World Wide ICS Honeypots: A Study into the Deployment of Conpot Honeypots

Sam Maesschalck
Lancaster University
Introduction

- ICSs often lack inherent security measures
- When connected to the Internet they are exposed to remote threats
- Adversaries targeting critical infrastructure environments include nation-states
- Honeypots can provide threat intelligence to identify threats and adversaries
Introduction

• Low-interaction honeypots are extremely popular
  • Easy to deploy
  • Simulated systems
  • Lack comprehensive interactions
• High-interaction honeypots
  • Risky
  • Require high level of resources
• Conpot is the most popular low-interaction ICS honeypot deployed on the Internet
  • But contains many common signatures
• Does the ease of detection hinder the detection of sophisticated attackers?
Contributions

The core contributions of this research are:

- Identify discrepancies between default Conpot and a real PLC
- Evaluate which changes to Conpot lead to more useful interactions
- Quantify the default Conpot deployments on the Internet
- Identify cases of obfuscation attempts
Conpot v.s. PLC
Setup

**Conpot**
- Default Configuration
- S7-200 template
- Ubuntu 20.04

**PLC**
- Siemens S7-300 PLC
- Deployed within our ICS Lab
- Basic configuration
Experiment

- NMAP
  - Slow comprehensive scan
  - Intense scan
  - Port 102 scan
  - Built-in S7 info script

- Snap7
  - Connect to PLC
  - Retrieve CPU info
  - Upload data block

Figure 1: Snap7 Commands
Discrepancies Nmap

Conpot
- **OS Detection:**
  Linux 2.6.32 (96%), Linux 3.2 - 4.9 (96%)...

- **S7 info:**
  _s7-info: ERROR: Script execution failed (use -d to debug)

- **FTP:**
  200 FTP server ready.
  Command 'GET' not understood

PLC
- **OS Detection:**
  BorderGuard 1000 firewall (93%)
  Xerox Document Centre 405 printer (92%)
  Motorola Canopy wireless bridge (92%)

- **S7 info:**
  Module: 6ES7 151-8AB00-0AB0
  Basic Hardware: 6ES7 151-8AB00-0AB0
  Version: 2.7.1
  System Name: ET200S
  Module Type: IM151-8 PN/DP CPU
  Serial Number: S C-B2VW09582011
  Copyright: Original Siemens Equipment
Discrepancies Snap7

Conpot
- Get connected: True
- Get CPU:
  ISO: An error occurred during recv
  TCP: Connection timed out
- Full upload(OB,1):
  ISO: An error occurred during recv
  TCP: Connection timed out

PLC
- Get connected: True
- Get CPU:
  info:<snap7.snap7types.S7CpuInfo
  object at 0x7f6d8292c040>
- Full upload(OB,1):
  (bytearray(b'pp\x01\x01\x02\x08\x00\x01\x00\x00\xba\x00...
Improving Default Configuration
Deployments

- Conpot 1
  - Default Conpot configuration
  - Multiple signatures
- Conpot 2
  - Modified Conpot Configuration
  - No common signatures
  - More closely resembles an actual PLC (network perspective)
- Conpot 3
  - S7Comm (Conpot implementation)
  - Closely resembles an actual Siemens PLC (network perspective)

<table>
<thead>
<tr>
<th></th>
<th>Conpot 1</th>
<th>Conpot 2</th>
<th>Conpot 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>(T)FTP</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HTTP</td>
<td>✓</td>
<td>✓</td>
<td>✓*</td>
</tr>
<tr>
<td>BACnet</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>MODBUS</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>CIP</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>S7Comm</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

Table 1: Conpot Deployments

* Modified
Deployment

Examples of common signatures not in Conpot 2

Technodrome

Status:

Current time: 09:12:25
System uptime: 39 timeticks (deciseconds)
Period 1

• 54 days
• Conpot 2 identified as ICS
• Shodan activity on:
  • Conpot 1: ftp & http
  • Conpot 2: http & CIP
  • Conpot 3: None

Period 2

• 47 days
• Conpot 1 & 2 identified as ICS
• Shodan activity on:
  • Conpot 1: ftp, http, CIP & BACnet
  • Conpot 2: http, CIP & BACnet
  • Conpot 3: None
**Results**

**Daily connections**

---

**1st Period**

**2nd Period**
Results

Protocol Connections per Deployment

1st Period

2nd Period
Results
IP Addresses only seen on one Honeypot

1st Period

2nd Period
Results

Total Connections for each Honeypot

1st Period

2nd Period
Results

• Overall Conpot 2 received the highest number of unique IP addresses* and the highest amount of returning IPs*

• During period 1, Conpot 2 received the most connections

• During period 2, Conpot 1 received the most connections
  • Conpot 2 received more connections on the common protocols than Conpot 1 during the second period (albeit slightly)

• Conpot 3 saw the most S7 connections during both periods, however these were limited (6 & 28) vs Conpot 1 (1 & 15) and Conpot 2 (4 & 14)

* Only seen on one honeypot
Conpot Deployments in the Wild
Conpot Deployments in the Wild

Search Engines
• Shodan
• Censys
• Zoomeye

Signatures
• PLC name: Technodrome
• Plant identification: Mouser Factory
• Serial number of module: 88111222
• Last-Modified: Tue, 19 May 1993 09:00:00 GMT (HTTP)
## Results

<table>
<thead>
<tr>
<th>Signature</th>
<th>Shodan</th>
<th>Censys</th>
<th>ZoomEye</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technodrome</td>
<td>319</td>
<td>385</td>
<td>4442</td>
</tr>
<tr>
<td>Mouser Factory</td>
<td>319</td>
<td>327</td>
<td>2951</td>
</tr>
<tr>
<td>‘88111222’ on port 102</td>
<td>336</td>
<td>348</td>
<td>1015</td>
</tr>
<tr>
<td>Tue, 19 May 1993 09:00:00 GMT</td>
<td>187</td>
<td>244</td>
<td>3442</td>
</tr>
</tbody>
</table>

Table 2: Results for Conpot Signatures
Results

Obfuscation Attempt

Central Pump

Status:
Current time: 08:38:24
System uptime: 18514 timer ticks (deciseconds)
Conclusion
Conpot shows many discrepancies when comparing to a real PLC
  • Especially when interacting with the device (Snap7/NMAP)

Conpot 2 received slightly more activity overall
  • More activity on industrial protocols (both periods)
  • More returning connections (both periods)
  • Improvement over the default deployment, but still major red flags when interacting with the deployment

Conpot 3 received the most S7 connections, however still a limited amount

There are a significant amount of default Conpot deployments on the Internet, which we expect knowledgeable attackers are able to identify
Questions?

Email: s.maesschalck@lancaster.ac.uk
Website: https://www.lancaster.ac.uk/scc/about-us/people/sam-maesschalck
LinkedIn: https://www.linkedin.com/in/sammaesschalck/