infracritical
YOUR INFRASTRUCTURE, THEIR FUTURE

Project RUGGEDTRAX
SCADA / ICS Analysis

Preliminary Findings Report

21 Oct
2014

Based on intelligence gathered from an
ICS device placed directly onto the Internet
13 Oct 2014 through 16 Oct 2014

This following findings report contains specific details of devices that were 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 It should be noted that the device utilized has an out-of-date version of its firmware that is subject to one or more known vulnerabilities that currently exist.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 updates; it is strongly suggested that any asset owners running this specific version of firmware update or 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:

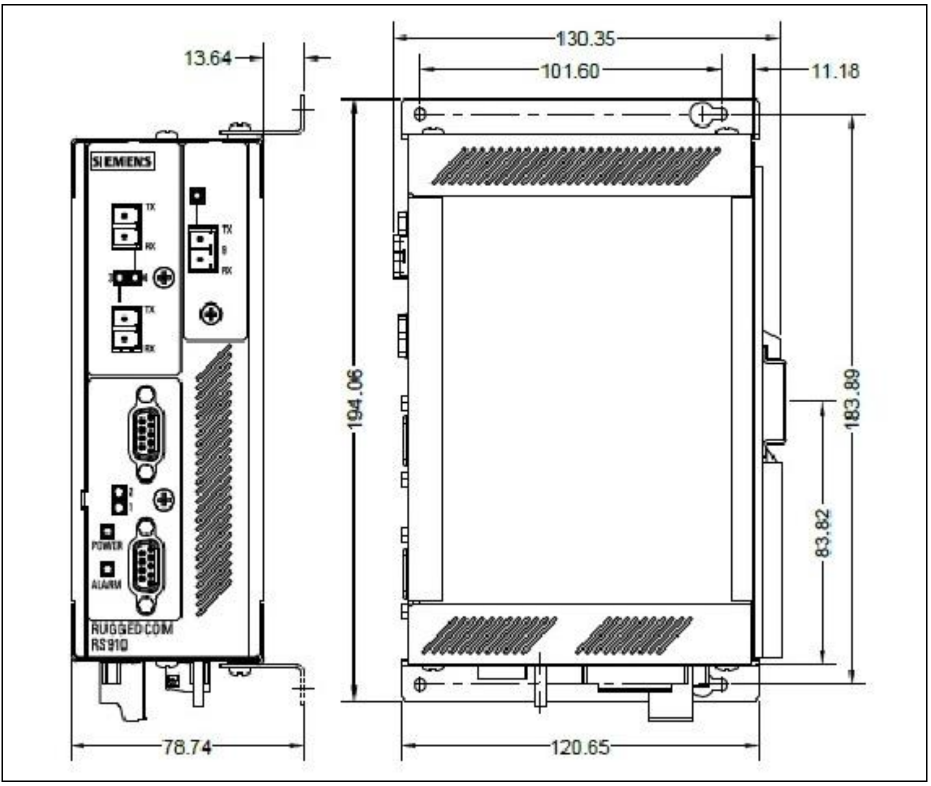


Figure 1.

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 access to any Siemens RuggedCom device, and has since been remediated by Siemens RuggedCom.

Device Configuration

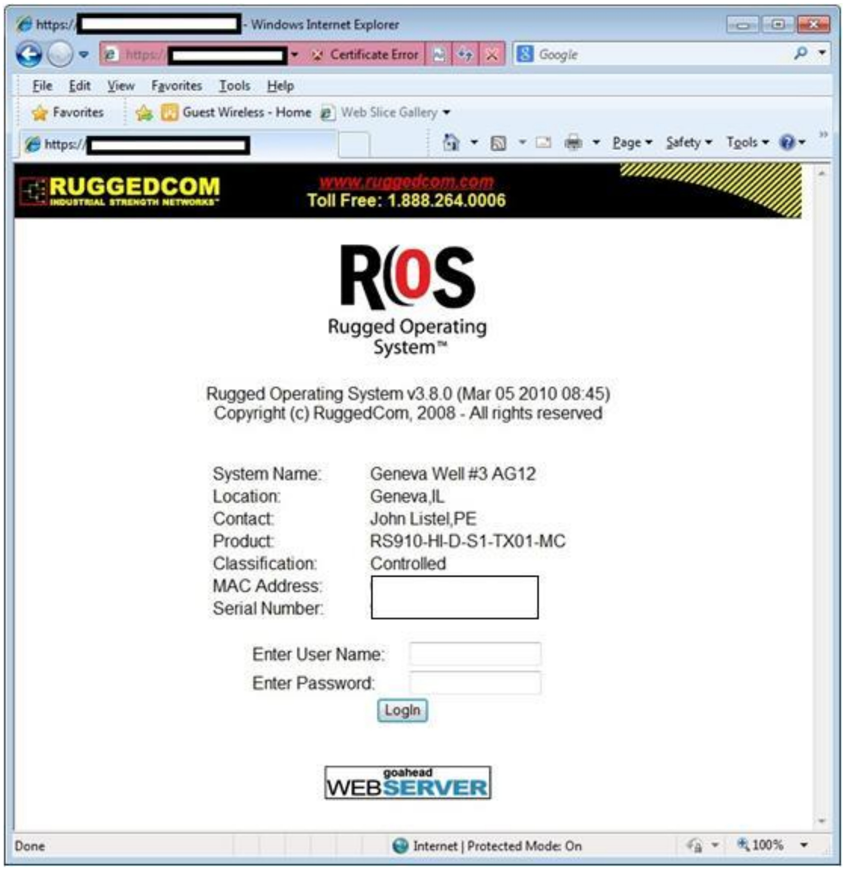
The device can communicate using the following protocols: TELNET, Trivial FTP (TFTP), Remote Shell (RSH), Secure Shell (SSH), SNMP, HTTP/HTTPS, MODBUS/TCP and DNP3. After resetting the device to factory defaults, all protocols are enabled and available.

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. *The DNP3 protocol cannot be disabled*.

The device was portrayed and configured as an access-point controlling a water pump to a wellhead for a local municipality's water system.

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:



Rugged Operating System v3.8.0 (Mar 05 2010 08:45)
Copyright (c) RuggedCom, 2008 - All rights reserved

System Name: Geneva Well #3 AG12
Location: Geneva,IL
Contact: John Listel,PE
Product: RS910-HI-D-S1-TX01-MC
Classification: Controlled
MAC Address: [redacted]
Serial Number:

Enter User Name:
Enter Password:
LogIn

[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 at 13-Oct-2014 (Monday) at approximately 1917 hrs Central.

The first attack began at approximately 2104 hrs Central, *less than two (2) hours from its inception*.

A snapshot was taken on 16-Oct-2014 (Thursday) prior to 0600 hrs Central; *at the time of the snapshot, metadata specific to the device's IP address was not harvested by the SHODAN search engine*.

Of the data analyzed, it was found that there were 4,261 entries, consisting of 16 unique IP addresses, representing 4 countries: China (12), Vietnam (1), United States (2), and The Netherlands (1).

Of the 4,261 entries, only 30 entries originated from IP addresses belonging to Vietnam, United States and The Netherlands. The remaining 4,231 entries all originated from IP addresses belonging to China.

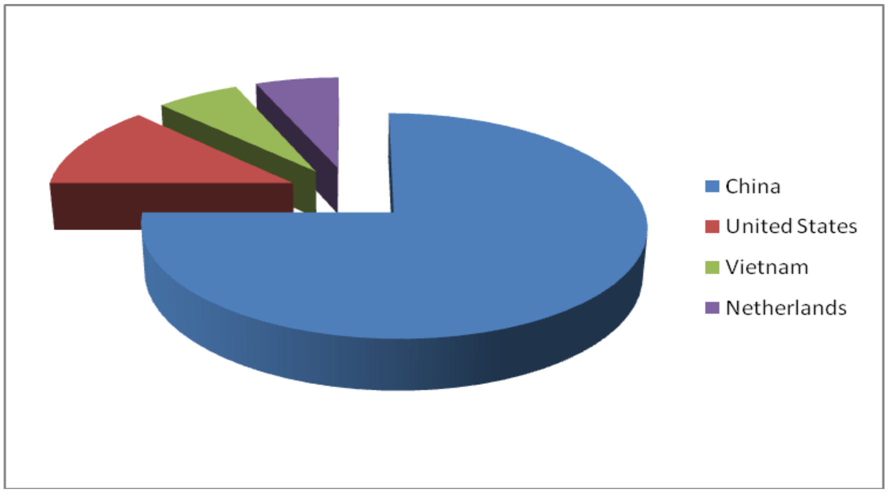


Figure 3.

China had 75% of the 16 IP addresses discovered, the United States at 12.50%, with the remaining IP addresses at 6.25% for Vietnam and The Netherlands (refer to Figure 3). China had 99.30% (4,231) of the entries logged, with the remaining 3 countries at 0.70% (30) of the entries logged (refer to Figure 4).

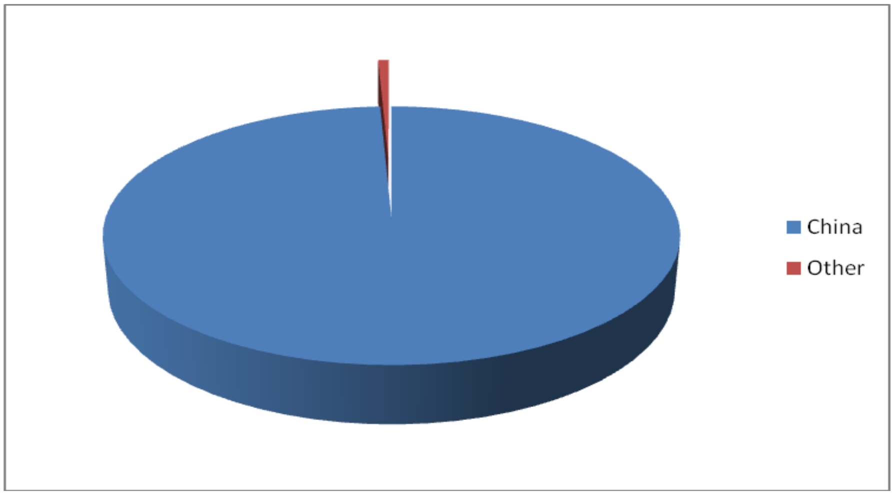


Figure 4.

Conclusion

Based on the data examined, it appears that majority of the attack attempts originated from IP addresses belong to the country of China. This does not mean nor infer that any of the attack attempts were conducted by Chinese nationals, 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.

As we were unable to determine any attack vectors other than what was logged within the device's log file, it appears that almost all attacks were performed against the Secure Shell (SSH) port. The accounts were primarily directed towards "root" – repetitively. Additional accounts included "admin", "support", "test", "bin", and "mysql". These accounts were only attempted a few times, with the "root" account representing almost the entire sampling.

It would be a presumption that these attack attempts were directed primarily at a critical infrastructure specifically; however, this does not mean that such an attack could not exist. Majority of the attempts appear to be automated, with repetitive attempts several times within 1-2 second periods 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" and "mysql"), as there are only a few logged entries, over the course of 1-2 minutes.

It is undetermined how the device was ascertained to be online, esp. within such a shortened timeframe of less than two (2) hours. As the device still has not been identified by the SHODAN search engine (at the date of this report), we cannot speculate as to how the device was known to be attacked.

It is too early to accurately determine if the device was specifically being attacked as a cyber asset controlling a critical infrastructure environment, or if this was merely a routine, automated "door knocking" used to determine if the device is vulnerable to any known attacks. A more detailed examination is currently underway, gathering network packet data, to determine if any ICS protocols were accessed (MODBUS/TCP and DNP3). This will be outlined within the final findings report for this project at a later date.

No further information is available at this time.