Who's Really Attacking Your ICS Devices?

Kyle Wilhoit
Threat Researcher, Trend Micro

#WHOAMI

- Threat Researcher at Trend Micro- research and blogger on criminal underground, persistent threats, and vulnerabilities.

- Research Interests:

  -Malware detection/reversing

  -Persistent Threats

  -ICS/SCADA Security

  -Vulnerabilities and the "Underground"

Agenda

- Overview of two SCADA protocols
- Story Time!
- Typical ICS Deployments
- ICS/SCADA IT Differences
- SCADA Systems Facing the Internet
- SCADA Systems Are Always Attacked, Right?
- Enter…The Honeypots…
- Findings
- Attacker Profile
- Recommendations

This presentation will focus on:

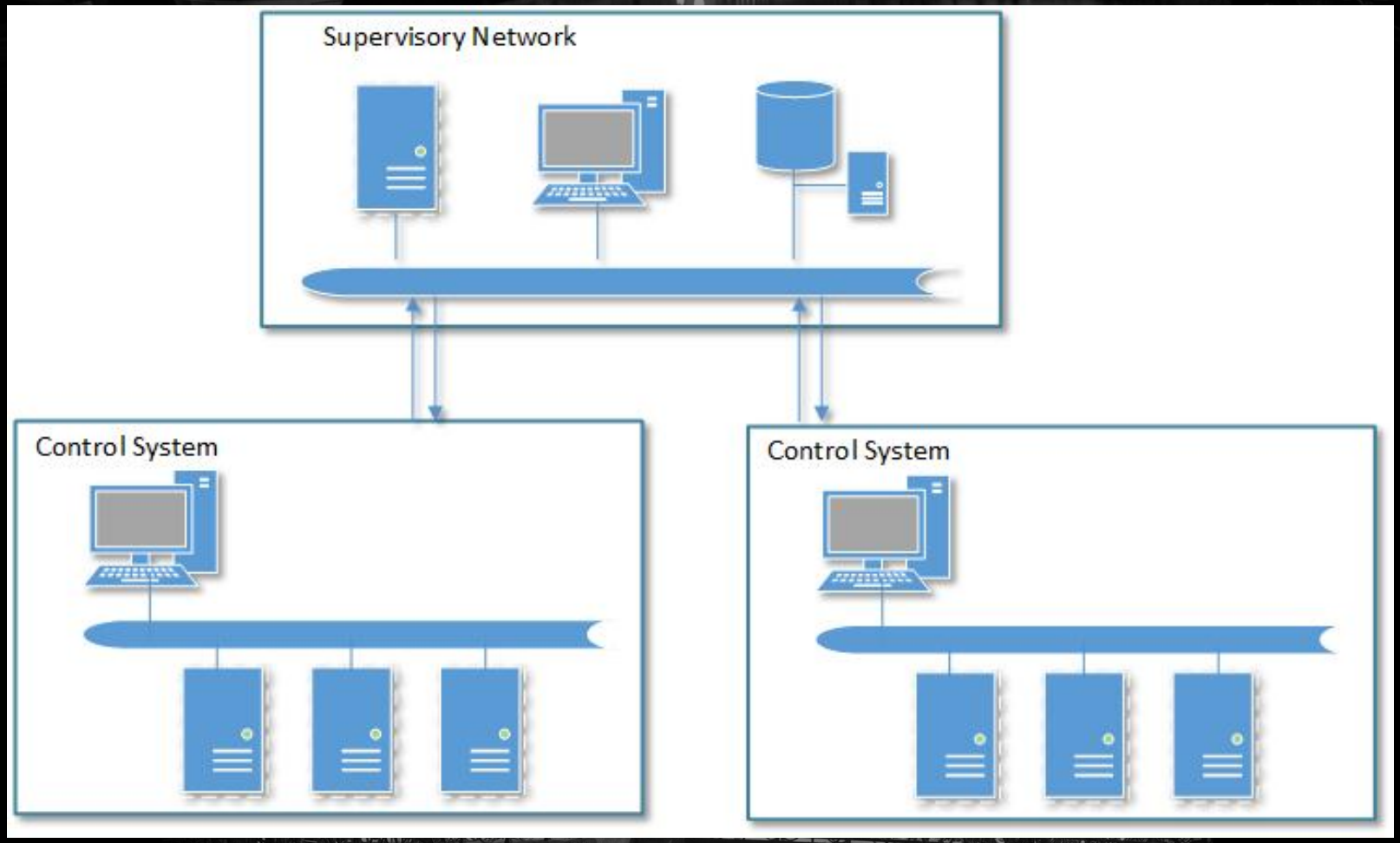
- Concerns/Overview of ICS Security
- How heinous the security profiles are ICS devices
- Are ICS devices attacked?
- Who attacks ICS devices?

ICS Overview

What are ICS devices?

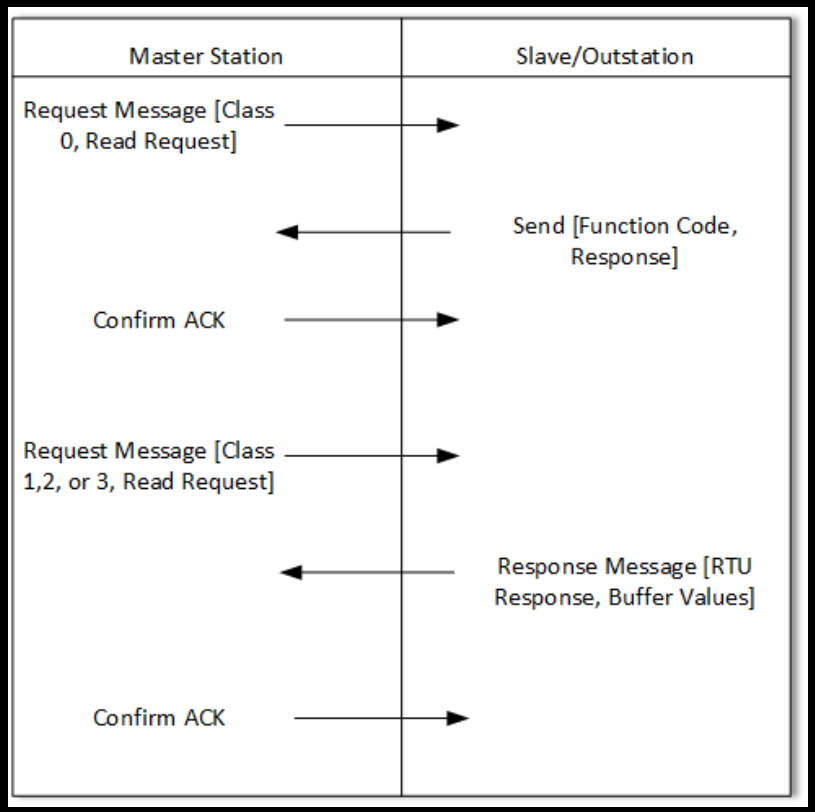
- Used in production of virtually anything
- Used in water, gas, energy, etc. etc. etc.
- Notoriously insecure…in every way
- Software is sometimes embedded, sometimes not
- Typically proprietary

TYPICAL ICS



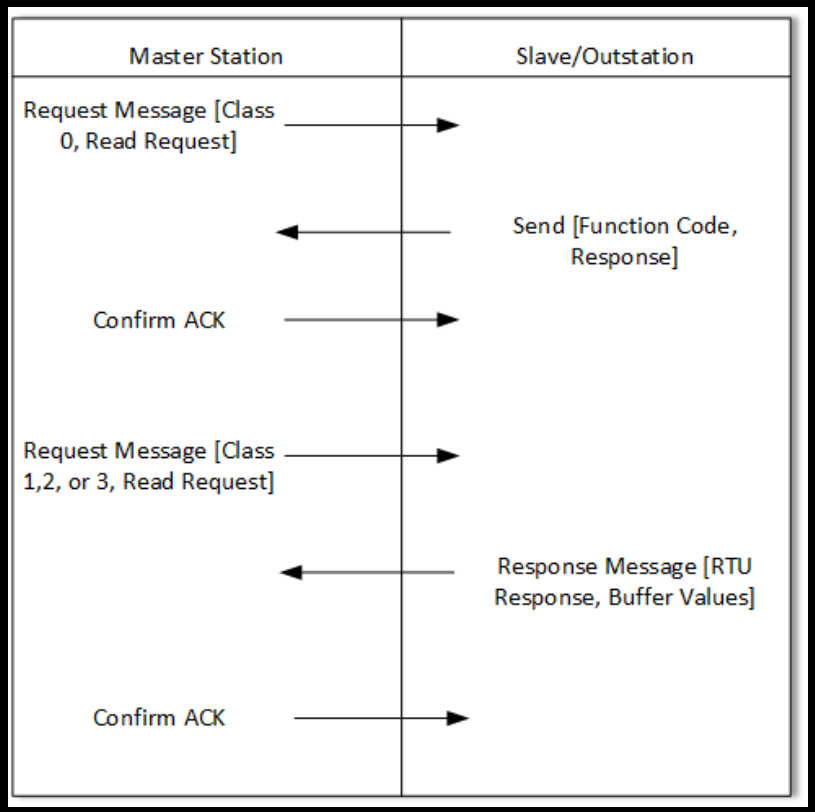
DNP3

- DNP3
  - Used to send and receive messages
  - Complex
  - No authentication or encryption
  - Several published vulnerabilities



Modbus

- Oldest ICS Protocol
- Controls I/O Interfaces (MOSTLY!!!!)
- No authentication or encrytion! (Surprise!!!)
- No broadcast suppression



ICS vs. Traditional IT Systems

- ICS
  - Productivity
  - Up-time
  - Reliability of data
- IT
  - Protect the data
  - Continued productivity
  - Limit interruptions

ICS Vulnerabilities

- In 2012, 171 unique vulnerabilities affecting ICS products.
  - 55 Vendors…

How many have you heard about?

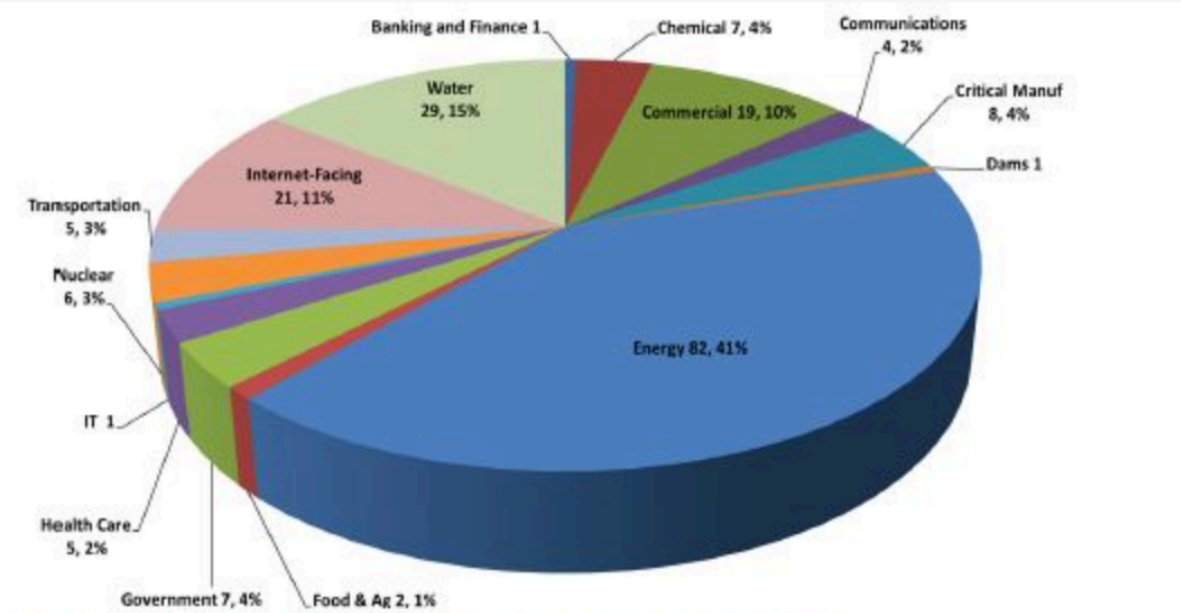
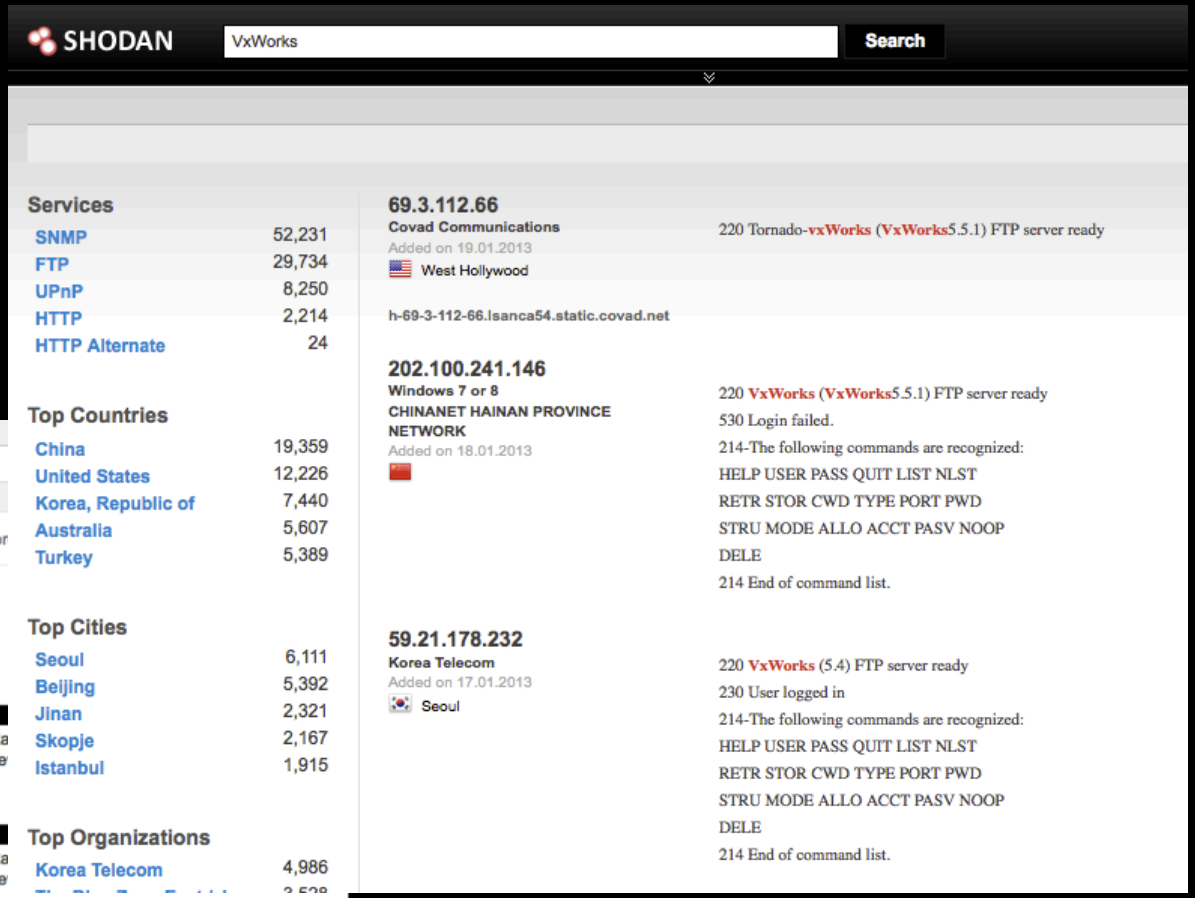
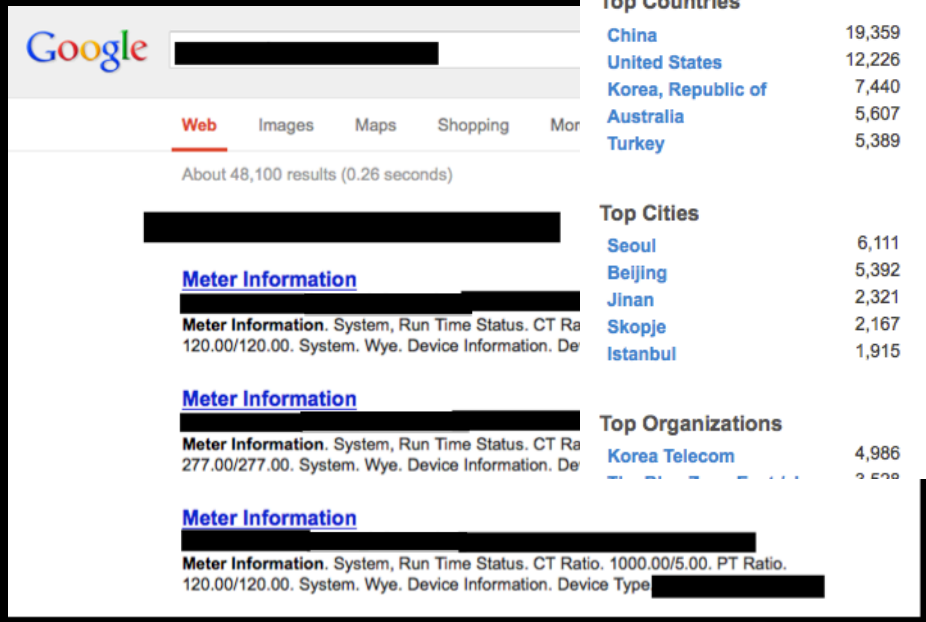


Figure 4. Incidents by Sector – Fiscal Year 2012

SCADA on the Internet???

- Google-fu
- Shodan
- Pastebin

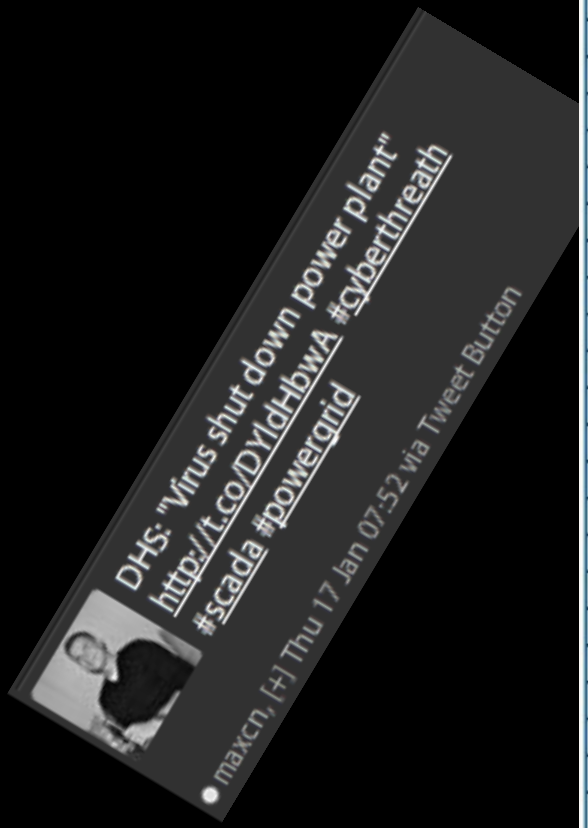




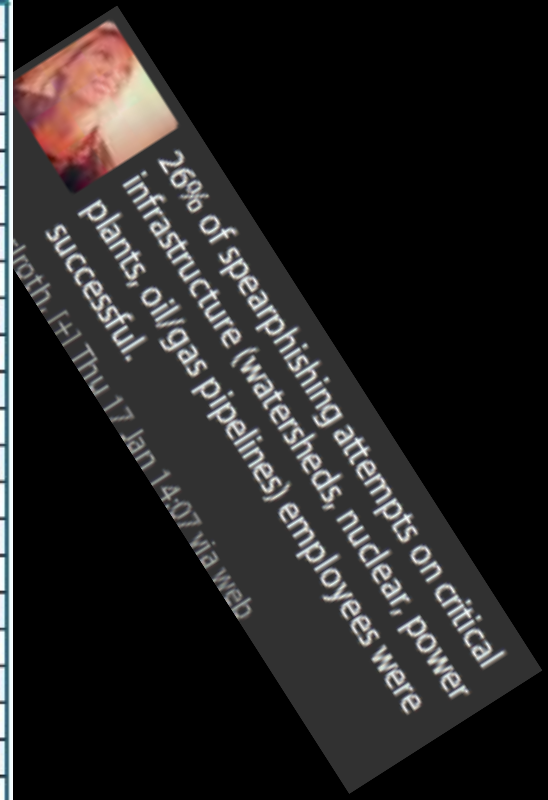
SCADA on the Internet???

- Google-fu
- Shodan
- Pastebin

SCADA is Never Attacked, Right?



Vulnerability Type	
Buffer Overflow	44
Input Validation	13
Resource Exhaustion	8
Authentication	8
Cross-site Scripting	8
Path Traversal	8
Resource Management	8
Access Control	7
Hard-coded Password	7
DLL Hijacking	6
SQL Injection	4
Credentials Management	3
Cryptographic Issues	3
Insufficient Entropy	3
Use After Free	3
Use of Hard-coded Credentials	2
Cross-Site Request Forgery	2
Privilege Management	2
Write-what-where Condition	2
Integer Overflow or Wraparound	2
Inadequate Encryption Strength	2
Missing Encryption of Sensitive Data	1
Code Injection	1
Forced Browsing	1
Miscellaneous	15
Total	171



Anonymous @YourAnonNews 30m

Nice list of #SCADA dorks from @scadastrangelov ICS/SCADA/PLC Google/Shodanhq Cheat Sheet on his log scadastrangelove.blogspot.nl/2012/12/icssca… (via @ntisec) #YA

Story Time!

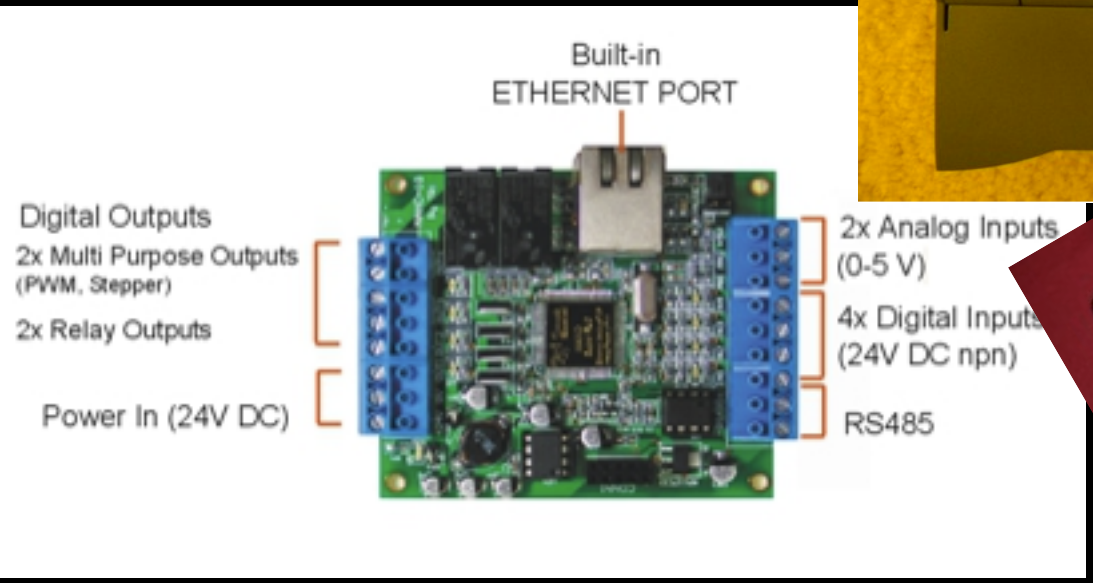
- Small town in rural America
- Water pump controlling water pressure/ availability
- Population 8,000~

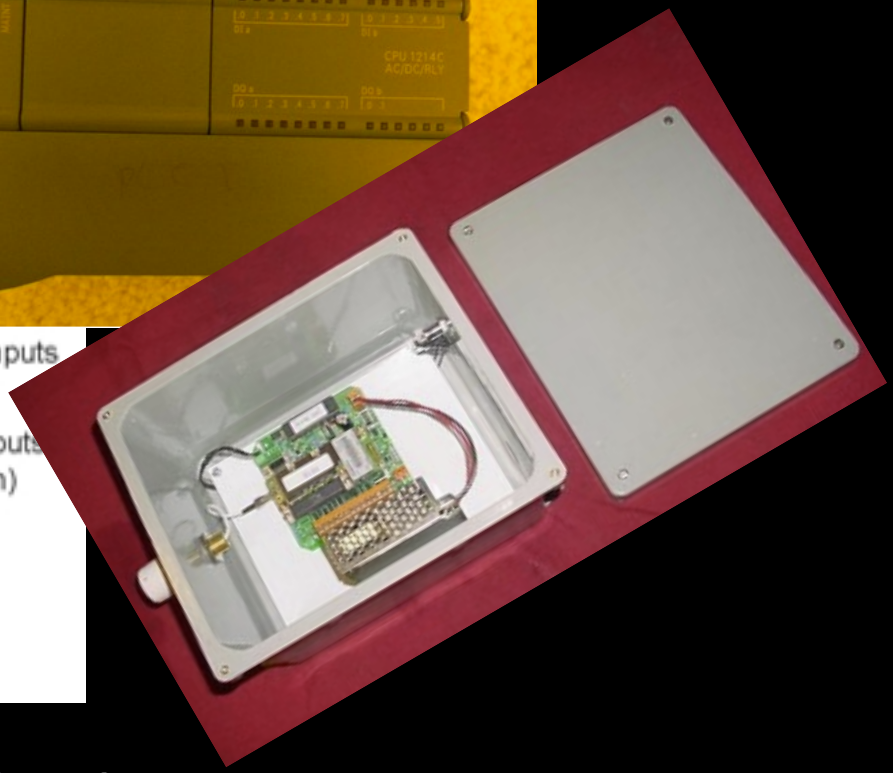
Story Time!

- Water Pressure System Internet Facing :/
- No firewalls/security measures in place
- **Attacked several times…Nov 14th through Dec 19th**
- Could have caused catastrophic water pressure failures.
- This is not a story…
- Real life event..
- **This Happened.**

Story Time!

IN MY BASEMENT.





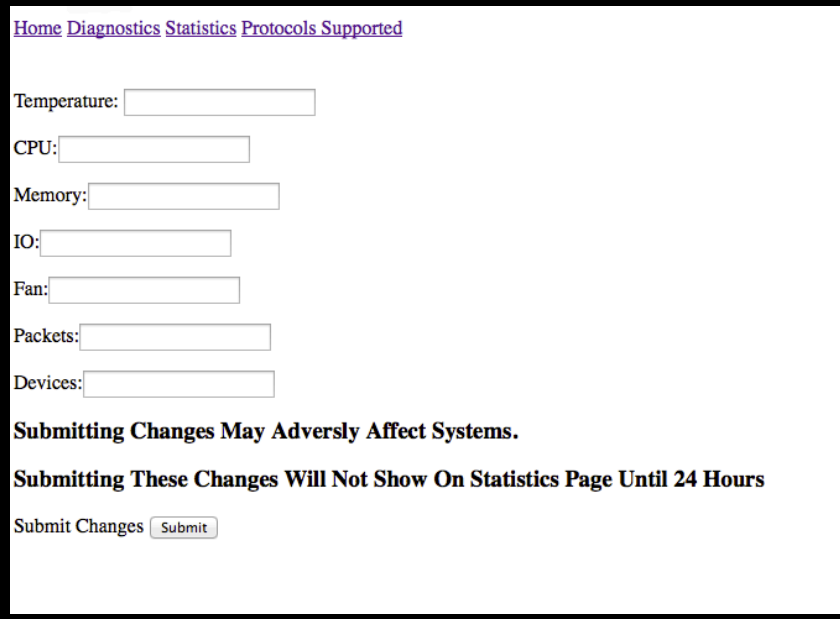
Enter…Honeypots…

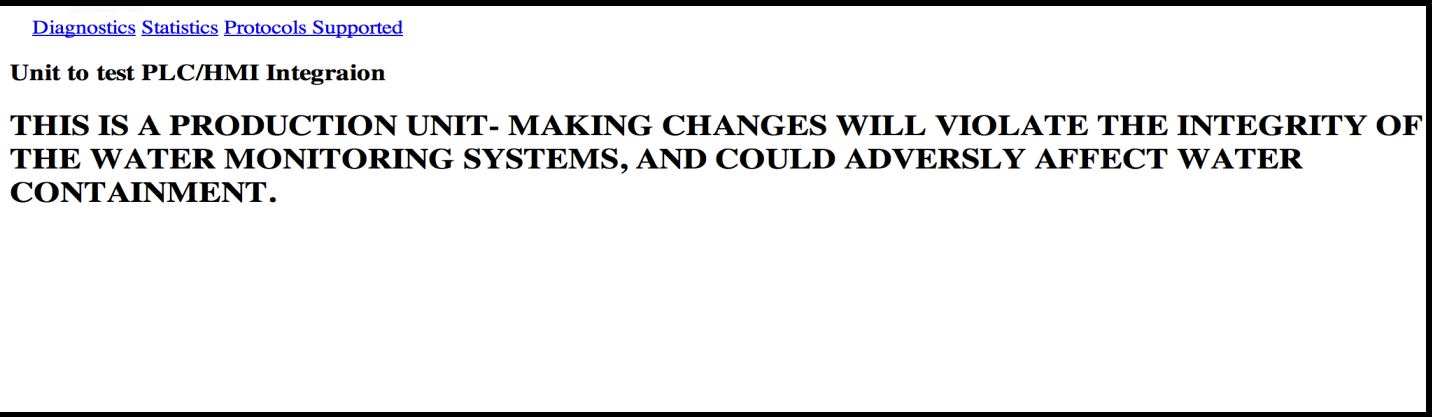
HONEY

Not always the best diet

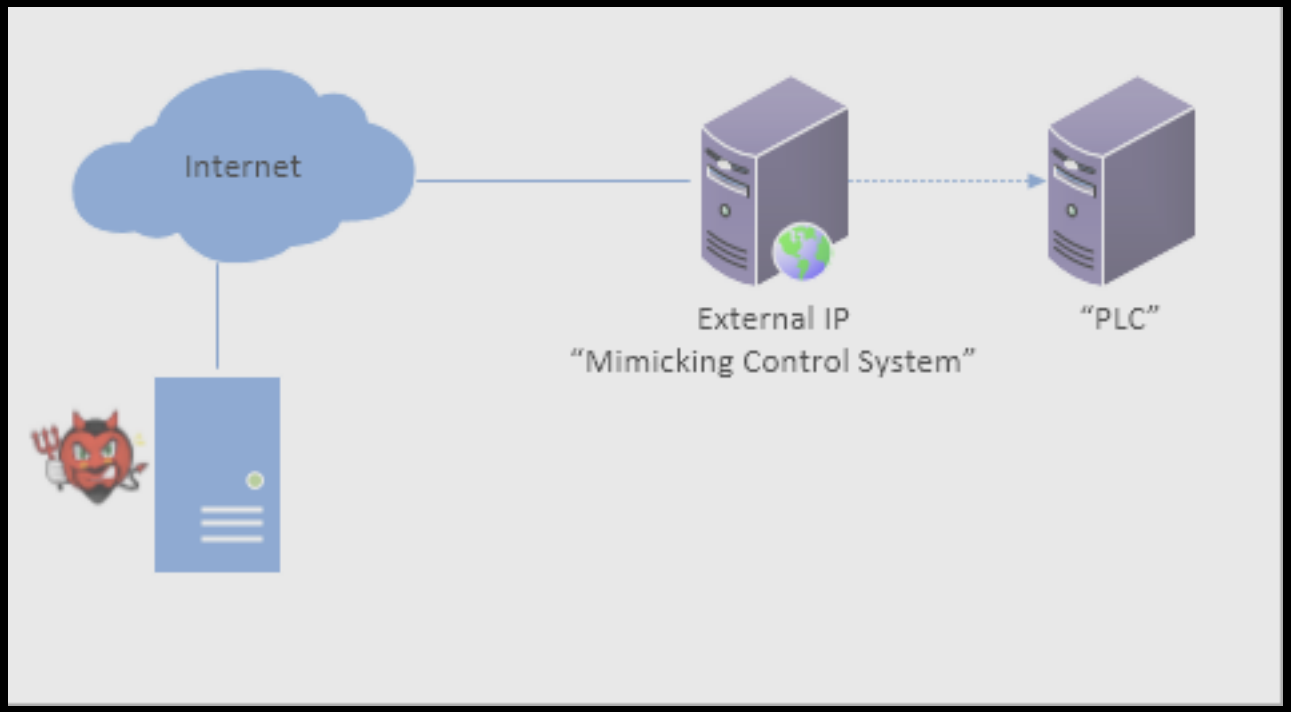
Honeypot Overview

- Two low-interaction
- One high-interaction
- Ran for 28 days in total
- One Windows Server 08
- Two Ubuntu 12.04 Servers

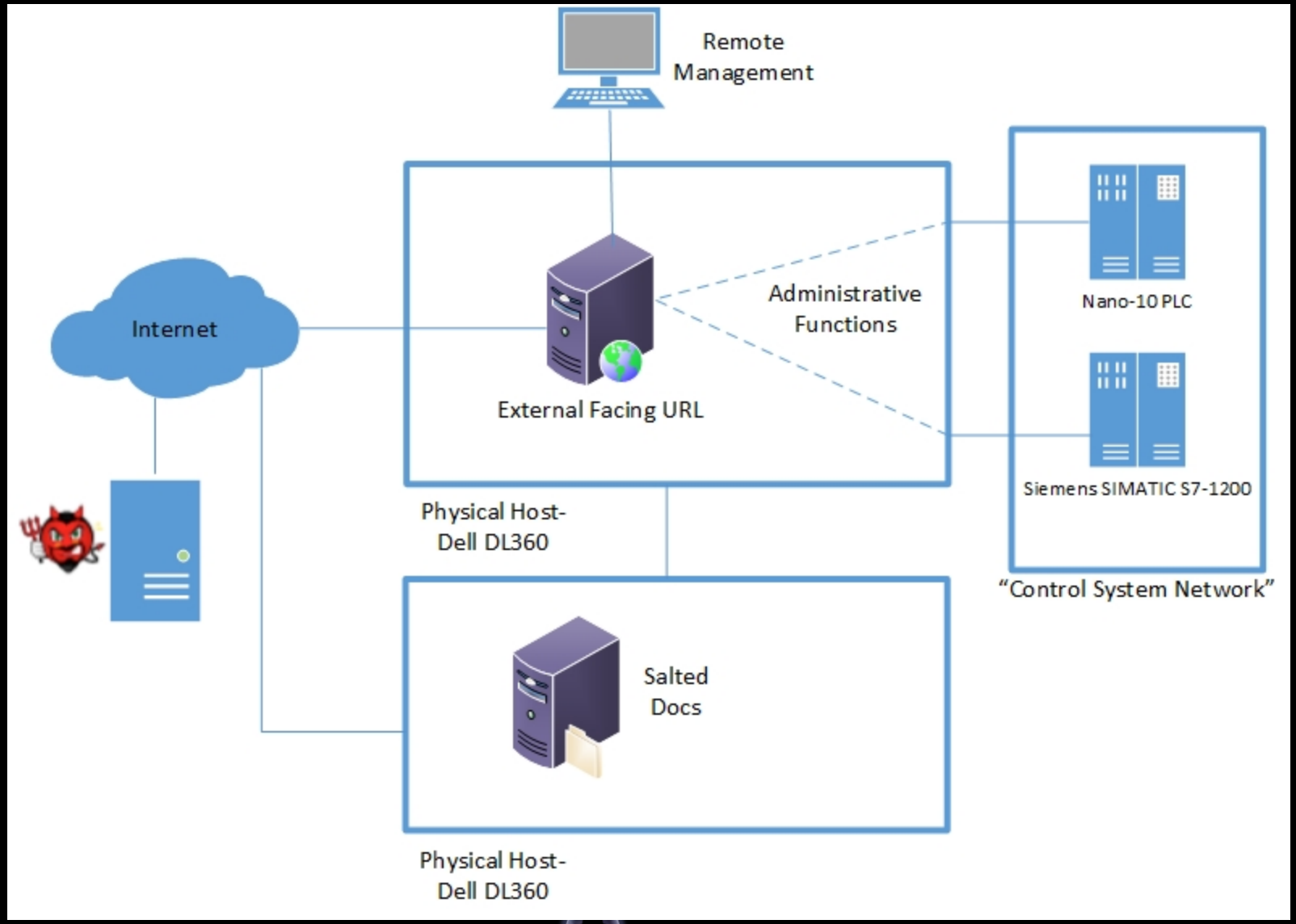




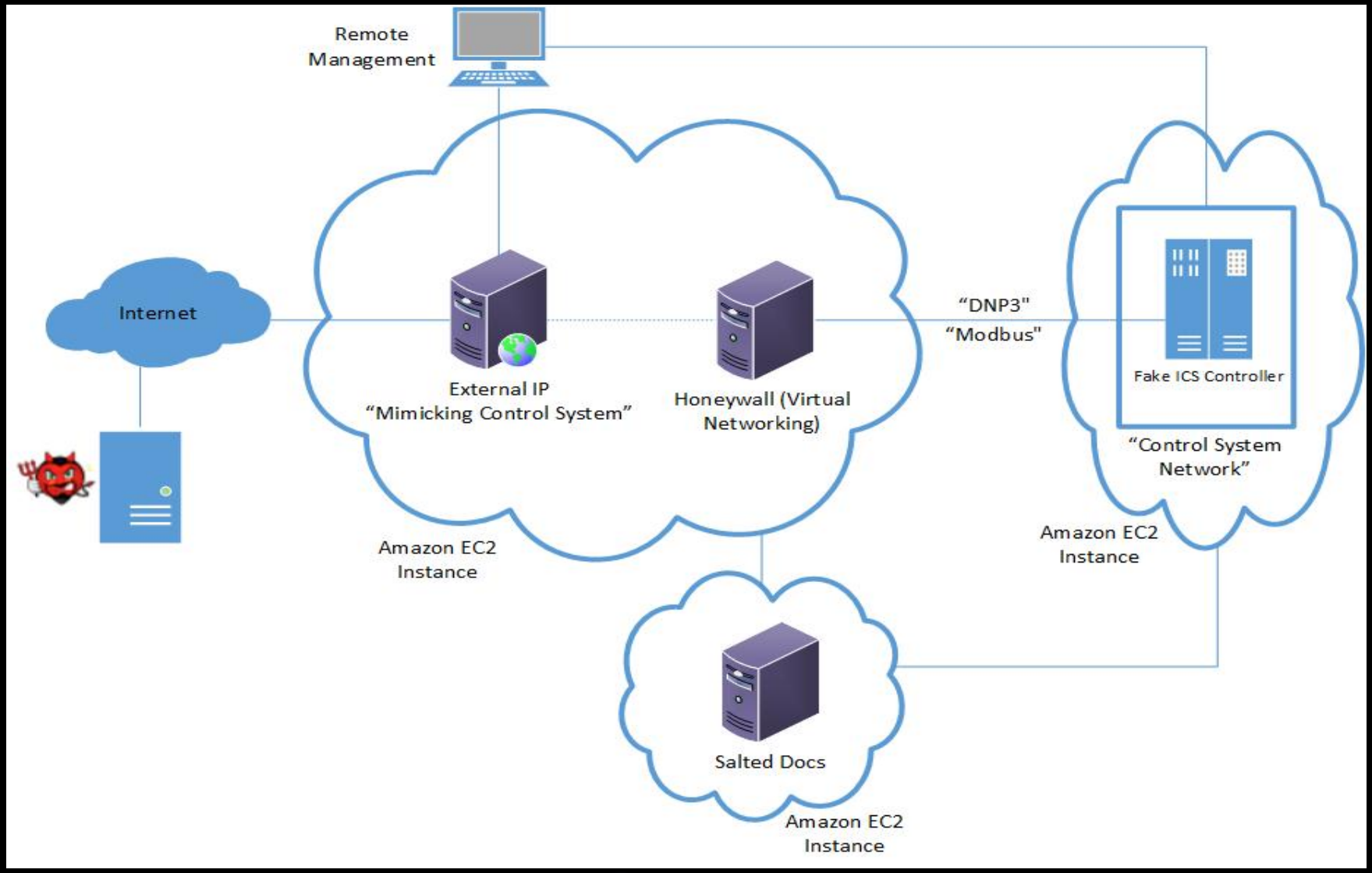
What They See



High-Interaction Architecture



Low-Interaction Architecture



Tools Used

- Snort (Digital Bond Modbus TCP Rules)
- Dionanea
- Tcpdump
- Honeyd
- Nano-10
- Siemens SIMATIC S7-1200 CPU 1212C
- Dell DL360
- Amazon EC2
- SMTP
- Salted sample data

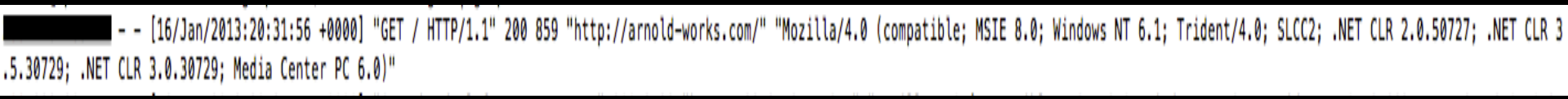
Vulnerabilities Presented

"If you can ping it, you own it"

- SNMP vulns (read/write SNMP, packet sniffing, IP spoofing)
- Authentication limitations
- Limits of Modbus/DNP3 authentication/encryption
- VxWorks Vulnerability
- Open access for certain ICS modifications- fan speed, temperature, and utilization.

Intelligence Gathering

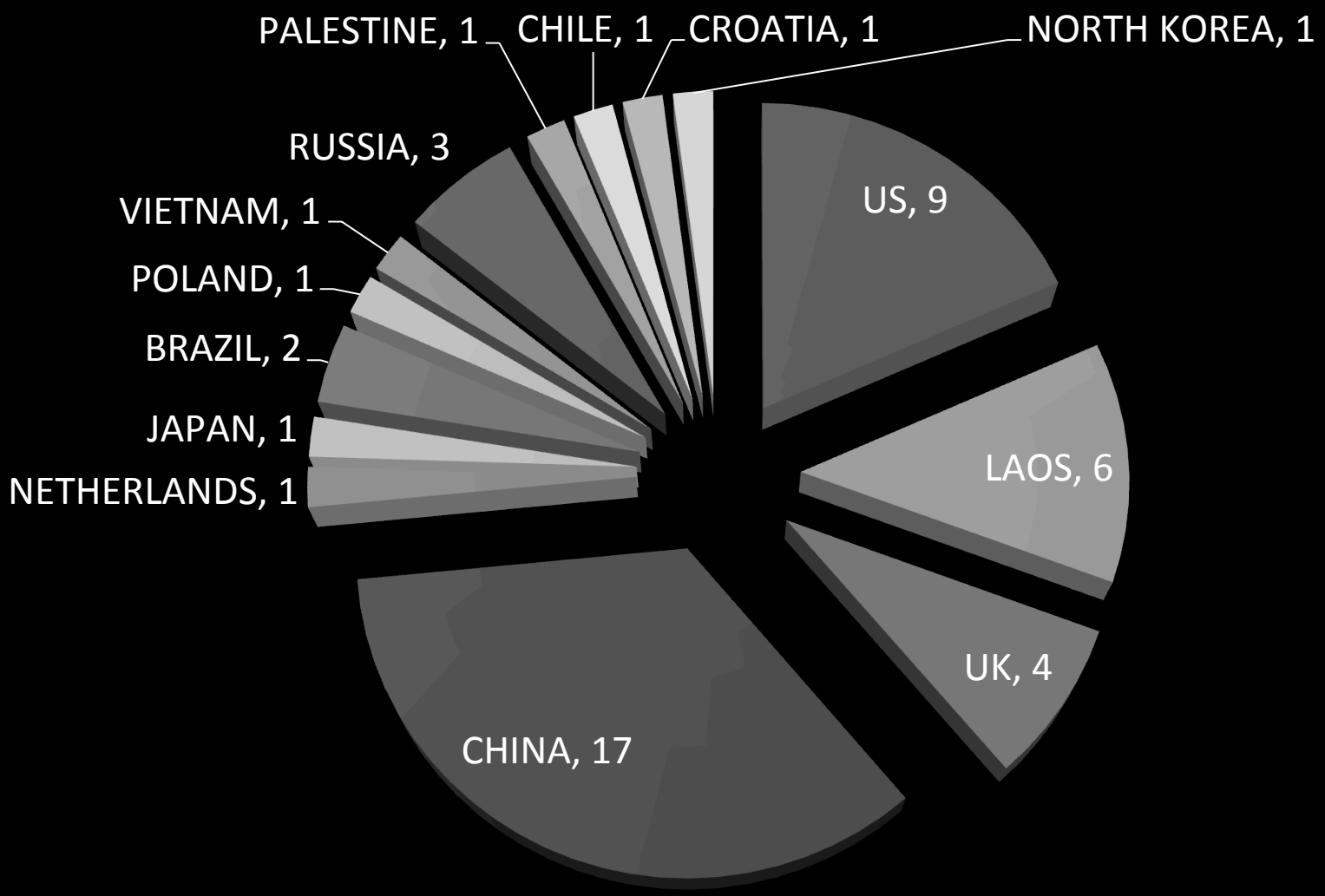
- Many of the same attackers probed ICS device(s) days before
- Port scans
- Maltego usage prevalent
- Shodanhq.com usage also prevalent



What is an “attack”?

- Not port scans, or non-targeted attacks.
- Not automated attacks
- Not drive-by
- **ONLY** attacks that were targeted
- **ONLY** attempted modification of pump system
- **ONLY** attempted modification via Modbus/DNP3
- **DoS/DDoS** will be considered attacks

Attack Profile Countries



Attack Overview

- One attempt to spear phish info@<domain>.com
- I pretended to fall for it…
- Unauthorized access attempt to diagnostics.php
- Modification of CPU Fan Speed on Water Pump
- Attempted Modbus traffic modification
- Attempted access to all secured areas of site
- Most attacks came from a few /24 netblocks
- Some attacks generated Snort alerts
- Others were manual attempts to modify pump pressure, temperature output, and/or shut down the system entirely

Unique attack attempts: 9

Countries participating: 14

Snort Findings

- Used Digital Bond's Quickdraw SCADA Snort Rules
- Custom Snort Rules Created

- *Modbus TCP - Non-Modbus Communication on TCP Port 502*
- *Unauthorized Read Request to a PLC*
- *Unauthorized Write Request to a PLC*
- *Incorrect Packet Length, Possible DOS Attack*

Snort Findings

Rules Triggered:

1111006	Modbus TCP – Unauthorized Read Request to a PLC
1111007	Modbus TCP – Unauthorized Write Request to a PLC
1111206 / 11112061	DNP3 – Unauthorized Read Request to a PLC
1111207	DNP3 – Unauthorized Write Request to a PLC
1111208	DNP3 – Unauthorized Miscellaneous Request to a PLC
1111675	CVE 20xx-xxx: Siemens Tecnomatix FactoryLink CSService GetFile path Buffer Overflow
1111676	CVE 20xx-xxx: Siemens Tecnomatix FactoryLink CSService GetFileInfo path Buffer Overflow

Spear Phished!

" 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

....Mr. <city administrator name> "

Spear Phished

X-MimeOLE: Produced By Microsoft Exchange V6.5
Content-Class: urn:content-classes:message
MIME-Version: 1.0
Content-Type: multipart/mixed;
boundary="_bc4e6dbe-64bc-49a8-9680-8bb5765d6d71_"
Subject: Report Needed!
Date: Fri, 18 May 2012 08:44:41 -0400
Message-ID:
<863A69EAF024D24EA6AC8AACA0FF762A08BCB4EE@mail.amccares.org>
X-MS-Has-Attach: yes
X-MS-TNEF-Correlator:
Thread-Topic: Report Needed!
Thread-Index: Ac008/58A6WQNgLMT5CXxoSfei68ag==
From: City Administrator <cityadmin@cityofarnold.org>
To: <info@arnold-works.com>
Return-Path: cityadmin@cityofarnold.org
X-MS-Exchange-Organization-SCL: 0

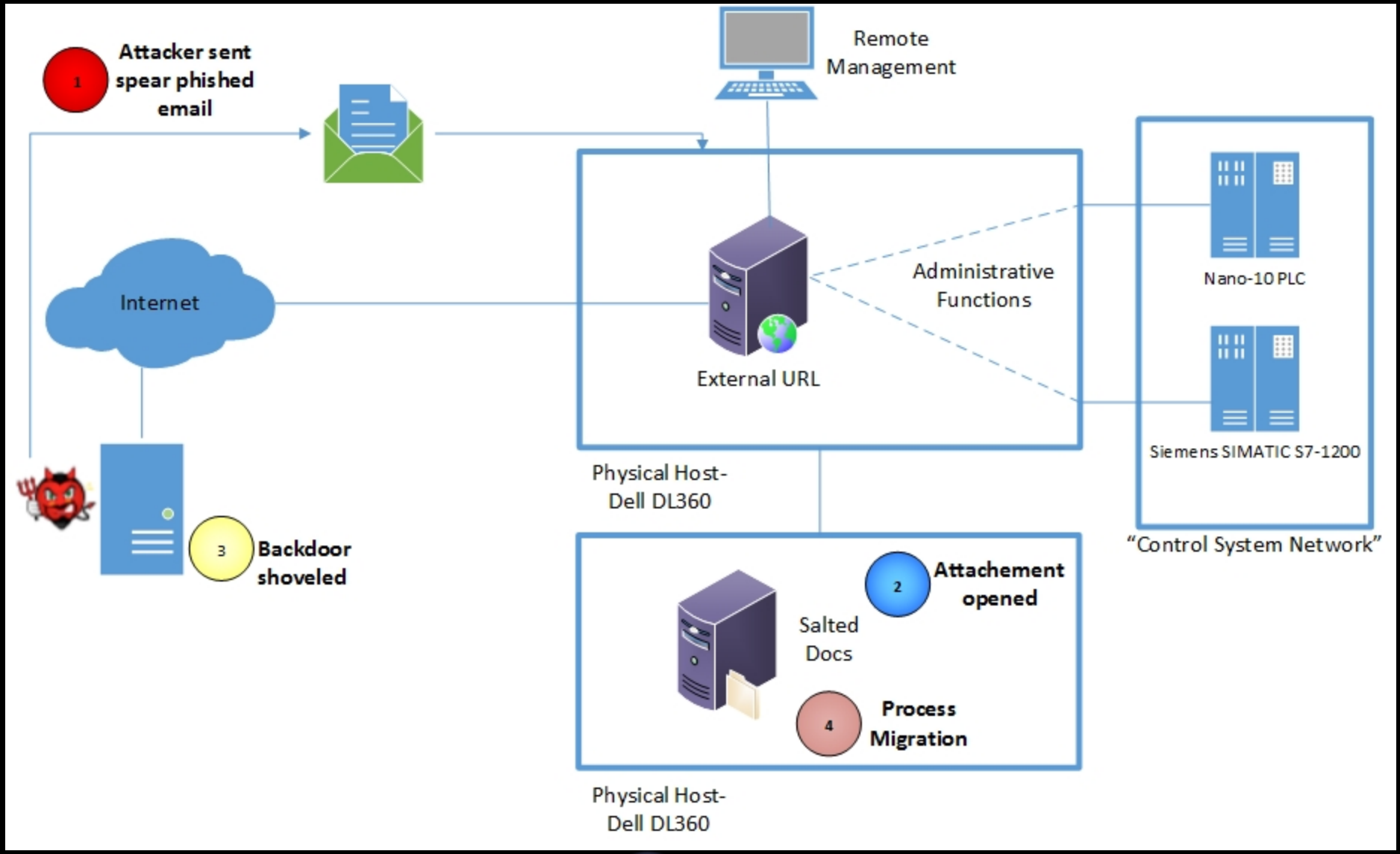
Malware

- Included in the email, was an attachement- **report.docx**
- Document dropped two PE files- gh.exe and ai.exe
- 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) –n (dll) >*
- Malware communicating to a drop/CnC server in China.

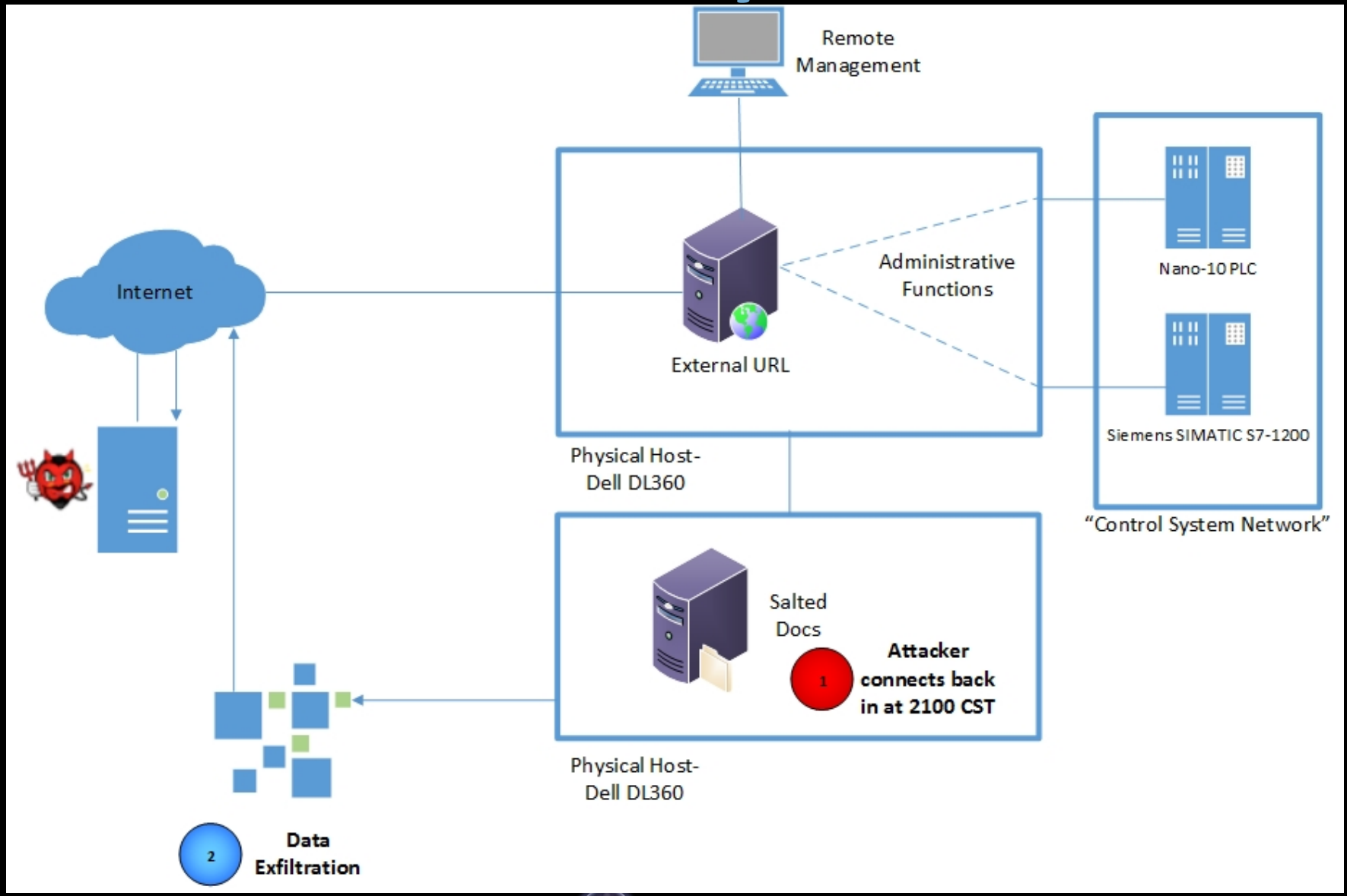
Execution

- Upon execution of report.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
- Persistence is first goal seemingly for this. Perceived future attempted lateral expansion with limited data exfiltration.

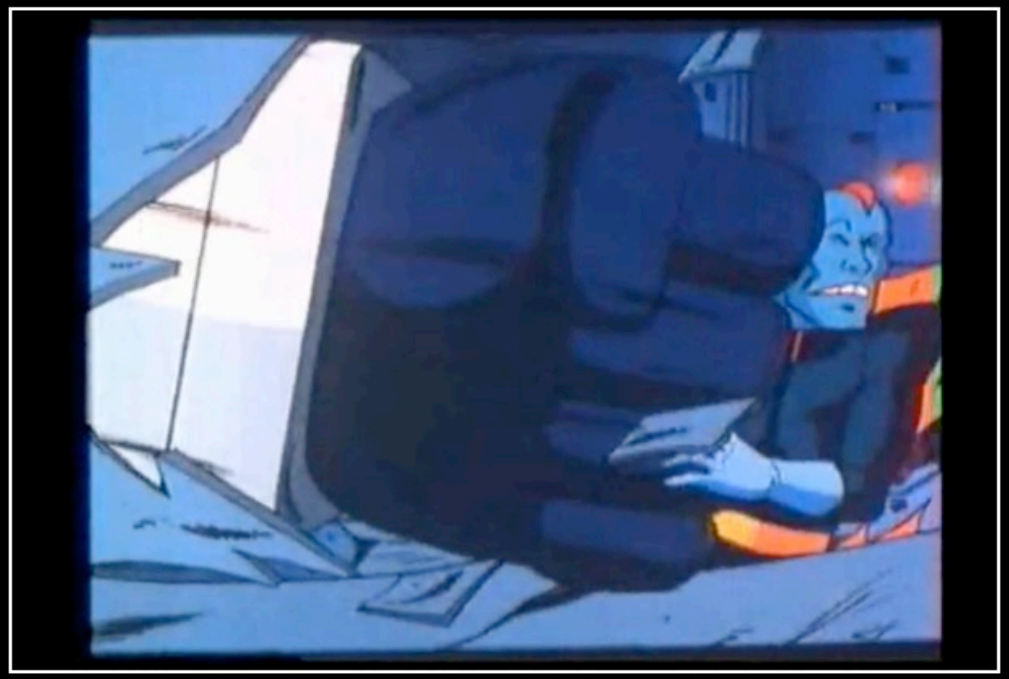
Attack: Days 1-4



Attack: Days 5-17



Attack: Days 18-???



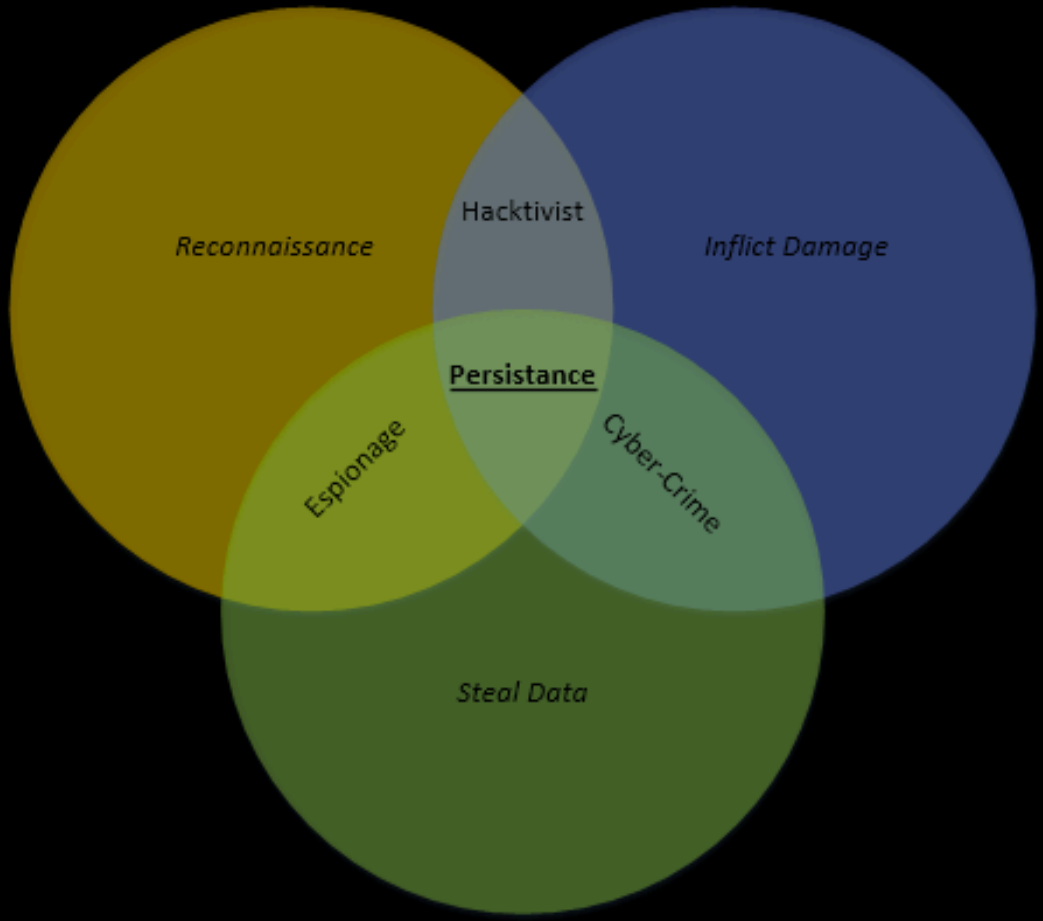
Attacker Profile

- Chose most prevalent attacker(s)
- Profiled, poked, and researched who they were
- Malware was code-reuse
- Majority traffic/development tied back to a university in China.
  - Nanjing University of Science and Technology

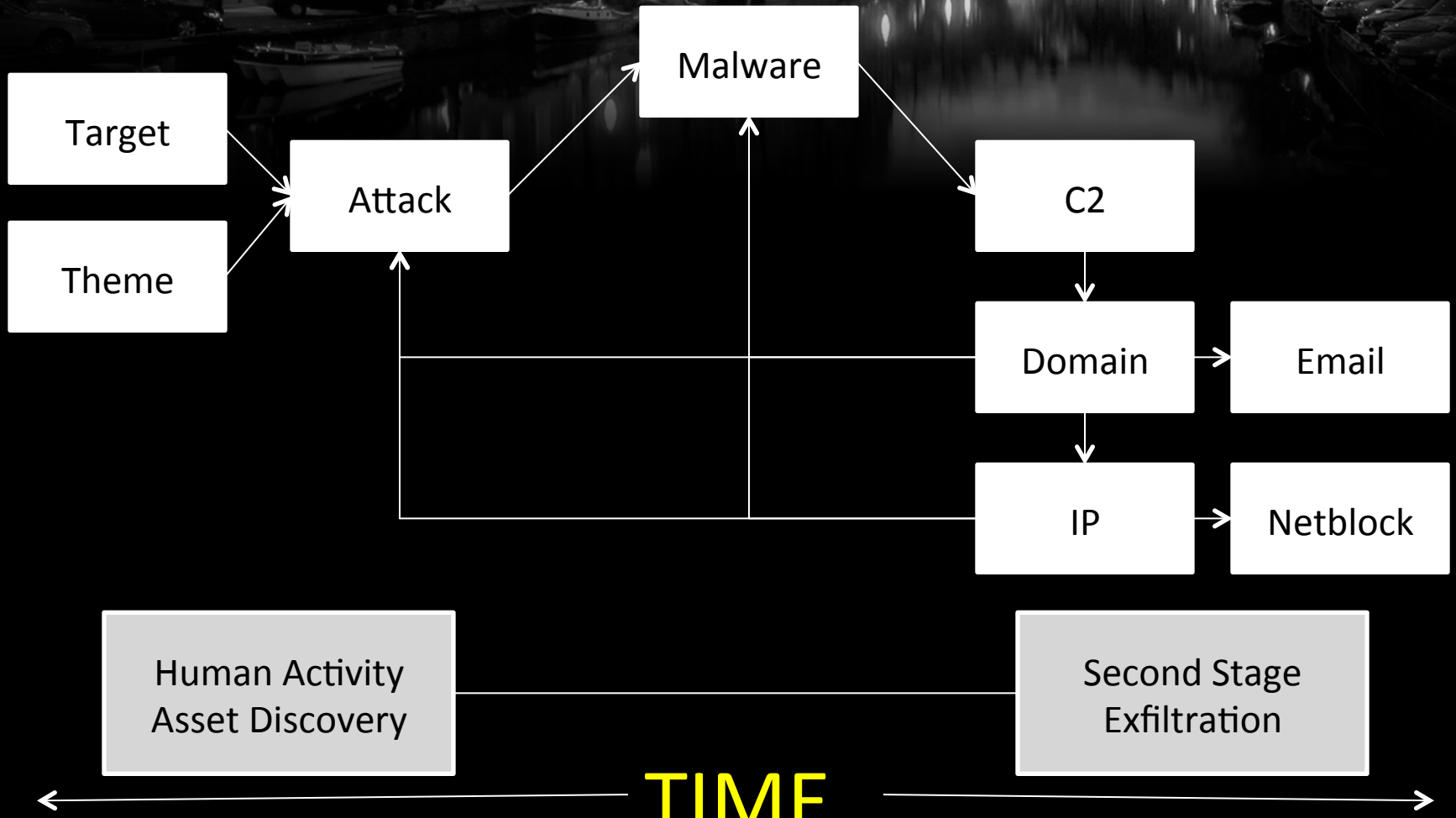
Targeted? Who Knows…

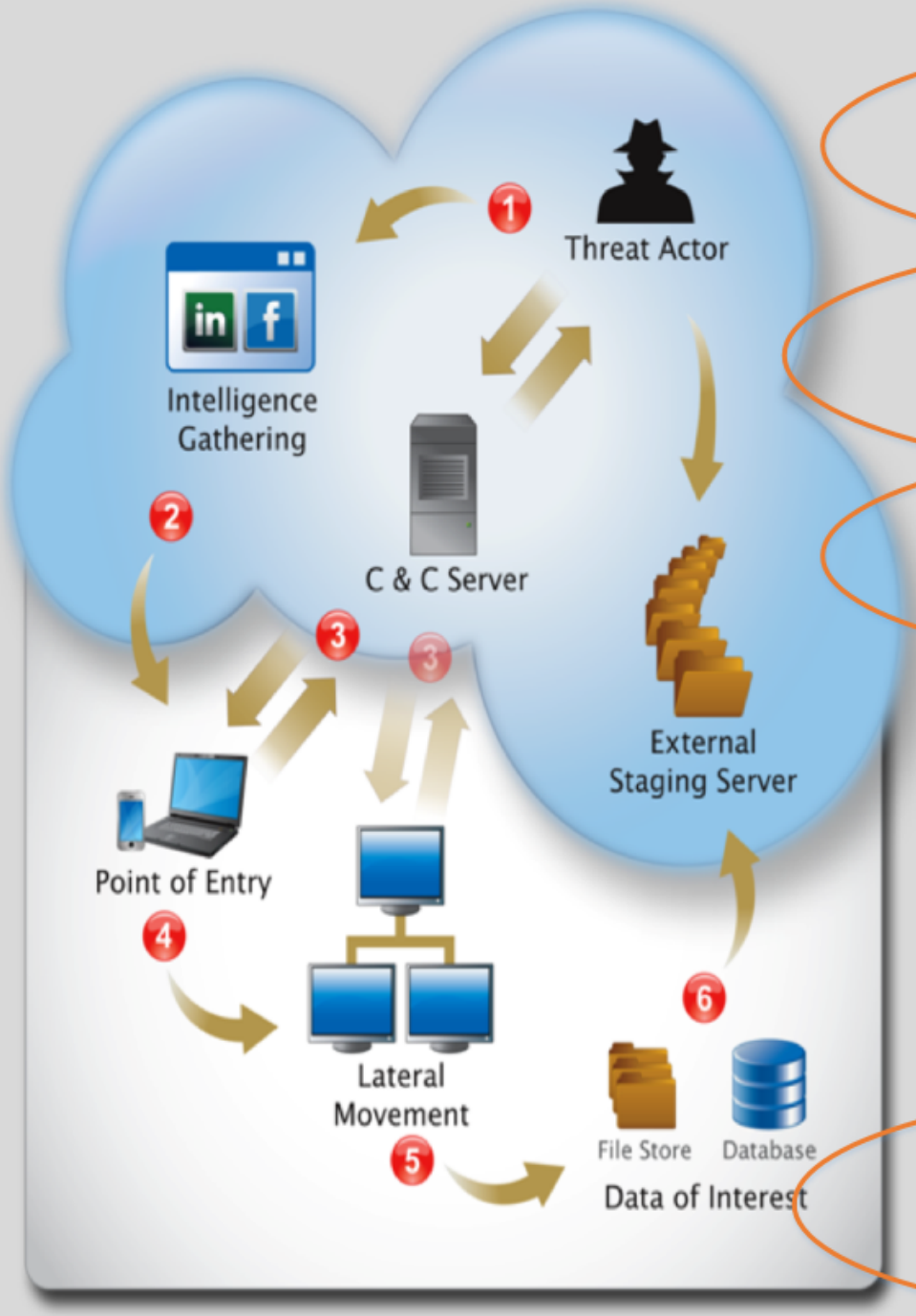
Motivation?

- Motivation is hard to establish…



Malware-Based Espionage





1. Intelligence Gathering

Identify & research target individuals using public sources (LinkedIn, Facebook, etc) and prepare a customized attack.

2. Point of Entry

The initial compromise is typically malware delivered via social engineering (email/IM or drive by download). A backdoor is created and the network can now be infiltrated.

3. Command & Control (C&C) Communication

Allows the attacker to instruct and control the compromised machines and malware used for all subsequent phases.

4. Lateral Movement

Once inside the network, attacker compromises additional machines to harvest credentials, escalate privilege levels and maintain persistent control.

5. Asset/Data Discovery

Several techniques and tools are used to identify the noteworthy servers and the services that house the data of interest.

6. Data Exfiltration

Once sensitive information is gathered, the data is funneled to an internal staging server where it is chunked, compressed and often encrypted for transmission to external locations.

Recommendations

- Disable Internet access to your trusted resources. Where possible.
- Maintain your trusted resources at the latest patch levels, and ensure you are diligent in monitoring when new patches/fixes are released.
- Require username/password (two-factor if possible) combinations for all systems, including those that are not deemed “trusted”.
- Control contractor access- Many SCADA/ICS networks utilize remote contractors, and controlling how they access trusted resources is imperative.

Recommendations

- Utilize SSL/TLS for all communications to web-based ICS/SCADA systems.
- Control access to trusted devices. For instance, for access to a segmented network, use a bastion host with ACL's for ingress/egress access.
- Improve logging on trusted environments, in addition to passing logs to SIEM devices for third party backup/analysis.
- Develop a threat modeling system to your organization- understand who's attacking you, and why.

Conclusions

- Stop exposing any critical system to the Internet
- Stop thinking ICS devices are secure- they inherently suck
- Spread the word about ICS security- it may help future
- Use two-factor authentication!
- Get your shit off Shodan!
- Continue robust logging for forensication purposes

Please complete the speaker feedback surveys!

Shout

Twitter: lowcalspam
Email: kyle_wilhoit@trendmicro.com
Non-Work: kylewilhoit@gmail.com

VM Image of honeypot (With tools) included at:
www.kylewilhoit.com/honeypot/