Case Studies

Chris Hankin
SANS Institute: The Industrial Control System Cyber Kill Chain
3 layers and their functions

- IT Layer – spread of malware
- Control system layer – manipulation of process control
- Physical layer – where the actual damage is created
Two attack vectors (Langner)
Two attack vectors

• **CPS**: cascade protection system – fault tolerance in cascades of centrifuges including pressure relief mechanisms.

• One Siemens S7-417 for 6 cascades (984 centrifuges)

• **CDS**: centrifuge drive system – controls rotor speeds.

• Self-replication method

• One Siemens S7-315 for 164 drives
Disruption

From *To kill a centrifuge*, white paper by Ralph Langner
Unique infected hosts
(29.09.2010)
Infected Organizations

Symantec: W.32 Stuxnet Dossier
Command and Control

1. Get
2. 200 OK
3. Get index.php?data=[DATA]
   - Data:
     - OS Version
     - Machine Name
     - Workgroup Name
4a. Response Type 1:
   - 200 OK execute RPC routine
4b. Response Type 2:
   - 200 OK encrypted binary code

1 & 2: Check internet connectivity
3: Send system information to C&C
4a: C&C response to execute RPC routine
4b: C&C response to execute encrypted binary code
Network Propagation

• Peer-to-peer communications and updates
• Infecting WinCC machines via a hardcoded database server password
• Propagating through network shares
• Propagating through the MS10-061 Print Spooler 0-day vulnerability
• Propagating through the MS08-067 Windows Server Service vulnerability
P2P

1. Call RPC 0 – Get version number
2. Send installed version number
3. Call RPC 4 – Request latest Stuxnet exe
4. Send latest Stuxnet version.
5. Install latest Stuxnet version received.

Infected machine acting as RPC client

Infected machine acting as RPC server

Latest Stuxnet Version

Symantec: W.32 Stuxnet Dossier
Removable Drive Propagation

1. Exploit the vulnerability to load \~WTR4141.tmp into memory and pass control to it

2. Hook Kernel32.dll to hide malicious files

3. Hook Ntdll.dll to watch for special LoadLibrary calls

4. Call LoadLibrary with a specific name

5. \~WTR4132.tmp is loaded and a specific export is called passing control to this .dll file

Infected removable drive:
- D:\Copy of Shortcut.Ink
- D:\\~WTR4141.tmp
- D:\\~WTR4132.tmp

Symantec: W.32 Stuxnet Dossier
Step 7 Project File Infections

- **S7P files** – when an infected project is opened by the Simatic manager it performs some checks and then loads the malicious code.

- **MCP files** – may be in a Step7 folder but usually created by WinCC; opening such a file may infect the WinCC database as well.

- **TMP files** – are used by Stuxnet to copy infected files.
Modifying PLCs
Man-in-the-middle

Symantec: W.32 Stuxnet Dossier
Infected PLC (S7-315)

Symantec: W.32 Stuxnet Dossier
Ladder Logic (Wikipedia)

**AND**

```
[ ]------------------[ ]------------------( )
  Key switch 1       Key switch 2       Door motor
```

**NOT**

```
[ ]------------------[\]------------------( )
  Close door         Obstruction        Door motor
```

**OR**

```
+-------------------+
  | Exterior unlock  |
  |                  |
  +-------------------+

  Interior unlock
```

[ ] input   ( ) output
Continued

---[ ]-----[ ]--------[ ]--------( )
ES    Stop    Start    Run
          |
          |
          +---[ ]---+
          Run

------[ ]------( )
Run      Motor

1. ------[ ]------[ ]------( )
   Switch    HiTemp    A/C
   |        |        |
   +------[ ]-----+
   Humid

2. ------[ ]-----[ ]-----------------( )
   A/C    Heat    Cooling
<table>
<thead>
<tr>
<th>Mnemonic</th>
<th>Program Elements Catalog</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AW</td>
<td>Word logic instruction</td>
<td>And Word</td>
</tr>
<tr>
<td>OW</td>
<td>Word logic instruction</td>
<td>Or Word</td>
</tr>
<tr>
<td>CD, CU</td>
<td>Counters</td>
<td>Counter Down, Counter Up</td>
</tr>
<tr>
<td>S, R</td>
<td>Bit logic instruction</td>
<td>Set, Reset</td>
</tr>
<tr>
<td>NOT</td>
<td>Bit logic instruction</td>
<td>Negate RLO</td>
</tr>
<tr>
<td>FP</td>
<td>Bit logic instruction</td>
<td>Edge Positive</td>
</tr>
<tr>
<td>+I</td>
<td>Floating-Point instruction</td>
<td>Add Accumulators 1 and 2 as Integer</td>
</tr>
<tr>
<td>/I</td>
<td>Floating-Point instruction</td>
<td>Divide Accumulator 2 by Accumulator 1 as Integer</td>
</tr>
<tr>
<td>*I</td>
<td>Floating-Point instruction</td>
<td>Multiply Accumulators 1 and 2 as Integers</td>
</tr>
<tr>
<td>&gt;=I, &lt;=I</td>
<td>Compare</td>
<td>Compare Integer</td>
</tr>
<tr>
<td>A, AN</td>
<td>Bit logic instruction</td>
<td>And, And Not</td>
</tr>
<tr>
<td>O, ON</td>
<td>Bit logic instruction</td>
<td>Or, Or Not</td>
</tr>
<tr>
<td>=</td>
<td>Bit logic instruction</td>
<td>Assign</td>
</tr>
<tr>
<td>INC</td>
<td>Accumulator</td>
<td>Increment Accumulator 1</td>
</tr>
<tr>
<td>BE, BEC</td>
<td>Program Control</td>
<td>Block End and Block End Conditional</td>
</tr>
<tr>
<td>L, T</td>
<td>Load / Transfer</td>
<td>Load and Transfer</td>
</tr>
<tr>
<td>SE</td>
<td>Timers</td>
<td>Extended Pulse Timer</td>
</tr>
<tr>
<td>System Component</td>
<td>Absolute Address</td>
<td>Symbol</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Push Button Start Switch</td>
<td>I 1.1</td>
<td>S1</td>
</tr>
<tr>
<td>Push Button Stop Switch</td>
<td>I 1.2</td>
<td>S2</td>
</tr>
<tr>
<td>Push Button Start Switch</td>
<td>I 1.3</td>
<td>S3</td>
</tr>
<tr>
<td>Push Button Stop Switch</td>
<td>I 1.4</td>
<td>S4</td>
</tr>
<tr>
<td>Sensor</td>
<td>I 1.5</td>
<td>S5</td>
</tr>
<tr>
<td>Motor</td>
<td>Q 4.0</td>
<td>MOTOR_ON</td>
</tr>
<tr>
<td>Absolute Program</td>
<td>Symbolic Program</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------</td>
<td></td>
</tr>
<tr>
<td>O I 1.1</td>
<td>O S1</td>
<td></td>
</tr>
<tr>
<td>O I 1.3</td>
<td>O S3</td>
<td></td>
</tr>
<tr>
<td>S Q 4.0</td>
<td>S MOTOR_ON</td>
<td></td>
</tr>
<tr>
<td>O I 1.2</td>
<td>O S2</td>
<td></td>
</tr>
<tr>
<td>O I 1.4</td>
<td>O S4</td>
<td></td>
</tr>
<tr>
<td>ON I 1.5</td>
<td>ON S5</td>
<td></td>
</tr>
<tr>
<td>R Q 4.0</td>
<td>R MOTOR_ON</td>
<td></td>
</tr>
</tbody>
</table>

**STL**

<table>
<thead>
<tr>
<th>STL</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>O I 1.1</td>
<td>//Pressing either start switch turns the motor on.</td>
</tr>
<tr>
<td>O I 1.3</td>
<td></td>
</tr>
<tr>
<td>S Q 4.0</td>
<td></td>
</tr>
<tr>
<td>O I 1.2</td>
<td>//Pressing either stop switch or opening the normally closed contact at</td>
</tr>
<tr>
<td></td>
<td>//the end of the belt turns the motor off.</td>
</tr>
<tr>
<td>O I 1.4</td>
<td></td>
</tr>
<tr>
<td>ON I 1.5</td>
<td></td>
</tr>
<tr>
<td>R Q 4.0</td>
<td></td>
</tr>
</tbody>
</table>
UKRAINE 2015
Timeline

• 23 December 2015, Ukrainian Kyivoblenergo reported outages to customers
• Starting at around 3.35pm, 7 110kV and 23 35kV substations were disconnected for 3 hours
• 80,000 customers affected
• It later emerged that 3 different oblenergos were attacked
• In total 225,000 customers were affected
• The cyber attacks were launched within 30 minutes of each other
Generation: None
Transmission: None
Distribution: 3 Oblenergos
Loads: First Order Impacts
Attacker capability

- Spear phishing emails
- BlackEnergy 3 malware
- Manipulation of Microsoft Office documents to deliver malware
- Ability to harvest information and credentials to gain access to ICS system
- Expertise in Uninterruptable Power Supplies (UPS), SCADA and HMI
- Ability to target field devices at substations
- Denial of service on telephone system
Consolidated Technical Components

Ukraine Event
Significant Events based on publicly available reporting.

- Spearphish
- Credential Theft
- Control & Operate
- Tools & Tech
- Workstation Remote
- VPN Access
Opportunities

• Detailed list of infrastructure (such as RTU vendors and versions) posted online by vendors
• VPNs into business and ICS networks lack 2-factor authentication
• Firewall allowed remote access facility
• No continuous monitoring of ICS network

• Result: adversary could have been resident in system for 6 months or more to conduct reconnaissance
Some details

• BlackEnergy 3 embedded in Microsoft Windows files – Word and Excel

• Enabling macros allowed the installation of the malware

• BlackEnergy3 connects to a C2 server – this appears to have happened 6 months before the outages

• Attackers gathered intelligence about the Distribution Management Systems (DMSs) used by the companies
Stage 2 Details

• Attackers learnt how to interact with the 3 different DMSs
• Developed malicious firmware for the serial-to-ethernet devices ("blowing the bridges")
• There is evidence that the attacker capabilities were tested
• Use of remote admin tools on operator workstations
• Installed modified KillDisk across the environment
• Use HMIs to open breakers
Stage 2 Attack elements

• **Supporting elements**
  • Schedule disconnects for UPS systems
  • Telephone system attack for at least one oblenergo

• **Primary attack**: SCADA hijack with malicious operation to open breakers

• **Amplifying attacks**
  • KillDisk wiping of workstations, servers and an HMI
  • Firmware attacks against serial-to-ethernet devices at substations
Sliding Scale of Cyber Security

- **ARCHITECTURE**: The planning, establishing, and upkeep of systems with security in mind.
- **PASSIVE DEFENSE**: Systems added to the Architecture to provide reliable defense or insight against threats without consistent human interaction.
- **ACTIVE DEFENSE**: The process of analysts monitoring for, responding to, and learning from adversaries internal to the network.
- **INTELLIGENCE**: Collecting data, exploiting it into information, and producing Intelligence.
- **OFFENSE**: Legal countermeasures and self-defense actions against an adversary.
Disrupting Spear Phishing

• Communication with untrusted areas should be segmented, monitored and controlled
• Consider using sandboxing to evaluate emails and documents coming into the system
• Use proxy systems to control outbound and inbound communication paths
• Limit workstations to communicate only through the proxy devices by implementing perimeter egress access control
Credential Theft

- Performed by keystroke loggers – could be detected by forensic tools
- Change user and shared passwords – if permitted by vendor
- Monitor account behavior
- Implement a multi-level alarm capability
Data exfiltration

• Understand where relevant data exists in the system
• Maintain a vaulted copy of known good project files, control and safety logic and firmware
• Use file integrity checkers
• Network Security Monitoring is an active cyber defense method that detects data exfiltration
VPN Access

- Recommend use of 2-factor authentication
- Know which trusted communication paths exist
- Consider implementing time of use access
- Time-outs and manual disconnection
- Force choke points – such as all access through a DMZ. This allows monitoring by active defenders
Workstation Remote Access

• Disable remote access at host and at perimeter firewall
• Host-based application aware firewalls, application whitelisting and configuration management
• Good architecture to segment or disable remote connections
• Incident response capability
Control and Operate

• Areas of responsibility (AoRs) to restrict capabilities of operators – determined by username, workstation or hybrid

• Communication path or protocol authentication to require commands issued from an authorized asset

• Collect logs not only from hosts but from SCADA applications to – use active defenders to analyse logs
Respond and Restore

- Contingency analysis
- Failure planning
- Conservative operations
- Cyber load shed
- Root Cause Analysis
- Blackstart
- Information Sharing
Opportunities to Disrupt

IT Preparation
- Target selection
- Observable target mapping
- Malware development and testing

Hunting and Gathering
- Lateral Movement and Discovery
- Credential Theft and VPN access
- Control system network and host mapping

Sequence Pre Work
- Upload additional attack modules - KillDisk
- Schedule KillDisk wipe
- Schedule UPS load outage

Attack Launch
- Issue breaker open commands
- Modify field device firmware
- Perform TDoS
- Scheduled UPS and KillDisk

Spear phishing
- Delivery of phishing email
- Malware launch from infected office documents
- Establish foothold

ICS Preparation
- Unobservable malicious firmware development
- Unobservable DMS environment research and familiarization
- Unobservable attack testing and tuning

Attack Position
- Establish Remote connections to operator HMI’s at target locations
- Prepare TDoS dialers

Target Response
- Connection sever
- Manual mode / control inhibit
- Cyber asset restoration
- Electric system restoration
- Constrained operations
- Forensics
- Information sharing
- System hardening and prep
BlackEnergy 3

• F-Secure White Paper
• BlackEnergy originally a toolkit for DDoS attacks
• Quedagh variant of BlackEnergy
• Customisations include support for proxy servers, bypass of User Access Control and driver signing in 64-bit Windows systems
• Used by multiple groups – plausible deniability
OVERVIEW OF INFECTION VECTORS USED AGAINST UKRAINIAN TARGETS

1. Trojanized app
   - msiexec.exe installer
   - Persistent component

2. Exploit document
   - msiexec.exe installer
   - Persistent component

3. Dropper malware
   - msiexec.exe installer
   - Persistent component

4. Fake installer
   - Non-persistent component
TIMELINE OF BLACKENERGY & QUEDAGH HISTORY

BLACKENERGY Development
- BlackEnergy 1
- Quedagh APT campaign

CYBERATTACKS AGAINST GEORGIA
- 2007
- 2008
- 2009
- 2010
- 2011
- 2012
- 2013
- 2014

2012
- May 12
- BlackEnergy 3

2014
- POLITICAL CRISIS IN UKRAINE

2013
- Apr 9
- New UAC-bypassing Installer (msiexec.exe)
- Nov 14
- 64-bit support for BlackEnergy 2 driver

2012
- Dec 14
- First Installer (regedt32.exe)
- Some time after Dec 25
- Targets Ukrainian entities

2011
- 2010
- 2009
- 2008
- 2007
**Diagram 3: Configuration Data Handling**

1. **Main DLL**
   - Config

2. **HTTP POST**
   - Config

3. **C&C Server**
   - Main DLL processes configuration data embedded in its body; will only process fields related to C&C communication. BlackEnergy 2 configuration may also contain initial commands to execute.
   - Main DLL reports to C&C.
   - Main DLL processes the configuration data returned by the C&C. This time, it processes fields related to plugins and commands.

**Table 6: Main DLL’s Additional Commands During Download of Additional Files**

<table>
<thead>
<tr>
<th>HTTP POST Field</th>
<th>Description of Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>getp</td>
<td>The plugin name to be downloaded</td>
</tr>
<tr>
<td>plv</td>
<td>Some variants specify the version of the plugin to be downloaded</td>
</tr>
<tr>
<td>getpd</td>
<td>The binary name to be downloaded</td>
</tr>
</tbody>
</table>
UKRAINE 2016

www.dragos.com
CRASHOVERRIDE

Modules

- Main Backdoor
  - INSTALLS: Additional Backdoor, Additional Tools
  - CONTROLS

- Data Wiper
  - EXECUTES

- Launcher
  - EXECUTES

101 Payload 104 Payload 61850 Payload OPC DA Payload Future Modules
Backdoor/RAT Module

• Authenticates with a local proxy via the internal network established before the backdoor installation
• Opens HTTP channel to external C2 server through internal proxy
• Receives commands from external C2 server
• Creates a file on the local system
• Overwrites an existing service to point to the backdoor so the malware persists between reboots
Launcher module

• Loads payload modules and causes destruction via the wiper
• Starts itself as a service likely to hide better
• Loads the payload modules defined on the command line during execution
• Launches the payload and waits 1 or 2 hours before launching the data wiper
Data wiper

• Clears all the registry keys associated with system services
• Overwrites all ICS configuration files across the hard drives and mapped network drives
• Overwrites generic Windows files
• Renders the system unusable
IEC 104 module

• Reads a configuration file defining the target (likely an RTU) and the action to take
• Kills the legitimate master process on the victim host
• Masquerades as the new master
• Manipulates the RTU in one of four modes (not all analysed)
Attack options

- De-energize substation by an infinite loop opening closed breakers – a few hours of outages
- Force an islanding event by toggling breakers between open and closed – a few days of outages
- Amplification attacks
  - Denial of visibility
  - Denial of service against protective relays
Defense

- Develop clear understanding of where vulnerable protocols are used
- Understand OPC implementations and how the protocol is being used
- Robust backups of engineering files such as project logic, IED config files and ICS application installers
- Incident response plans
- Use forensic tools (YARA) to search for infections
- Air-gapped networks, uni-directional firewalls, antivirus etc are not appropriate. Human defenders are needed against a determined human adversary
TRITON
Summary

- Malware targeting Schneider Triconex safety controllers
- Single user of Tricon safety shutdown system
- Campaign of intelligence gathering likely to have lasted for weeks/months
- Triton malware has the ability to reprogram Triconex controllers
- Malware deployed via compromised Safety Instrumented System (SIS) engineering workstation
- System entered failed safe state and shutdown
TRISIS/Triton (www.dragos.com)

- Each SIS is unique – attackers need specific knowledge about the target system
- Therefore the attack is not highly scalable
- Compromise of the SIS does not necessarily impact on the safety of the system because the SIS should fail safe
- However changes to the control elements could change the points at which the safety system would take control of the process in an unsafe condition
Possible Attack Scenarios

- Plant shutdown
  - Create operational uncertainty
  - Trip safety fail-safes to halt operation

- Unsafe physical state
  - Typical operations safety layering should mitigate

- TRISIS is a Stage 2 attack – so an adversary must have already achieved success in Stage 1
Completion of Stage 1 of the ICS Cyber Kill Chain:
Identify and gain access to a system able to communicate with target SIS.

Stage 2 Develop:
Identify target SIS type and develop TRISIS with replacement logic and loader

Stage 2 Test:
Ensure TRISIS works as intended, likely off network in the adversary environment

Stage 2 Deliver:
Transfer TRISIS to the SIS which contains the ‘loader’ module for the new logic and support binaries that provide the new logic

Stage 2 Install/Modify:
Upon running the TRISIS executable, disguised as Triconex software for analyzing SIS logs, the malicious software utilizes the embedded binary files to identify the appropriate location in memory on the controller for logic replacement and uploads the ‘initializing code’ (4-byte sequence)

Stage 2 Execute ICS Attack:
TRISIS verifies the success of the previous step and then uploads new ladder logic to SIS
Details

• Compiled Python Py2EXE script plus:
  • inject.bin – malicious function code
  • imain.bin – malicious control logic

• TsHI is the high level interface that allows adversary’s operators to implement attack scripts

• TsBase translates the attacker’s intended operation to the TriStation protocol function code

• TsLow implements the TriStation UDP wire protocol
Defending against Triton

• Safety systems on isolated networks
• Physical access control
• Controllers in locked cabinets
• TriStation terminals in locked cabinets and only ever connected to the safety system
• Mobile data devices scanned before connection
• Proper sanitation for laptops that are connected to the safety system
• Operator stations should be configured to display an alarm when the Tricon key switch is in Program mode