#RSAC

RSAConference2017

San Francisco | February 13 – 17 | Moscone Center

POWER OF OPPORTUNITY

SESSION ID: SEM-M03

Out of Control: Ransomware in Industrial Control Systems

David Formby

PhD Candidate, Georgia Institute of Technology
www.ece.gatech.edu/cap

CEO/CTO, Fortiphyd Logic
www.fortiphyd.com

Putting on the Black Hat

- Most malware authors and attackers are in it for the money
- Ransomware is the hot new business model
  - $209 Million profit in Q1 2016 Source: CNN, “Cyber-extortion losses skyrocket, says FBI”
- High profile ransomware attacks
  - San Francisco’s light rail system
  - Hospitals
- Where might an enterprising young hacker attack next?

RSA Conference2017

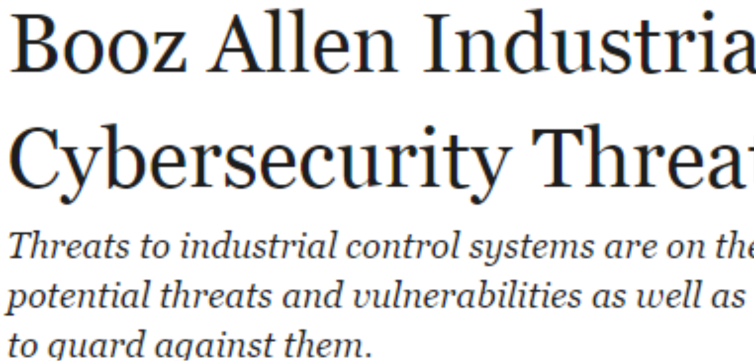
Market Research

Brief History of Ransomware

- Locker Ransomware
  - Renew software license
  - Fake AV
  - FBI threats
  - Awareness and security tools decreased effectiveness
- Crypto Ransomware
  - No false pretense, clear extortion
  - No easy recovery

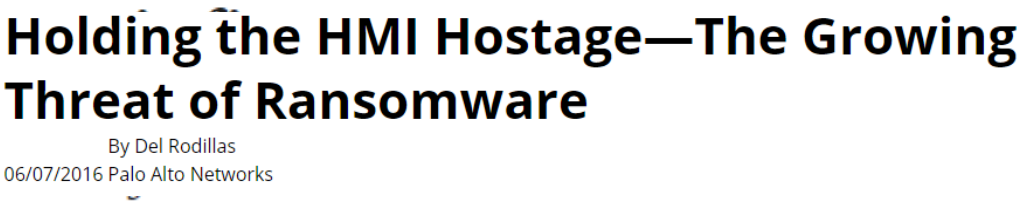
Symantec Whitepaper “The Evolution of Ransomware”

Brief History of Ransomware



Booz Allen Industrial Cybersecurity Threa

Threats to industrial control systems are on th potential threats and vulnerabilities as well as to guard against them.

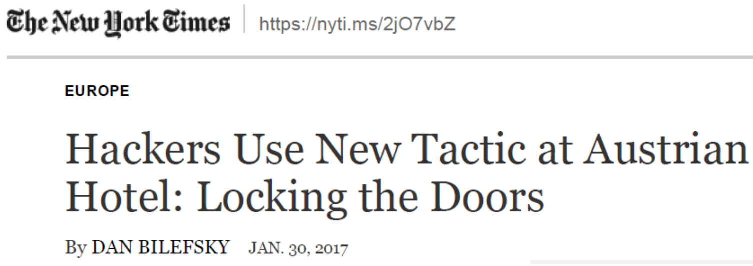


Holding the HMI Hostage—The Growing Threat of Ransomware

By Del Rodillas

06/07/2016 Palo Alto Networks

Move over Healthcare, Ransomware Has Manufacturing In Its Sights

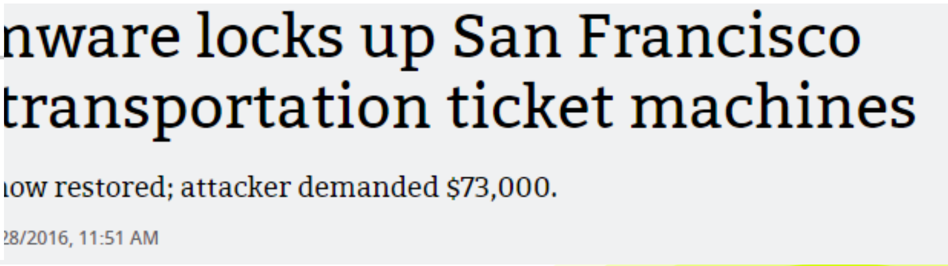


The New York Times | https://nyti.ms/2jO7vbZ

EUROPE

Hackers Use New Tactic at Austrian Hotel: Locking the Doors

By DAN BILEFSKY JAN. 30, 2017

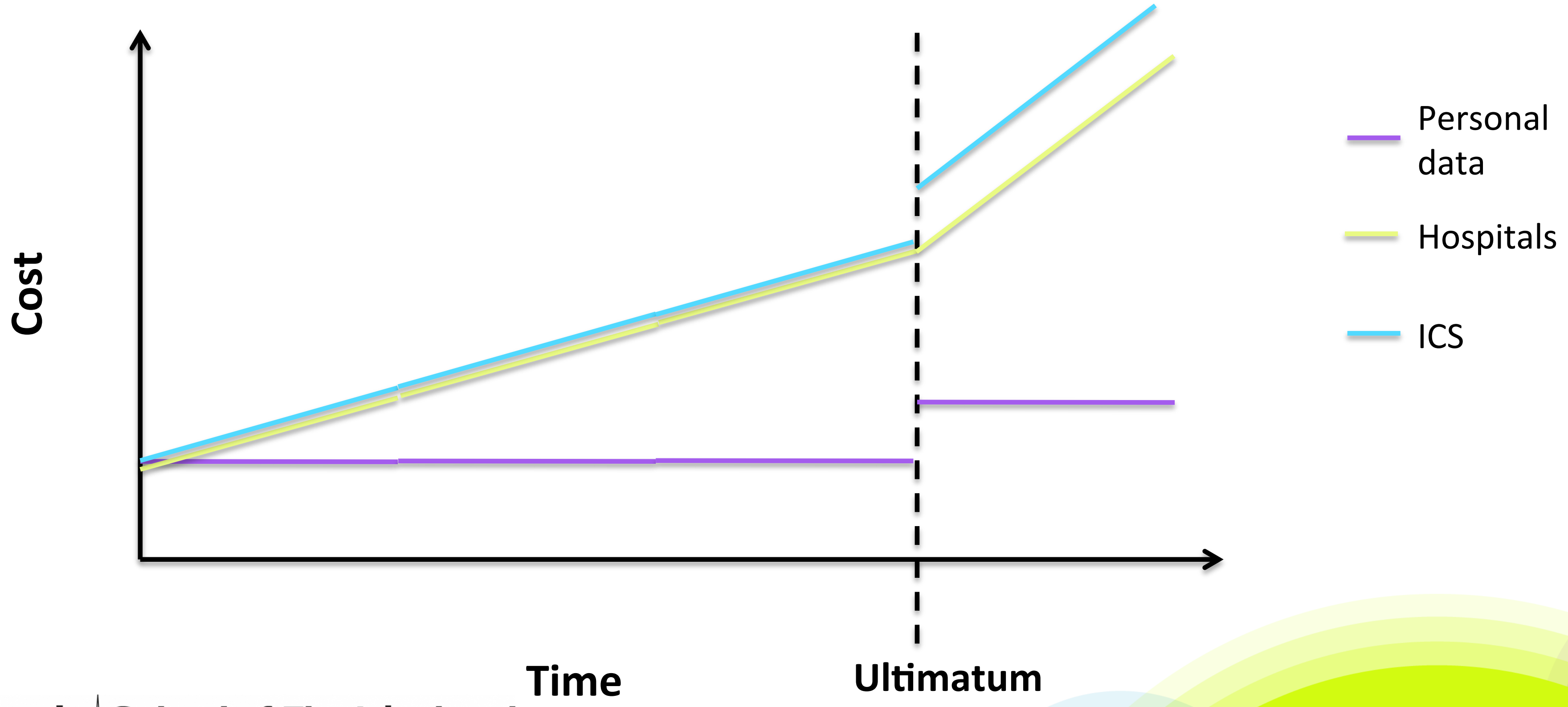


nware locks up San Francisco transportation ticket machines

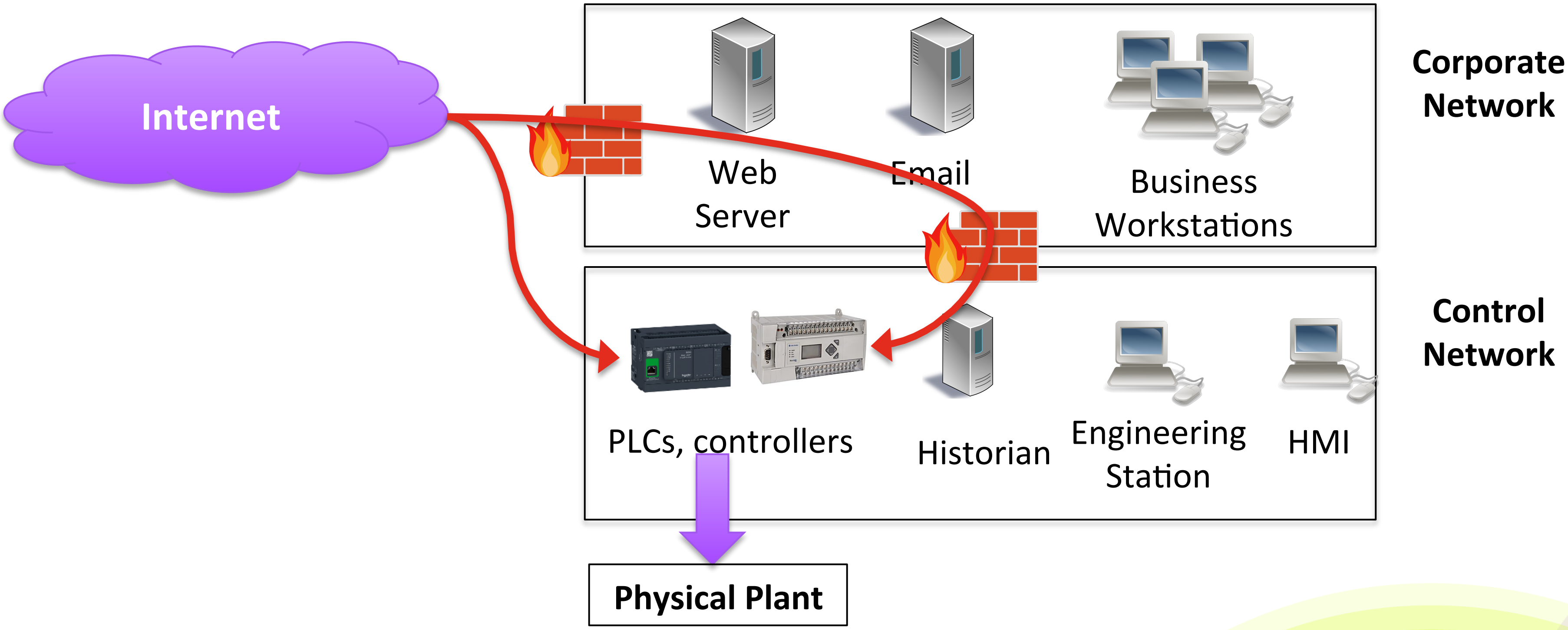
iow restored; attacker demanded $73,000.

28/2016, 11:51 AM

The Ransomware Races

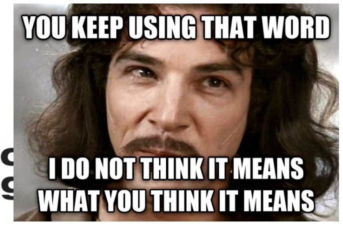


Overview of Industrial Control Systems



ICS Security

- Most protocols have no message authentication
  - Accept any command injected on the network
- Most PLC programming interfaces lack solid password authentication
  - Nonexistent
  - Misleading
  - Poor protection against brute forcing
- Rely on fallacies
  - Security through obscurity
  - “Airgaps”



What Makes a Ransomware Attack Successful?

Hospitals

- Easier targets
  - Old equipment
  - Traditionally weak security posture
- Increasing time pressure
- Lives at stake
- Crown jewels = patient data

ICS Networks

- Easier targets
  - Old equipment
  - Traditionally weak security posture
- Increasing time pressure
- Lives at stake
- Crown jewels = safe operation

Market Size Analysis

Businesses Hit by Ransomware

- 70% paid the ransom
- Median payout approx. $10k
- Small, medium sized businesses less prepared

Source: IBM, “Ransomware: How consumers and businesses value their data”

PLCs on the Internet

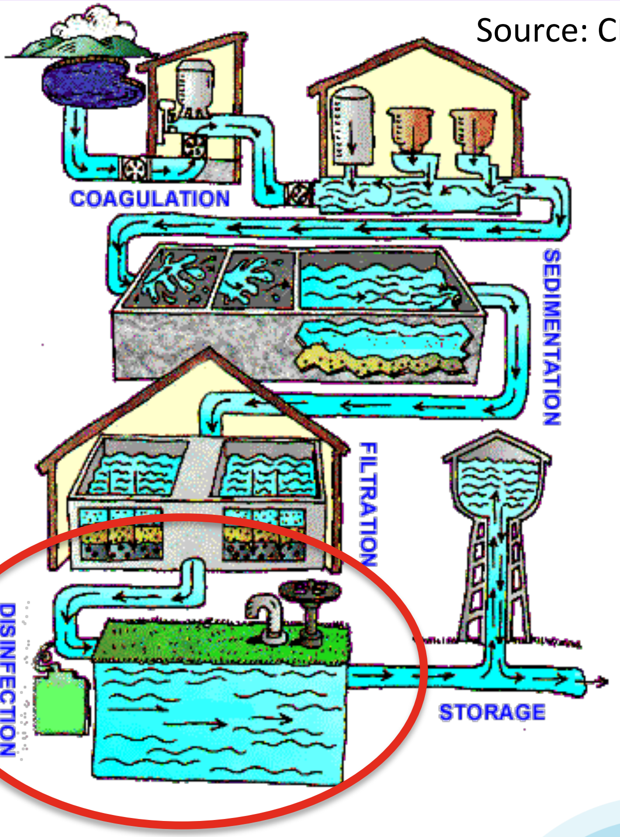
- MicroLogix 1400
  - 1,300
- Schneider Modicon M221
  - 200

1,500	**X**	**$10,000**	**X**	**50%**	**=**	**$7.5 Million**
Trivial PLCs		Expected payout		Conservative success rate		

RSAConference2017

Attack

Water Treatment Facility



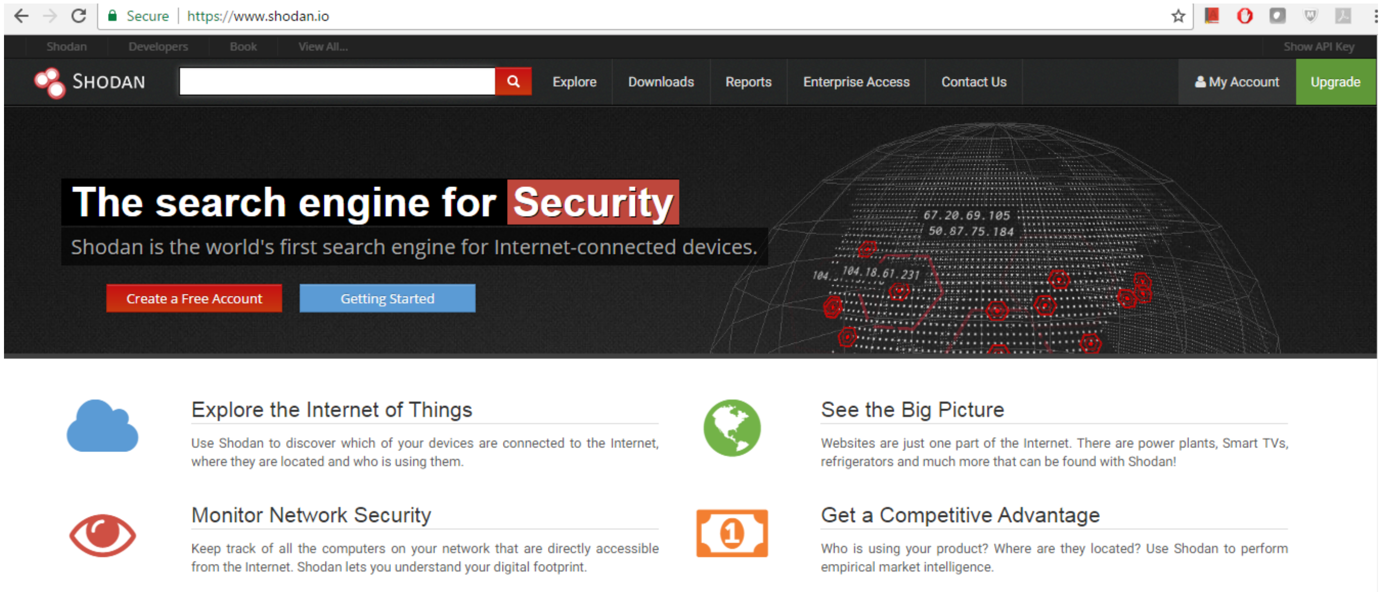
Source: CDC, “Water Treatment”

Testbed simulates the Disinfection and Storage stages

Typically mixed with chlorine to kill bacteria

We use iodine because it’s safer to handle and cooler looking

Recon



The search engine for Security

Shodan is the world's first search engine for Internet-connected devices.

Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

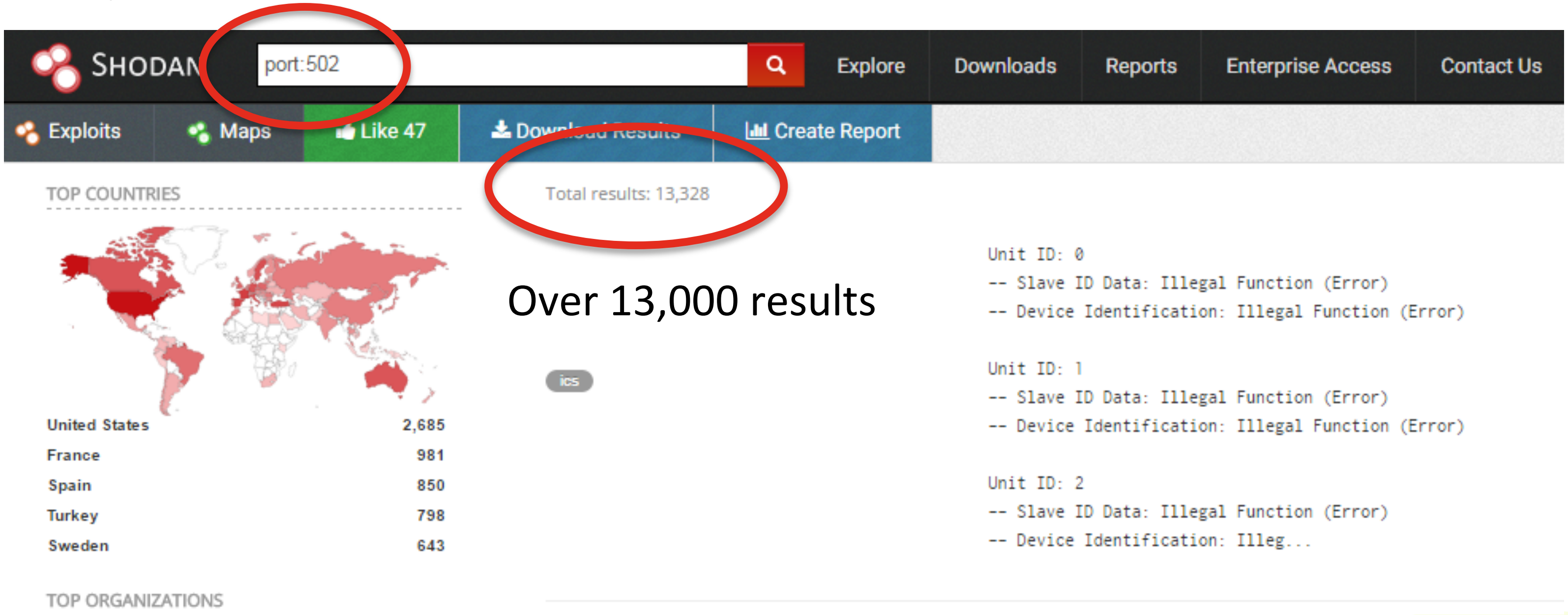
Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

Search engine for connected ICS devices

Recon

Common protocol, Modbus



TOP COUNTRIES

Total results: 13,328

Over 13,000 results

United States	2,685
France	981
Spain	850
Turkey	798
Sweden	643

TOP ORGANIZATIONS

```
Unit ID: 0
-- Slave ID Data: Illegal Function (Error)
-- Device Identification: Illegal Function (Error)

Unit ID: 1
-- Slave ID Data: Illegal Function (Error)
-- Device Identification: Illegal Function (Error)

Unit ID: 2
-- Slave ID Data: Illegal Function (Error)
-- Device Identification: Illeg...
```

Plenty of choices to choose from, just pick one

Initial Foothold

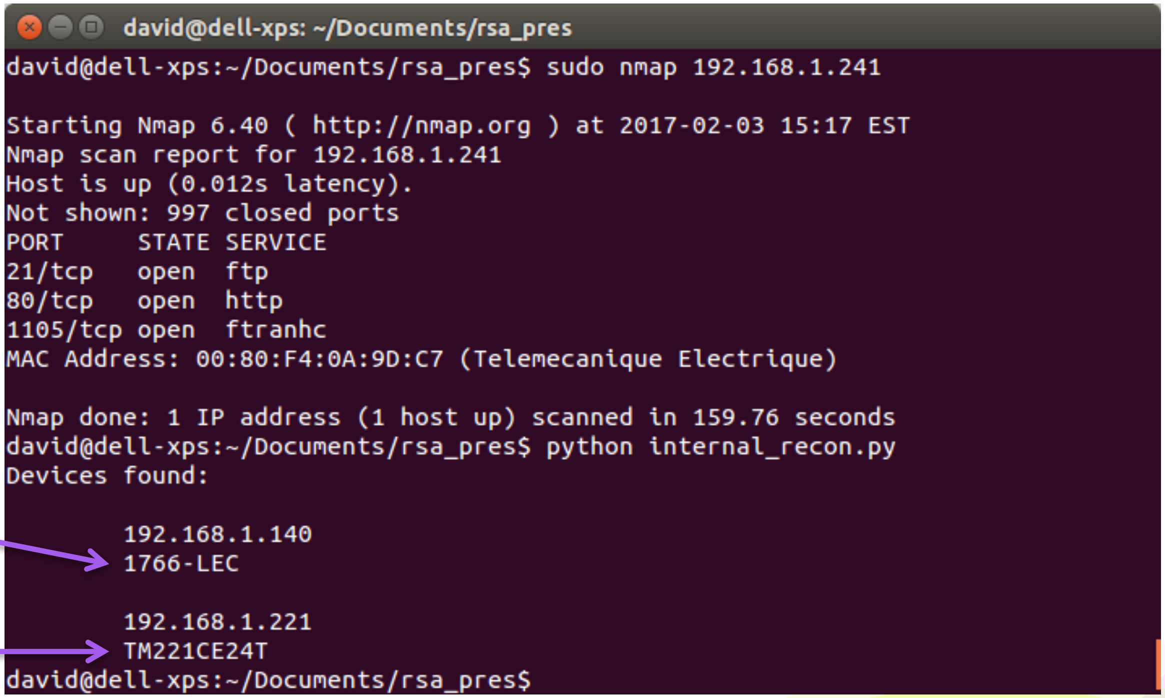
- Schneider Modicon M241
  - Running CODESYS V3
  - Third party PLC runtime environment used by over 200 vendors
  - Password
    - No brute force checks
    - No strength policy
  - Controlling the water input and monitoring the storage levels

Internal Network Scan

Reprogram the M241 to scan the internal network and grab model numbers

Allen Bradley
MicroLogix 1400

Modicon M221



```
david@dell-xps:~/Documents/rsa_pres$ sudo nmap 192.168.1.241

Starting Nmap 6.40 ( http://nmap.org ) at 2017-02-03 15:17 EST
Nmap scan report for 192.168.1.241
Host is up (0.012s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
1105/tcp open  ftranhc
MAC Address: 00:80:F4:0A:9D:C7 (Telemecanique Electrique)

Nmap done: 1 IP address (1 host up) scanned in 159.76 seconds
david@dell-xps:~/Documents/rsa_pres$ python internal_recon.py
Devices found:

        192.168.1.140
        1766-LEC

        192.168.1.221
        TM221CE24T
david@dell-xps:~/Documents/rsa_pres$
```

Internal Network Scan

Allen Bradley MicroLogix 1400

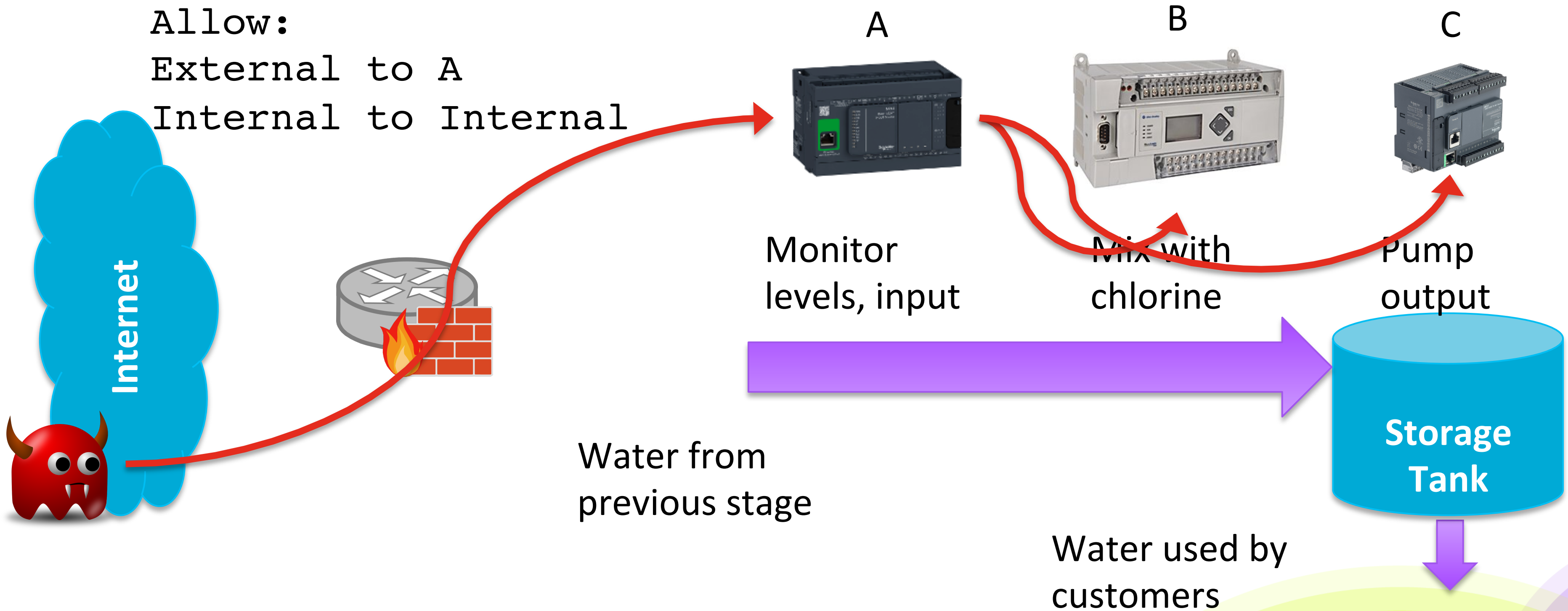
- Password only checked in engineering software, **NOT** the PLC
- SMTP mail client
- Controlling the addition of chlorine (ioc

Schneider Modicon M221

- Password only checked in engineering software, **NOT** the PLC
- Controlling the final output of treated water

Actual Network

```
Allow:
External to A
Internal to Internal
```



Monitor levels, input

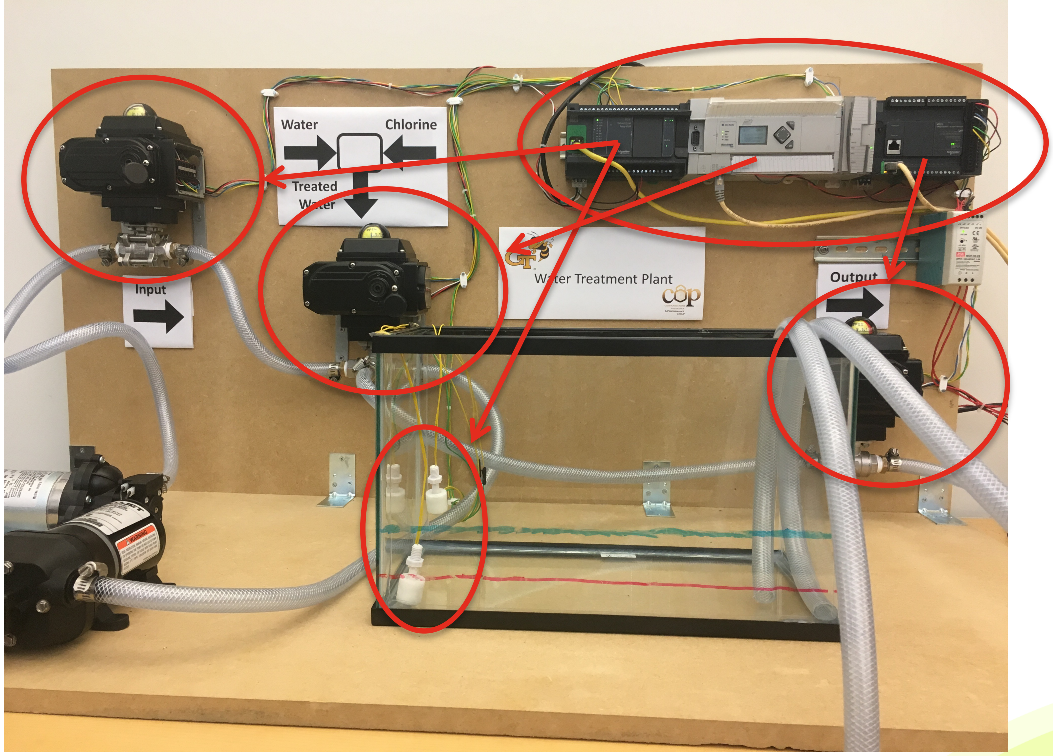
Mix with chlorine

Pump output

Water from previous stage

Water used by customers

Actual Network



Input water valve

Mixing valve to control ratio of water/ iodine

Level sensors

Programmable logic controllers

Output water valve

How Can We Maximize Success Rate

- Pick targets with high downtime costs
- Understand the process behind the PLCs
- Threaten to screw things up if they don’t meet deadline
  - What if they just unplug everything?
- Covertly move system into critical state **before** notifying them
  - Allow reserve storage tank to get low first, blinding operators
  - Make continued operation by attacker more attractive than shutting everything down

Water Treatment Testbed

https://youtu.be/KTKRjvTgTQI

Attack

https://youtu.be/t4u3nJDXwes

Discussion

Apply: Lessons Learned

- ICS networks and devices are STILL very vulnerable
  - Poor/nonexistent password protection
  - Vendors slow to fix obvious problems
  - A lot of exposed devices on the Internet
- Ransomware trend is likely to jump to ICS
  - Early signs attacking corporate networks of ICS
  - Easy targets
  - Money and lives at stake

Apply: Defenses

- Know your network
  - Devices, remote vendor connections
- Security assessment
  - Firewall rules, segmented network, proper remote access
  - Passwords
- Monitor at the ICS level
  - Communication patterns
  - PLC programming events
- Pressure vendors to build more security into their products

Thank You!

David Formby

www.cap.gatech.edu
djformby@gatech.edu
@gtcapgroup @davidjf12

Fortiphyd Logic

www.fortiphyd.com
info@fortiphyd.com
@fortiphyd