblance to any individuals with a similar name is entirely coincidental. A screen shot of the redacted web interface is shown below:



[1] [2]

Figure 2.

[1] The name "RUGGEDCOM", "Rugged Operating System", and "ROS" are copyright and registered trademarks of Siemens RuggedCom.

[2] The name "goahead" and "goahead WEBSERVER" are copyright Embedthis Software.

The device was placed online 14-Oct-2014 (Tuesday), and taken out of service 27-Dec-2014 (Saturday).

Once placed directly on the Internet, the device was monitored closely for any activity. For sake of brevity, this report was limited to 53 countries, identifying the most significant counted countries, top-to-bottom, left-to-right, which include the following:

Country	Count	Percent	Country	Count	Percent	Country	Count	Percent
China	**125299**	**89.2424**	**France**	**3344**	**2.3817**	**United States**	**3247**	**2.3126**
Germany	**1794**	**1.2778**	**Korea**	**1602**	**1.141**	**Singapore**	**1576**	**1.122**
Tunisia	509	0.363	Ukraine	327	0.233	Indonesia	253	0.180
Canada	220	0.157	Turkey	198	0.141	Italy	196	0.140
Japan	193	0.137	Poland	185	0.132	Netherlands	183	0.130
Lithuania	178	0.127	United Kingdom	159	0.113	Hong Kong	137	0.0.98
Russian Federation	105	0.075	Brazil	85	0.061	Vietnam	81	0.058
Sweden	76	0.054	Belarus	65	0.046	Austria	64	0.046
Taiwan	56	0.040	Panama	47	0.033	Peru	45	0.032
Mexico	44	0.031	Kazakhstan	25	0.018	Norway	17	0.012
Israel	12	0.009	Estonia	10	0.007	India	8	0.006
Hungary	7	0.005	Iran	7	0.005	Malaysia	7	0.005
Romania	7	0.005	Belgium	6	0.004	Moldova	6	0.004
Greece	3	0.002	Spain	3	0.002	Thailand	3	0.002
Australia	2	0.001	Kenya	2	0.001	Pakistan	2	0.001
Argentina	1	0.0007	Costa Rica	1	0.0007	Czech Republic	1	0.0007
Denmark	1	0.0007	Ecuador	1	0.0007	Ireland	1	0.007
Satellite Provider[3]	**1**	**0.0007**	Slovakia	1	0.0007			

Table 1.

The top-most country is highlighted in **red**; the remain 4 top-most countries are highlighted in **yellow**; of 100%, the 5 top-most countries represent **96.3555%** or **135,286** out of **140,403** non-unique entries.

[3] Based on the IP address, this belonged to an undisclosed satellite provider.

Percentages

With Chinese-based IP addresses representing 89.2424%; the next 4 countries representing 7.1131%; and the remaining 48 countries representing 3.6445%; out of a total of 53 countries.

Counts

With Chinese-based IP addresses represent 125,299 non-unique entries; the next 4 countries represent 9,987 non-unique entries; and remaining 48 countries representing 5,117 non-unique entries.

Total count is 140,403 non-unique entries out of 140,430 total entries.

The difference represents 27 erroneous entries (or 0.0192%) due to network connection retries.

The margin of error is ±3.04%.

Graph (Country Count Distribution)

The graph (shown below) demonstrates just how skewed the access attempts against the device were identified per country-based IP address(es). Please note that this does not infer that the country identified is representative of a nation-state sanctioned activity; merely, it is representative of the IP addresses correlated to a specific network address block for that country.

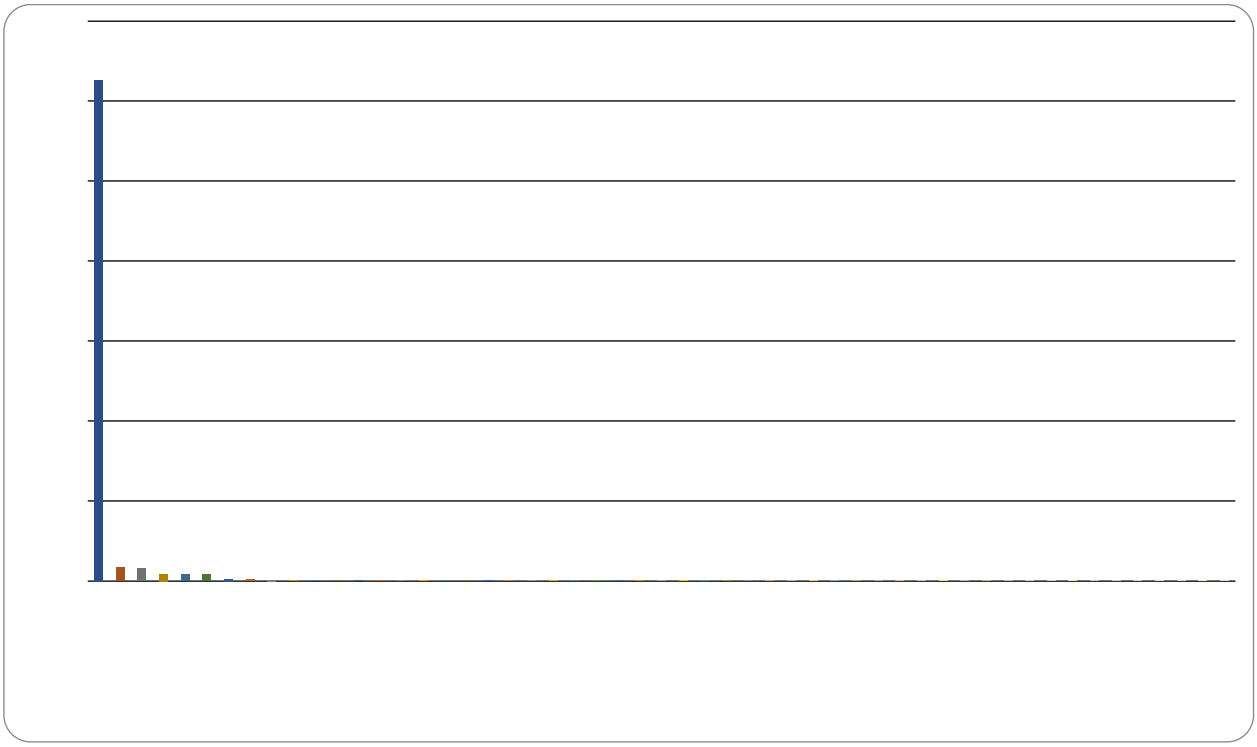


Table 2.

Graph (IP Network Address Count Distribution)

The graph (shown below) shows the top 5 IP addresses that are part of the 140,403 count distribution, with a count of 12,112, representing 8.6266% of the total count. Of the 5 IP addresses identified, numbers 1, 3, 4 and 5 are from Chinese-based IP addresses; number 2 is from a French-based IP address.

Identified as the following:

China: 3044, 2258, 2175, and 2056.
France: 2579.

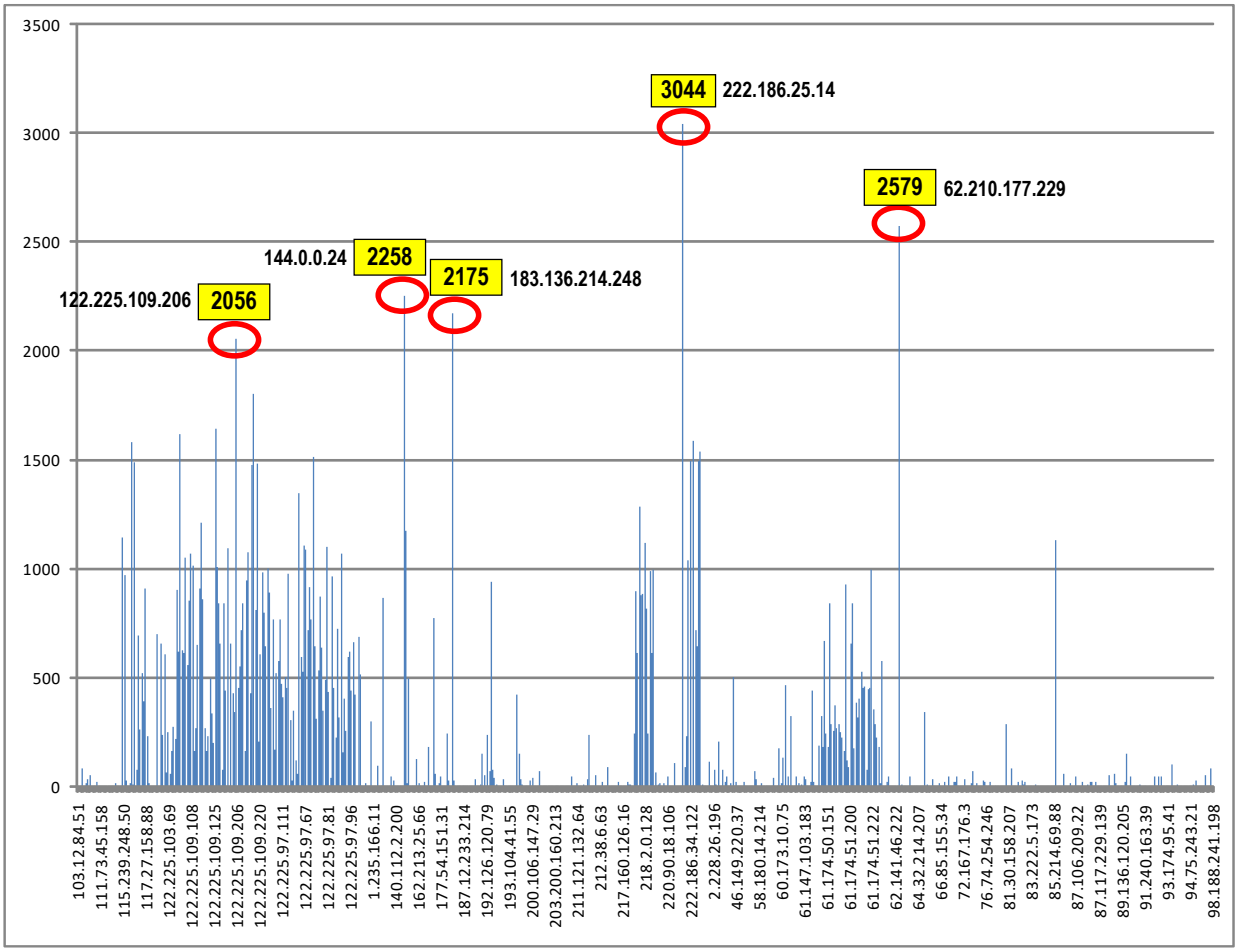


Table 3.

The top 5 IP addresses are part of a total of 651 IP addresses, minus 3 IP addresses used for local and/or remote access during the packet capture and evaluation.

Conclusion

Based on the data examined, it appears that the majority of the access attempts originated from IP addresses belong to the country of China. This does not mean nor infer that any of the access attempts were conducted by anyone from the Chinese nation, its government, or any organization based out of China.

The originating IP addresses may be proxied in an effort to mask the originating IP address sources.

It would be an assumption that these access attempts were directed primarily at a critical infrastructure specifically; however, this does not mean that such an attempted access could not exist. Majority of the attempts appear to be automated, with repetitive attempts several times within 1-2 seconds of each other, over the course of several minutes. The only exception would be accounts other than "root", which appear to be manually attempted ("admin", "support", "test", "bin", "mysql", et. al).

In conclusion, the data provided within this report, as well as through the GitHub repository, will allow anyone to see the amount of probing attempts against unprotected devices may experience. As this experiment was conducted for only 75 days (roughly 2.5 months), this demonstrates the intensity by which these probes are performed.

This data is being released publicly in an attempt to provide further aware and understanding of the magnitude of how bad it is for placing equipment directly onto the Internet without any form of protection whatsoever. Please utilize the data as you see fit; however, we request that credentials be given to "Infracritical" should you utilize any or all of the data set.

This report may be found on SlideShare:

http://www.slideshare.net/BobRadvanovsky/project-ruggedtrax-findings-report-28nov2015

The supporting data may be found on GitHub:

https://github.com/infracritical/ruggedtrax