SCADA, the “old” and new environment

- **Standard protocol (at least in the field)**
  - ModBusTCP

- **Power Outage**

- **ModBusTCP is an open protocol**
  - Allen Bradley
  - TotalFlow
  - GE
  - Siemens
  - etc
Attack
Beware

- MetaSploit is about to add attack code for Siemens systems (recently exploits for GENESIS32 and BizViz software of developer ICONICS was added)

- Dillon Beresford has given MetaSploit the details

- He was about to make it public at the Takedown Conference but Siemens and the US CERT asked him not to yet. Siemens is working on a fix. He did present it partially at BlackHat
Beware

- Convergence of IT and SCADA Technologies resulted in Data Transport Requirements

- Leveraging Existing Networks as an “Easy” Solution

- And that’s the problem: has disclosed a laundry list of unpatched vulnerabilities and detailed proof-of-concept exploits that allow hackers to completely compromise major industrial control systems.
Beware

• A week ago the Italian security researcher, Luigi Auriemma, has disclosed a laundry list of unpatched vulnerabilities and detailed proof-of-concept exploits that allow hackers to completely compromise major industrial control systems.

• 50+ Step-by-step exploits that allowed attackers to execute full remote compromises and denial of service attacks.
Beware

- Multiple vulnerabilities in Cogent DataHub 7.1.1.63 (SCADA)
- Stack overflow in DAQFactory 5.85 build 1853 (SCADA)
- Multiple vulnerabilities in Progea Movicon / PowerHMI 11.2.1085 (SCADA)
- Directory traversal in Carel PlantVisor 2.4.4 (SCADA)
- Denial of Service in Rockwell RSLogix 19 (SCADA)
- Multiple vulnerabilities in Measuresoft ScadaPro 4.0.0 (SCADA)
- Denial of Service in Beckhoff TwinCAT 2.11.0.2004 (SCADA)
- Vulnerabilities in BroadWin WebAccess Client 1.0.0.10 (SCADA)
- Vulnerabilities in Siemens Tecnomatix FactoryLink 8.0.1.1473 (SCADA)
- Vulnerabilities in Iconics GENESIS32 9.21 and GENESIS64 10.51 (SCADA)
- Vulnerabilities in 7-Technologies IGSS 9.00.00.11059 (SCADA)
- Vulnerabilities in DATAC RealWin 2.1 (Build 6.1.10.10) (SCADA)
- Stack overflow in Winlog 2.07.00 (SCADA)
- Directory traversal in IntegraXor 3.6.4000.0 (SCADA)
- Wonderware InBatch 9.0sp1 (SCADA)
- Two buffer-overflow in DATAC RealWin 2.0 (Build 6.1.8.10) (SCADA)
Largest Malware Threat in SCADA Environment

1. Office
2. Contractors Maintenance
3. PLC Engineer Maintenance
4. USB
5. MES
6. SCADA

PLC

MES

SCADA

Contractors Maintenance

PLC Engineer Maintenance
Device Control
Device Control
Device Control
Device Control

ALZHEIMER'S Erasers

YOUR MEMORIES. SAVE THEM.
Device Control
Device Control
Device Control
Device Control

And more...
Device Control
Device Control

GIZMODO

ART

Why Is There a USB Drive Sticking Out of This Wall?

Across New York, there are USB drives embedded in walls, buildings and curbs. The idea is to create an anonymous, offline file-sharing network in public space. The drives are completely public and anyone can plug in to drop and download files.

Seriously, you can plug the USB drive into your laptop. Like that guy right there.

It’s part of an art project called "Dead Drops" by Aram Bartholl and I have to say, it’s pretty awesomely creative. I mean, if I saw a USB stick stick out of a random wall, I’d be dying to know what’s in there. I’d have to plug in. It’d also be interesting to see what people would anonymously share on the public drive, well, until some jackass decides to upload a virus to screw up everybody’s computer. [Dead Drops via MAKE]

Device Control

• “foreign” media
Defense
After Stuxnet

• What did Stuxnet shows us
  – Pro-active security is essential ➔ anticipate ➔ inline security (scan the network cable)
Most used spreading protocols

Malware spread vector: widely used ports

CIFS/SMB
RPC
Why are CIFS and SMB important?

Malware spread vector: widely used ports

- CIFS/SMB
- RPC
In-Line Network Content Scanner

Network transparent real-time scanner

Scan protocols as HTTP, FTP, SMTP, TFTP, RPC, POP3, IRC, SMB(2)/CIFS
Block the spread by scanning

SCADA Environment

STOP
Where to install?

STOP

Legacy Networks?
After Stuxnet

• What did Stuxnet shows us
  – Pro-active security is essential $\rightarrow$ anticipate $\rightarrow$ inline security (scan the network cable)
  – Disable/block any “port or service” not required
  – But also: create Clearly Defines Trustzones
  – And make sure the standards are consistent between SCADA and IT
  – Mandate Patch Management Requirements
  – Make sure you know what is executed on your network
Application Control

• Makes sure the applications used are legitimate
• Avoids foul applications to be executed
• Keeps control of your applications authorization
Unauthorized Applications & Unknown Threats

Applications
- Authorized
  - Operating Systems
  - Business Software
- Unauthorized
  - Games
  - iTunes
  - Shareware
  - Unlicensed S/W

Malware
- Known
  - Viruses
  - Worms
  - Trojans
- Unknown
  - Viruses
  - Worms
  - Trojans
  - Keyloggers
  - Spyware
Application Whitelisting

- Authorized
  - Operating Systems
  - Business Software

- Unauthorized
  - Games
  - iTunes
  - Shareware
  - Unlicensed S/W

- Unknown
  - Viruses
  - Worms
  - Trojans
  - Keyloggers
  - Spyware

- Known
  - Viruses
  - Worms
  - Trojans
How It Should Work

Individual User

Groups of Users

• Accounting
• Sales People
• Network Admins
• Support Team

Users can now only run the executables they are allowed to

0. IDENTIFY .EXE SOURCES

1. COLLECT

• Scan Explorer
• Log Explorer
• EXE Explorer

3. ASSIGN RIGHTS TO EXECUTE

Organize into File Groups

- Admin Tools
- Entertainment
- Communication
- MS Office
- etc...

Operating Systems

Standard Software

Corporate specific applications
As all of our industries become more connected, a simple malware infection can result in a major disruption of production, services or something worse.

ACTION REQUIRED IMMEDIATELY
Let me check...
Questions and Answers

Righard J. Zwienenberg
Chief Research Officer
Righard.Zwienenberg@norman.com

Norman Data Defense Systems (UK) Ltd
CBXII, West Wing
382-390 Midsummer Boulevard
Central Milton Keynes
MK9 2RG
Tel: 01908 847413
Fax: 0870 1202901