Embedded and IOT Security

Industry perspective

OCTOBER 2017

parsec

technology partner • infinite possibilities

A SUBSIDIARY OF ansys LIMITED | 30 YEARS of innovation

INTERNET OF THINGS

ALWAYS ON

CONNECTED TO THE INTERNET

EXAMPLES

Consumer

- Consumer electronics
  - Mobile devices (phones etc)
  - Fridges
  - Toasters
  - Baby monitors
- Home automation devices
- Fitness sensors
- Home routers
- Home PCs

Industrial

- Sensors
- Process Control systems
- Building management
- Traffic lights
- Smart grid
- Smart city
- Connected cars
- Internet Protocol (IP) cameras

According to "BI Intelligence" more than 24 billion IoT devices will be installed globally in 2020, and the vast majority of these will fall into the small, low-power category.

But millions of devices are directly connected to the Internet TODAY

They are nicely catalogued for us:

https://www.shodan.io

Cameras

TOTAL RESULTS

232,811

TOP COUNTRIES

United States	27,460
Germany	26,669
Iran, Islamic Republic of	18,017
China	17,628
France	16,002

Routers

TOTAL RESULTS

1,804,351

TOP COUNTRIES

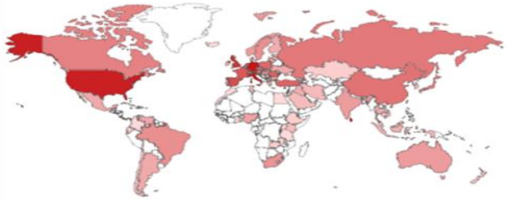
Brazil	506,465
United States	205,046
China	143,953
Russian Federation	79,535
Taiwan	69,239

PLC

TOTAL RESULTS

3,409

TOP COUNTRIES



Sri Lanka	489
Germany	440
Italy	408
United States	368
United Kingdom	251

https://www.shodan.io

WHY IS THIS A PROBLEM ?

MIRAI BOTNET

- Disrupted major portions of the Internet
- Large DDOS attack that overwhelmed DYN, a DNS service provider.
- Mostly launched from IP Cameras and Digital Video Recorders
- IOT used to attack

GETTY IMAGES

STUXNET

- Reported to be of Israeli/US origin
- Targeting Siemens PLCs
- Ultimately destroyed a fifth of Iran's nuclear centrifuges

HAVEX TROJAN

- Iranian origin
- Specifically aimed at Energy providers in Europe
- "Spear Phishing" attack
- Caused widespread damage at German Steel Plant
  - Operator stations became unresponsive
  - PLCs could not be controlled
  - Could not shutdown or control furnace

AURORA

- Staged attack demonstrating potential damage to power grid
- Severe generator damage (by opening and closing circuits of generator out of phase)

DAMAGE IS DIRECT AND INDIRECT

Even if the affected process or organization is not the intended target, the nature of a virus or trojan is such that its outbreak is generally uncontrolled and various **unrelated entities can suffer damages** because of it.

WHAT IS YOUR LIABILITY

- **If your process controller is hacked and there is a loss of life**
  - ✓ Who is liable ?
  - ✓ What is the exposure

- **If your customer data is leaked**
  - ✓ What is the reputational damage
  - ✓ What is the loss of revenue – indirect and direct

- **What if your plant has to shut down for a few months ?**

WHAT CAN WE DO ABOUT IT ?

parsec
technology partner • infinite possibilities

DESIGN SECURITY IN FROM THE START

WHAT CAN BE DONE FOR EXISTING DEPLOYMENTS

- **Accounts can be protected with Unique passwords**

✓ Password Managers– there is no excuse for default device passwords

- **Multi-factor authentication is getting simpler and cheaper**
- **Devices do not always have to be directly connected to the Internet**
  - ✓ New generation firewalls provide multiple segments
  - ✓ Understand industrial protocols and allow whitelisting
- **New generation VPNs**
  - ✓ Easy to deploy
  - ✓ Provide strong security, even over wireless links
- **AI being used for threat detection**

NEW DEPLOYMENTS: LIGHT AT THE END OF THE TUNNEL

- **More secure networks**
  - ✓ More Security built into some networks
  - ✓ RPMA is a good example
- **Device security improvements**

✓ Trusted Processor Modules

✓ Inexpensive crypto chips for IOT

✓ Trusted OS and boot environments

parsec
technology partner • infinite possibilities

SUMMARY AND RECOMMENDATIONS

- **Do a security audit that includes**
  - ✓ Industrial Control Systems
  - ✓ Partner network access
  - ✓ Maintenance network access
  - ✓ Wireless links
- **Isolate your ICS from the internet**
  - ✓ Using an airgap if possible
  - ✓ Using multiple firewalls if not possible
- **Educate your users**
  - ✓ How to spot a spear phishing attack
- **Be prepared**
  - ✓ It’s not a questions of IF but WHEN…

Don’t be a victim

Buy the best security tools you can afford

Use the tools you have

Be prepared for a disaster

The bad guys are rattling the fence.

parsec
technology partner • infinite possibilities

Thank you

A SUBSIDIARY OF ansys LIMITED | 30 YEARS of innovation