The SCADA That Didn’t Cry Wolf: Who’s Really Attacking Your SCADA Devices

Kyle Wilhoit
Sr. Threat Researcher
Trend Micro
Security Concerns - ICS vs. IT

ICS
• Correct commands issued (Integrity)
• Limit interruptions (Availability)
• Protect the data (Confidentiality)

IT
• Protect the data (Confidentiality)
• Correct commands issued (Integrity)
• Limit interruptions (Availability)
Primary Security Concerns

- **HMI:** Allows arbitrary command execution as well as set point modifications.
- **Data Historian:** Allows inbound traffic to secure network segments. (Replication of data)
- **RTU:** Allows remote communication ability

And many more...
Incidents Exist

- First half of 2013
- Over 200 confirmed “incidents”
SCADA Internet Facing

- Google-fu
- Shodan
- ERIPP
- Pastebin
- Twitter
SCADA Internet Facing

EXPOSE ONLINE DEVICES.
WEBCAMs. ROUTERS.
POWER PLANTS. IPHONES. WIND TURBINES.
REFRIGERATORS. VOIP PHONES.

TAKE A TOUR FREE SIGN UP

DEVELOPER API
Find out how to access the Shodan database with Python, Perl or Ruby.

LEARN MORE
Get more out of your searches and find the information you need.

FOLLOW ME
Contact me and stay up to date with the latest features of Shodan.

IN THE PRESS
Shodan pinpoints shoddy industrial controls.

Shodan is the Google for hackers.

It greatly lowers the technical bar needed to canvas the Internet...

'Shodan for Penetration Testers' presented at DEF CON 18

Firmen öffnen Stuxnet und Co. selbst

It's a reminder to many to know what's on your network...

dark READING

Computerangriffe werden einfacher.
Story Time!
Attacks

• Attacked several times - over a period of months
• Attackers gained access
• Exfiltrated data
• Not made public

• This is not a story…
• This happened…
In my basement...
Enter Honeypots…

HONEY
Not always the best diet
Phase 1:
Nov. 2012-March 2013
Physical Deployment

- Small town in rural America
- Water pump controlling water pressure/availability
- Population 18,000~
Physical Deployment

- Fake water pressure system Internet facing
- Very little security measures in place
- Could cause catastrophic water pressure failures if compromised
What They See

Diagram:
- Internet
- External IP
  - "Mimicking Control System"
- "PLC"
Physical Deployment

Diagram showing the physical deployment setup with components such as Internet, External Facing URL, Administrative Functions, Remote Management, Physical Host-Dell DL360, Salted Docs, Nano-10 PLC, Siemens SIMATIC S7-1200, and "Control System Network".
Phase 2: March. 2013-July 2013
Virtualized Environment

HONEYPOT COUNTRY DEPLOYMENT

IRELAND
RUSSIA
CHINA
JAPAN
SINGAPORE
UNITED STATES OF AMERICA
AUSTRALIA
BRAZIL
Logically…
Some Tools Used

- scADaBR
- Modbus.py
- EeEF
- Arduino
- OpenDNP3
- Pi-Face
- Siemens
- Raspberry Pi
- Snort
Vulnerabilities Presented

“If you can ping it, you own it”

- SNMP vulns (read/write SNMP, packet sniffing, IP spoofing)
- Specific ICS Vendor vulnerabilities
- HMI (Server) Vulnerabilities
- Authentication limitations
- Limits of Modbus/DNP3 authentication/encryption
- VxWorks Vulnerability (FTP)
- Open access for certain ICS modifications- fan speed, temperature, and utilization.
What’s an Attack?

- ONLY attacks that were targeted
- ONLY attempted modification of pump system (FTP, Telnet, Modbus, set points, etc.)
- ONLY attempted modification via Modbus/DNP3
- DoS/DDoS will be considered attacks
Total Attacks

-74 attacks

**ATTACK ORIGIN BREAKDOWN**

- **NETHERLANDS**: 2.7%
- **CHINA**: 9.5%
- **GERMANY**: 6.8%
- **KAZAKHSTAN**: 1.4%
- **CANADA**: 1.4%
- **USA**: 4.1%
- **AUSTRALIA**: 1.4%
- **MOLDOVA**: 1.4%
- **UKRAINE**: 2.7%
- **UK**: 1.4%
- **FRANCE**: 1.4%
- **PALESTINE**: 4.1%
- **POLAND**: 1.4%
- **SLOVENIA**: 1.4%
- **JAPAN**: 1.4%
- **RUSSIA**: 58.1%
Non-Critical Attack Profile - Source Countries

- 63 non-critical attacks

**Noncritical Attack Origin Breakdown**

- Netherlands: 3.1%
- China: 3.1%
- Germany: 6.3%
- Kazakhstan: 1.6%
- Canada: 1.6%
- USA: 4.7%
- Australia: 1.6%
- Moldova: 1.6%
- Ukraine: 3.1%
- Palestine: 4.1%
- Poland: 1.4%
- Slovenia: 1.6%
- Russia: 67.2%
Critical Attack Profile - Source Countries

- 11 critical attacks
Some Attack Stats

- Shutdown pump system
- Modify temperature output
- Modify pump pressure
- HMI access
- Modbus traffic modification
- Modification of CPU fan speed
- Data exfiltration attempt
“Hello sir, I am <name of city administrator> and would like the attached statistics filled out and sent back to me. Kindly Send me the doc and also advise if you have questions. Look forward you hear from you soon”

I HAVE A NEW HOBBY. IT'S CALLED PHISHING.

I SEND FAKE BANKING E-MAILS TO GULLIBLE EXECUTIVES. THEN I FIND OUT THEIR FINANCIAL INFORMATION AND USE IT TO STEAL THE MONEY THEY DON'T DESERVE.

Dear Customer,
This is your bank. We forgot your social security number and password. Why don’t you send them to us so we can protect your money.
Sincerely,
I. B. Banker

LOOKS LEGIT.
Cityrequest.doc

• Decoy doc - not much substance
Dropped Files

- CityRequest.doc
- File gh.exe dumps all local password hashes
  - `<gh.exe –w>`
- File ai.exe shovels a shell back to a dump server.
  - `<ai.exe –d1 (Domain) –c1 (Compare IP) –s (Service) >`
- Malware communicating to a drop/CnC server in China.
- exploiting CVE 2012-0158
- Malware communicating to a drop/CnC server in USA
  - `70.254.245.X`
  - `70.254.245.X`
  - `Has been taken down…by the US government`
Firmware Rippage

- Firmware was ripped off 3 times total
- Done in 3 separate intervals
- Used binwalk
- Viewed strings
- Exfiltrated unpacked firmware

```
$ strings MX1A4d.lod
...
XlatePhySec, h[Sec],[NumSecs]
XlatePhySec, p[Sec],[NumSecs]
XlatePlpChs, d[Cyl],[Hd],[Sec],[NumSecs]
XlatePlpChw, f[Cyl],[Hd],[Wdg],[NumWdgs]
XlateSfi, D[PhyCyl],[Hd],[Sfi],[NumSfis]
XlateWedge, t[Wdg],[NumWdgs]
ChannelTemperatureAdj, U[TweakTemperature],[Partition],[Hd],[Zone],[Opts]
WrChs, W[Sec],[NumSecs],[PhyOpt],[Opts]
EnableDisableWrFault, u[Op]
WrLba, W[Lba],[NumLbas],[Opts]
WrLongOrSystemChs, w[LongSec],[LongSecsOrSysSec],[SysSecs],[LongPhySecOpt],[SysOpts]
RwPowerAsicReg, V[RegAddr],[RegValue],[WrOpt]
WrPeripheralReg, s[OpType],[RegAddr],[RegValue],[RegMask],[RegPagAddr]
WrPeripheralReg, t[OpType],[RegAddr],[RegValue],[RegMask],[RegPagAddr]
```
Execution

• Upon execution of CityRequest.docx, files leaving the server in question after 5 days.
  – Fake VPN config file
  – Network statistics dump
  – SAM database dump
  – Gain persistence via process migration
• Won’t execute on Office 2010.
Exfiltration: Days 5-17

1. Attacker sent spear phished email
2. Attachment opened
3. Backdoor shoveled
4. Process Migration
APT1 Report

- APT1 (Comment Crew) report released in Feb 2013.
- Included many APT variants we’ve seen.
- One of particular interest was HACKSFASE.
- Commonly used in energy sector.
Examination

ERROR! Cannot cancel connect to %s\IPC$.
%s\IPC$
system32\system32\system32\WindowsSubSystemForLinux\tsm1\com</p>

Get to share %s local path failed: error %d
Get share %s unicode form failed: error %d
%s: %d
The last Error Code is r+b

User name or Password input wrong.
Domain Name input wrong.
The Remote Machine input wrong.
tthacksfas@#$
ERROR! Cannot connect to %s\IPC$.
%s\ADMIN$
“APT1” is Still Active

• Operation Siesta- Published last week
• Uses “sleep” functionality
• Uses valid looking download links
• Uses targeted documents (Sometimes)
  • CVE 2012-0158
  • CVE 2013-3906
Attribution
Attribution

- IP
- BeEF
- Code Analysis
BeEF Usage

- Detect Tor
- Get Registry Keys
- Get Physical_Location
- Get_System_Info
- Get_Internal_IP
Attacker Profile

- Most attacks appeared to be non-targeted
- Many attackers were “opportunists”
- Some were targeted…

![Attacker Profile Diagram](image-url)
Some Takeaways

• Red team/Blue team often
• Perform specialized vulnerability assessments
• Control contractors
• Perform basic security controls
  • Network segmentation
  • Two-factor authentication
  • Patch your stuff!
  • Lockdown external media
  • Manage vulnerabilities
  • Classify your data/assets
  • etc.
Email  kyle_wilhoit@trendmicro.com
Non-Work  kylewilhoit@gmail.com
Twitter  @lowcalspam