Emerging and Continuing Threats
Lessons Learned from SCADA APT Infection Remediation Efforts in the Field

part 1 – the bad stuff (focus on APT, Night Dragon, Stuxnet)
part 2 – what to do about it
Jonathan Pollet – CISSP, PCIP, CAP

12 Years of Electrical Engineering, SCADA, Industrial Controls, and IT Experience
- PLC Programming and SCADA System Design and Commissioning
- Wireless RF and Telecommunications Design and Startup
- Front-end Web Development for SCADA data
- Backend Database design for SCADA data
- Acting CIO for Major Oil Company for 2 years – Enterprise IT Management

Last 8 Years Focused on SCADA and IT Security
- Published White Papers on SCADA Security early in 2001
- Focused research and standards development for SCADA Security since 2002
- Conducted over 120 security assessments on Critical Infrastructure systems
- Conducted over 75 International conferences and workshops on CIP
- Developed safe security assessment methodology for live SCADA Systems
- Co-developed the SCADA Security Advanced 5-day training course
Joe Cummins, PCIP, OPST

- Canadian Information Security practitioner
  - President and Principal Consultant of Red Tiger Security - Canada,
  - Provision of Threat and Vulnerability Assessments

- SME in the areas of:
  - Critical Infrastructure,
  - Federal Readiness

- Speaker:
  - IEEE Boston, Mass
  - Canadian CIP Symposium
  - ISA Expo, Houston
  - SANS USA, SANS EURO
wall of shame....

what were they thinking....
notice anything?
this machine is used to swipe credit cards, is connected to the Internet, and has the username/password in clear sight...
microsoft vista...

you want to run your control system on this – right?
employees are lazy
...or malicious... this was a female showering facility...
vendors aren’t any better...

who builds a cash register with an Ethernet port dangling from it?
attackers assume smart people make mistakes
part 1 – the bad stuff

update on the Threat Landscape with a focus on APT, Night Dragon, and Stuxnet
part 1 - the bad stuff

- Threat Profile
  - External Threats
    - Intentional Targeted Advanced Persistent Threats (APT)
    - Unintentional External Threats
  - Internal Threats
    - Contractors
    - Employees
  - Financial Threats
    - FERC fines
    - Impact on shareholder value
    - Cost of APT infection remediation
Timeline of Attacker Motivation

1970 - 1995 (Hackerz)

2001 - 2005 (Hactivism)

2010 (Political and $$)

1995 - 2000 (Hobbyist Hacking)

2005 - 2009 (Hacker for Hire)
APT Spelled Out

- Advanced:
  - Taking advantage of latest techniques
  - Leverages Open Source Intelligence and Social Networks
  - Usually involves knowledge of specific operating system or application compromises
  - Code Reversing and Fuzzing techniques can help locate unique weaknesses in specific targeted systems

- Persistent
  - Intent dedication – resilience even after system reboot
  - Almost always has a (C&C) Command and Control capability
  - Patient / Latent ability ... *can go to sleep for months*

- Threat
  - Signatures / Vectors
APT - Threat Vectors

External

- Internet
  - Email attachments
  - File sharing
  - Pirated Software
  - Spearphishing
  - DNS / Routing Modifications

- Physical
  - Infections of Media (USB, CD)
  - Infected Appliances
  - Malicious IT equipment

- External
  - Mass Vulnerability Exploits
  - Co-location Exploitation
  - Rogue Wifi AP

Internal

- Trusted Insider
  - Rogue Employee
  - Subcontractors
  - SOC-ENG
  - Break-In
  - Dual Use software

- Trusted Channel
  - Stolen VPN Credentials
  - Hijacked Cell Communications
  - P2P tapping
  - 3rd party breach
  - Un-trusted Devices

web: redtigersecurity.com
APT - Threat Vectors

- Malware / Worms
  - 2009 May – July
  - 1335 Unique variants and infections
    - Incl. Conficker Worm / Conficker A, B, C, D and E
    - Malicious AV Advertisements/Products
    - Segmentation of the Network (ITSG-ITSB)

- Mobile Devices
  - USB drives
    - U3 Devices
  - Stolen or lost Laptops

- Insecure Builds
  - Devices that are mis-configured / unpatched before activation
• Information leakage
  • Exposure of sensitive media / material online
  • Small / Irrelevant

• Application Security
  • Fuzzing / Reverse Engineering
  • Overflows, Cross Site Scripting,

• Social Engineering
  • Spear phishing
  • Social Engineering Toolkit (SET) Framework
APT - Tools

• Open Sourced Information

• Search Aggregators

• Malware:
  • Botnets
  • Crimeware
  • Rootkits
  • Malicious Attachments

• Live DVD – Distributions
  • Backtrack
  • A.P.E.
Don’t take my word for it...

• General Keith Alexander
  • Head, US Cyber Command
  • On Operation Buckshot Yankee
  • "probed by unauthorized users approximately 250,000 times an hour, over six million times a day."

• Richard A. Clark
  • "It is the public, the civilian population of the United States and the publicly owned corporations that run our key national systems, that are likely to suffer in a cyber war."
• William J. Lynn III,
  • Deputy Secretary of Defense
  • "Computer-induced failures of U.S. power grids, transportation networks, or financial systems could cause massive physical damage and economic disruption"

• Jonathan Evans
  • Head MI-5
  • Both traditional and cyber espionage continue to pose a threat to British interests, with the commercial sector very much in the front line along with more traditional diplomatic and defense interests
tools and tradecraft

skills and methodology used in construction of APT
APT – Techniques / Tradecraft

- OSINT
- Social Engineering
- Targeted “Spear Phishing”
- Malicious Attachments
- USB devices
- Websites
Social Engineering

• Attack the 8\textsuperscript{th} (Human) Level
• Contextual
• Implied / Explicit
• Leverages social interaction
• “Robyn Sage” Experiment
Targeted Spear Phishing

• Require in-depth knowledge of the target
• Sophistication based on posted / known information
• Seemingly benign small amounts of information leveraged to gain trust and access to specific people / groups
Malicious Attachments (Malware)

- PDF
- MS Products
  - Word, Excel, etc...

- The usual suffixes...
  - mp3, exe, lnk, dll, mov, com, mp4, bat, cmd, reg, rar, emf, shs, js, vb, yourcompany.com.zip, cab, mda, zip, mdb, scr, aiff, mde, cpl, msi, vbs, aif, m4p, msp, fdf, mdt, sys, wmf, hlp, hta, pif, jse, qef, scf, chm, <#>.txt, wsf, fli, vbe
Malware favored as attack vector

- Malware: 66.8%
- Other: 7.7%
- Phishing: 8.6%
- Physical Loss: 3.1%
- Denial of Service: 1.8%
- Unauthorized Access Attempt: 11.8%
- Inappropriate Use: 0.2%

Hardware backdoor

• Provision of devices/equipment that have “malware” already
  • Projectors
  • Printers
  • Photocopiers
    • Flash memory
  • W32 Spybot worm

Malware Kits

• Proliferation of cheap and easy to use
  • Free (Webattacker)
  • Torrents, P2P

• Complex $7,000 kits
  • 12+ kits available every 3-4 months

  • Zeus (ZBOT)
  • GHOSTNET (GHOSTRAT)
  • MUMBA (Zeus v3)
  • Mariposa
ZEUS (ZBOT)

- Professional Crime-ware toolkit
- Versions: v.1 – v3 +
- Targets banks, banking systems
  - Harvests client data
  - Accounts
Zeus (ZBOT) Server location

- ZeuS C&C servers tracked: 307
- ZeuS C&C servers online: 164
- ZeuS FakeURLs tracked: 38
- ZeuS FakeURLs online: 27
Command and Control (C&C)

- Leverages communication systems to relay messages
- Command Vectors
  - Twitter
  - IRC
  - Facebook
  - Google Groups
What are they after...

- Intellectual Property
  - Code
  - Applications
  - Protocols

- Designs
  - Schematics
  - Drawings
  - Illustrations

- Chemical / Biological
  - Formula’s
  - Equations
  - Chemical Compounds
APT – Other Recent Examples

- Eastonia vs Russia: 2007
- Ghostnet: 2009 – 2010
- Operation Aurora: June 2009 – January 2010
- Stuxnet – 2010 - Present
Russia – Georgia Conflict (July – August 2007)

• Objective:
  • Precursor to the South Ossetia War
  • Destabilization / PsyOps support / Mis-Information

• Targeted:
  • 7 August: Georgian servers and the Internet traffic were seized and placed under external control;
  • 8 August, country wide cyber attack. Alleged connections to “Russian Business Network”;
  • 9 August, Defacement of Georgian MFA, MIA, MOD. DDOS National bank of Georgia as well as news portals;
  • 12 August, President Saakashvili’s website, Georgian TV websites were attacked;
  • 12-13 August, the Georgian MOD website suffered direct attack as well as compromise.
Operation Aurora

- **Objective**
  - Dubbed “Operation Aurora” based on a filename in the malicious payload traced to one of the hackers
  - leveraged a Windows Internet Explorer browser vulnerability (CVE-2010-0249)

- **Targeted:**
  - Intellectual property,
  - software configuration management (SCM) systems
  - Gmail e-mail accounts of Chinese human rights activists and three dozen large enterprises.
  - Google, IBM, Juniper, +28 others
  - STILL IN THE WILD
Operation Aurora (Con’t)

• Stages of infection
  • A targeted user received a link in email or instant message from a “trusted” source.
  • The user clicked on the link which caused them to visit a website hosted in Taiwan that also contained a malicious JavaScript payload.
  • The user’s browser downloaded and executed the malicious JavaScript, which included a zero-day Internet Explorer exploit.
  • The exploit downloaded a binary disguised as an image from Taiwan servers and executed the malicious payload.
  • The payload set up a backdoor and connected to command and control servers in Taiwan.
  • As a result, attackers had complete access to internal systems.
GhostNet (Ghostrat)

• Objective
  • Infection and Exfiltration

• Targeted
  • over 1,2000 infected in over 100 countries.

• Stages of Infections
  • infected host downloads trojans that give the attacker control of actions made on host computer.
  • the trojan attacks the computer by downloading files and activating the host’s webcams and microphones.
Stuxnet Dissected

• STUXNET
  • Took advantage of Jmicron / Realtek private keys to hack drivers that were signed by these companies
  • Legitimate signatures
  • Leveraged 4 Windows 0day vulnerabilities
  • Flexible to spread and infect over USB or over connected networks
  • Targeted specific Siemens applications, DLLs, and PLC code
Valid Certificates ?!?!
Certificates – Con’t

Verify Certificate

Common Name: JMicron Technology Corp.
Status: Valid
Class: Digital D Class 3 - Software Validation Renewal
Organization: JMicron Technology Corp.
Organizational Unit: Digital D Class 3 - Microsoft Software Validation v2 System Design
State: Taiwan
City/Location: Hsinchu
Country: TW
Serial Number: 476f49f4c959/656e9a1eb67fc529bb
Issuer Digest: 4e302aae92e8d99951ec2be99ec85757
Multiple Infection Vectors
- USB replication (x3)
- Network propagation

Multiple Windows 0days
- SMB - MS08-067
- Printer spooler
  - CVE-2010-2729
  - MS10-061
- USB - BID 41732 + ~WTR4121.tmp and WTR4132.tmp

Highly Selective Targets
- Looks for s7ttxdx.dll to indicate presence of Step7 WinCC PLC Configuration software
- If Step7 WinCC not present, STOP

Siemens Default Passwords
- Knowledge of default hardcoded username and password to access the Step7 WinCC application

Certificate Substitution
- Substitute compromised certificates to gain access to the Siemens API and system drivers

Inject Rouge PLC Logic
- Leverage access to the APIs and drivers, forged certificates, and known default passwords to scan for specific S7 PLCs (post 2008 firmware versions)
- Inject new STL (Structured Text Language) PLC code
- Injected code suggests insider knowledge of specific industrial plant processes

Hide Injected PLC logic
- If PLC logic is uploaded back into the Step7 WinCCU Configuration, the new STL logic is suppressed
Night Dragon... Staged attack

• Series of weeks/months to fully compromise a system

• Incremental uploads/downloads/xchanges

• Results are fully “rooted” devices

• Random “radio” silence
  • Remain hidden,
APT – Steps to compromise

1. Intel Gathering
2. Initial Attack Vector

Target Research
Build Attack Vectors

Corporate Firewall

3. Hide Itself by Hooking to Known Services

4. Privilege Escalation
5. Setup Command Posts
6. Launch Internal Attacks
7. Locate Critical Systems

Upload Malware / C&C

8. Achieve Persistence and Extricate Data

Full Compromise

Learn The Systems

web: redtigersecurity.com

46
The Horizon

• Mutating Bots / Command & Control
  • Quiet installation
  • Obfuscated Exfiltration (HTTP, DNS, Masked)

• Directed Social Engineering
  • Staggered Attack
  • Combined with other styles
  • Building relationships over time

• Leverage of Social Networks (SOCNET)
  • Facebook is not your friend
  • Twitter or Linkedin aren’t too fond of you either...
part 2 – what do do do about it

Advanced Persistent Threats meet Advanced Persistent Diligence
part 2 – what to do about it

• Advanced Persistent Diligence

• Security Frameworks (NERC CIP, CFATS, ISA S99)

• Technical Controls > Defense in Depth
  1. Physical (should compliment/reinforce cyber)
  2. Network (perimeter)
  3. DMZ (what goes here?)
  4. SCADA HMI (hosts / applications)
  5. Protocols (transport)
  6. End Devices (PLCs, RTUs)

• Procedural Controls > Enforcement

• How Recent Cyber Attacks Evade Security Controls
Advanced Persistent Diligence

- Defense in Depth Approach is required
  - Active Network Defense systems such as firewalls, UTMs, and IPS are not enough, since APT threats can easily slide through these cyber defenses.
  - Having situational awareness of what is attempting to connect to the system, as well as what is going on within the system is the only way to start to regain control of the system.

- Testing patches before pushing
  - Development of a lab environment
  - Functional
  - Compressed version of ACTUAL devices and configuration

- Cyber Security Awareness
  - Employees are the best security barometer
Advanced Persistent Threat vs. Advanced Persistent Diligence

External Steps

1. Intel Gathering
2. Initial Attack Vector
3. Build Attack Vectors

Actions Taken Once on the Inside

4. Privilege Escalation
5. Setup Command Posts
6. Launch Internal Attacks
7. Locate Critical Systems

Full Compromise

8. Achieve Persistence and Extract Data

Corporate Firewall

Tighter Network and Host Controls + Situational Awareness

- Blue Team
- Defender
- (APD) Advanced Persistent Diligence

Target Research

Red Team
Attacker
(APT) Advanced Persistent Threat

Learn The Systems

SCADA Firewall (if present)
How to Detect if Your System is Infected

• **Watch for unauthorized changes being made to any system accounts.** If new domain controller accounts are added to the system, or if user accounts are randomly locked, then unlocked, or if the administrator account starts to be used when the administrators are clearly not on the network, then the APT attacker has already established a bi-directional link with the network.

• **Analyze the server(s) or workstation(s) involved.** Typically the logs will point out specific systems by IP address that are exporting data or used to escalate system privileges. Often, the malware and command and control (C&C) rootkits used by APT are not discovered by rootkit detectors because they hook into and hide behind known services. On Windows systems, analyze the following commonly-used services files for size (to see if they’re too large) and number of instances (too many) on Windows systems:
  • `svchost.exe` (most common)
  • `iexplore.exe`
  • `iprinp.dll`
  • `winzf32.dll`

• **Investigate.** By using a combination of network and host investigative tools, determine how many instances of these files are running in memory, the size of those files, and what specific process identifiers (pids) are associated with them. Before shutting infected systems down, follow calls the malware is making to other computers, and to their command and control in order to determine scope of intrusion.
Security Mapped to 6 Functional Areas

1. Physical Access
   (Limit Direct Access to Control Rooms and Equipment)

2. Network Architecture
   (Firewalls, Routers, Switches, Network Segmentation, etc.)

3. SCADA DMZ
   (Data Historians, Web Servers, Patching Servers, AV Servers, etc.)

4. Assessing Mission Critical Servers/Workstations for Host and Application Vulnerabilities
   (Operating System settings for SCADA Server(s) and Workstation(s). This includes Domain/Workgroup settings, Active Directory, Group Policy Settings, and critical applications like HMI, CEMS, SCADA, and others.)

5. Control System COMM
   (wired and wireless communications from control room out to local controllers)

6. Local Controllers
   (PLCs, RTUs, IEDs, and any other local control devices)
Across all Six Layers spans the need for procedural controls that include:

- Asset Inventory, System Documentation, Management of Change, and Test / Development Systems
- Risk Management, Patch Management, Lifecycle Planning, and Routine Assessments
- Crisis Management, Emergency Planning, Safety, and Safe Shutdown Procedures, Backup and Recovery

### Technical Controls

1. **Physical Security**
   - (Fencing, Surveillance, Guards, Gates, Locks)

2. **Network Infrastructure**
   - (Switches, Routers, Firewalls, 3rd Party Connections, and Modems)

3. **Manufacturing IT DMZ**
   - (Data Historians, Data Logging, Web Servers)

4. **Mission Critical DCS Servers, Workstations, and Operator Consoles**
   - (Operating System Security, Application Security)

5. **Communications to Field Devices**
   - (Profinet, Modbus, OPC, and other protocols...)

6. **Field Devices**
   - (PLCs, RTUs, IEDs, Plant Equip.)
<table>
<thead>
<tr>
<th>Layer</th>
<th>Control Description</th>
<th>NERC CIP</th>
<th>CFATS</th>
<th>CHEMICALS</th>
<th>ISA 99</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Physically Secure Access to Control Devices</td>
<td>CIP-005</td>
<td>RBPS 2</td>
<td>CIP-005</td>
<td>ISA-T99.00.002, 6.6.8.3, “Physical and Environmental Security”</td>
</tr>
<tr>
<td></td>
<td>Physically Secure Access to Control Networks</td>
<td>CIP-005</td>
<td>RBPS 2</td>
<td>CIP-005</td>
<td>ISA-T99.00.002, 6.6.8.3, “Physical and Environmental Security”</td>
</tr>
<tr>
<td></td>
<td>Role-based Physical Access Controls</td>
<td>CIP-005</td>
<td>Metric 8.3.5</td>
<td>ISA-T99.00.002, 6.6.8.3, “Physical and Environmental Security”</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Visitor Controls</td>
<td>CIP-001</td>
<td>Metric 8.3.5</td>
<td>ISA-T99.00.002, 6.6.8.3, “Physical and Environmental Security”</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Inspection and Testing of Physical Controls</td>
<td>CIP-005</td>
<td>Metric 8.3.5</td>
<td>ISA-T99.00.002, 6.6.8.3, “Physical and Environmental Security”</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Temporary Physical Security During an Outage</td>
<td>CIP-006</td>
<td>Metric 8.3.5</td>
<td>ISA-T99.00.002, 6.6.8.3, “Physical and Environmental Security”</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Written Plan to Repair Physical Security Deficiencies</td>
<td>CIP-005</td>
<td>Metric 8.3.5</td>
<td>ISA-T99.00.002, 6.6.8.3, “Physical and Environmental Security”</td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Networking Architecture</td>
<td>CIP-005</td>
<td>Metric 8.3.5</td>
<td>ISA-T99.00.002, 6.6.8.3, “Physical and Environmental Security”</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Firewalls</td>
<td>CIP-005</td>
<td>Metric 8.3.5</td>
<td>ISA-T99.00.002, 6.6.8.3, “Physical and Environmental Security”</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Typical Network Traffic</td>
<td>CIP-005</td>
<td>Metric 8.3.5</td>
<td>ISA-T99.00.002, 6.6.8.3, “Physical and Environmental Security”</td>
<td></td>
</tr>
</tbody>
</table>

**Security Controls by Functional Areas Mapped to NERC CIP, CFATS, and ISA S99 standards**

[web: redtigersecurity.com]
Utilities should be able to show at minimum they meet the (R) required controls in the NERC CIP standards.
Down in the Protocols and Field Devices areas, NERC and CFATS do not provide adequate guidance...

ISA S99 can fill in the gaps
### DHS CFATS Standards

DHS CFATS standards provide more clarity in topics relating to Crisis Management and communications with Emergency Responders.

<table>
<thead>
<tr>
<th>Standards, Policies, or Procedures that Map to the Controls</th>
<th>NERC CIP &gt;&gt; REQUIRED</th>
<th>CFATS (DHS) &gt;&gt; CHEMICALS STANDARD</th>
<th>ISA 99 &gt;&gt; INTERNATIONAL BEST PRACTICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site Vulnerability Assessments (Audits) - Facilities must perform a risk-based, security/vulnerability assessment to determine the realistic threats and potential consequences that a breach of security might have on the facility. As part of this assessment process, the facility shall arrange for an independent audit of the process control LAN infrastructure to be carried out. The facility should conduct annual audits that measure compliance with the facility's cyber security policies, plans, and procedures and reports audit results to senior management. Electricity utilities must perform this vulnerability assessment every year.</td>
<td>CIP-005, 007 Metric 8.9 – Audits</td>
<td>ISA TR99.00.002, section 6.6.5 Vulnerability Assessment</td>
<td></td>
</tr>
<tr>
<td>Risk Management - The results of the vulnerability assessment should be fed into a remediation plan to reduce the risk to the facility</td>
<td>CIP-002 Metric 8.7 – Systems Lifecycle</td>
<td>ISA TR99.00.002, Section 9, Conduct Risk Assessment and Gap Analysis</td>
<td></td>
</tr>
<tr>
<td>Asset Lifecycle Planning - System Manager shall develop and maintain an asset life plan for the Facility's manufacturing IT network, and must be reviewed annually. The facility should integrate cyber security into the system lifecycle (design, procurement, installation, operation, disposal). The facility should establish security requirements for all systems and networks before they are put into operation, and for all operational systems and networks throughout their lifecycle.</td>
<td>CIP-002 Metric 8.7 – Systems Lifecycle</td>
<td>ISA-TR99.00.002, 6.6.10 Living Program, ISA-TR99.00.002, 6.6.11 Industry Participation, ISA-TR99.00.002, 6.6.12 The Security Lifecycle</td>
<td></td>
</tr>
<tr>
<td>Crisis Management - The facility has a comprehensive crisis management plan</td>
<td>CIP-009 Metric 9.1 – Comprehensive Crisis Management Plan</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Emergency Communications Capabilities - The facility has a communications and emergency notification system with emergency back up power and/or an equivalent written contingency procedure in place that is designed, laid-out, and constructed to avoid common cause/dependent failures and equipped with redundant signal processing.</td>
<td>CIP-009 Metric 9.2 – Communication Systems</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Safety and Safe Shutdown Procedures - All process units have an automated control system or other process safeguards to rapidly place designated target asset (e.g., CO2 equipment in a safe and stable condition, and procedures for their use in an emergency. Additionally, all process units have a procedure for safe shutdown in an emergency.</td>
<td>CIP-009 Metric 9.3 – Process Safeguards</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communications with Emergency Responders - The facility has an active outreach program to the community and local law enforcement and emergency responders. Examples of outreach activities include participation in Local Emergency Planning Committees (LEPC) (where local law enforcement is a LEPC member), Community Hazards Emergency Response-Capability Assurance Program (CHER-CAP) (where local law enforcement is a CHER-CAP member), Border Zone Protection Program (BZPP) activities, Neighborhood Watch Programs (where industry and businesses are included in these programs), or participation by the facility in security-related drills and exercises in conjunction with off-site responder organizations.</td>
<td>CIP-006 Metric 9.4 – Outreach</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
How Recent Cyber Attacks Evade Security Controls

• We understand that NERC CIP and most security standards require several physical and cyber controls that could prevent and detect APT attacks including tight access controls at the perimeter, logging and monitoring of all access points, malicious software detection at the host level, administrator account monitoring, and change controls.

• **However, these controls are often not enough to thwart a motivated attacker**, since they are gambling on some of the following assumptions about typical cyber defenses...
Typical Weak Links in the Chain

1. Most corporations are not aware about what information can be found about them in public available open source channels.

2. Even though end uses are provided security awareness training, a large majority of internal users will click on attachments and links that they should not trust.

3. Typical local host defenses such as Antivirus do not detect modifications to known good windows services and most APT attacks can avoid detection by AV.

4. Most system administrators do not pay close attention to misuse of administrator accounts, so privilege escalation attempts are also often not detected.
Typical Weak Links in the Chain

5. Once on the inside, malware can move fairly freely to setup command posts, deploy drones, and begin looking for useful data since internal network traffic monitoring can not pick up slow attacks that can hide within the same corporate traffic patterns.

6. Most firewalls are programmed focusing on blocking incoming traffic, but allow unfettered outbound communications. When configuring the communications to outbound C&C servers, attackers use ports commonly left open through firewalls like 53 (DNS), 80 (HTTP), and 443 (HTTPS).

Command and Control communications tend to use benign communication channels such as Twitter. Attack commands just appear as legitimate traffic. Attackers also bet on the fact that in most cases outbound firewall traffic is not monitored, nor are any traps placed to alert on abnormally high amounts of traffic going to any one particular external source.
Typical Weak Links in the Chain

7. Lack of internal network monitoring and centralized logging allows the attacker to launch NMAP scans and other searches through firewalls to detect the presence of SCADA protocols, applications, and devices.

8. SCADA systems often lack appropriate end point security technology like UTM (Unified Threat Management) code, operating system level firewalls, HIDS (Host Intrusion Detection Sensors), HIPS (Host Intrusion Prevention Sensors), AV (Antivirus), and application whitelisting technology. Since security event logging is rarely enabled on SCADA servers and workstations, APT attacks can achieve persistence and extricate data off of the system without detection.
Lastly...step your game up :) 

- The best defense spends most of their time understanding the offense
- Get training
- Get plugged into RSS feeds and threat watch lists
- Practice offensive techniques
- Stand up an internal lab
- Try things
- Weave Penetration Testing into your overall strategy
contact info / q & a

Jonathan Pollet, CAP, CISSP, PCIP
Founder, Principal Consultant
Red Tiger Security, USA
office: +1.877.387.7733
mobile: +1.281.748.6401
fax: +1.800.864.6249
jpollet@redtigersecurity.com
www.redtigersecurity.com

Joe Cummins, PCIP, OPST
Founder, Principal Consultant
Red Tiger Security, Canada
office: +1.877.387.7733
mobile: +1.613.878.6007
fax: +1.800.864.6249
jcummins@redtigersecurity.ca
www.redtigersecurity.ca