The ICS Cyber Kill Chain: Active Defense Edition

Presenter: Robert M. Lee

www.sans.org/ics

@RobertMLee

@SANSICS
What I Want You to Take Away

The Models

• The Sliding Scale of Cyber Security
• ICS Cyber Kill Chain
• Active Cyber Defense Cycle

Lessons Learned from Threats

• HAVEX
• Ukraine Cyber Attack

Your Takeaways

• Strategic
• Operational
• Tactical
Little Bobby can be found at: [www.LittleBobbyComic.com](http://www.LittleBobbyComic.com) and on Twitter @_LittleBobby_
ICS Cyber Attack: Stage 1

Stage 1 mimics a targeted and structured attack campaign.

Based on the Cyber Kill Chain® model from Lockheed Martin
ICS Cyber Attack: Stage 2

Stage 2 shows the steps associated with a material attack that requires high confidence.
The Sliding Scale of Cyber Security

**Architecture:**
Supply chain, architecting the network, maintaining/patching

**Passive Defense:**
Provide protection without constant human interaction. Firewalls, IPS, AV, etc.

**Active Defense:**
Analysts monitor for, respond to, and learn from adversaries internal to the network.

**Intelligence:**
Collecting data, exploiting it into information, and producing Intelligence.

**Offense:**
Legal countermeasures, “hack-back”, etc.
Active Cyber Defense Cycle
HAVEX

LITTLE BOBBY

WHEN ARE YOU THROWING OUT YOUR CHRISTMAS TREE?

IN ABOUT TEN YEARS.

WHAT?! BUT WHY?!

MY HOUSEHOLD IS MADE UP OF CONTROL ENGINEERS.

WE OPERATE IN 20 YEAR LIFECYCLE UPGRADES.

by Robert M. Lee and Jeff Haas
Asset ID and Network Security Monitoring

Pre-Havex

<table>
<thead>
<tr>
<th>Address</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.192.30</td>
<td>502</td>
</tr>
<tr>
<td>172.16.192.31</td>
<td>502</td>
</tr>
<tr>
<td>172.16.192.32</td>
<td>502</td>
</tr>
<tr>
<td>172.16.192.33</td>
<td>502</td>
</tr>
<tr>
<td>172.16.192.34</td>
<td>502</td>
</tr>
<tr>
<td>172.16.192.35</td>
<td>502</td>
</tr>
<tr>
<td>172.16.192.36</td>
<td>502</td>
</tr>
<tr>
<td>172.16.192.37</td>
<td>502</td>
</tr>
<tr>
<td>172.16.192.38</td>
<td>502</td>
</tr>
</tbody>
</table>

Post-Havex

<table>
<thead>
<tr>
<th>Address</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.192.30</td>
<td>102</td>
</tr>
<tr>
<td>172.16.192.31</td>
<td>102</td>
</tr>
<tr>
<td>172.16.192.32</td>
<td>102</td>
</tr>
<tr>
<td>172.16.192.33</td>
<td>102</td>
</tr>
<tr>
<td>172.16.192.34</td>
<td>502</td>
</tr>
<tr>
<td>172.16.192.35</td>
<td>502</td>
</tr>
<tr>
<td>172.16.192.36</td>
<td>502</td>
</tr>
<tr>
<td>172.16.192.37</td>
<td>502</td>
</tr>
<tr>
<td>172.16.192.38</td>
<td>502</td>
</tr>
<tr>
<td>172.16.192.39</td>
<td>11234</td>
</tr>
<tr>
<td>172.16.192.40</td>
<td>11234</td>
</tr>
<tr>
<td>172.16.192.41</td>
<td>11234</td>
</tr>
<tr>
<td>172.16.192.42</td>
<td>11234</td>
</tr>
<tr>
<td>172.16.192.43</td>
<td>12401</td>
</tr>
<tr>
<td>172.16.192.44</td>
<td>12401</td>
</tr>
<tr>
<td>172.16.192.45</td>
<td>12401</td>
</tr>
<tr>
<td>172.16.192.46</td>
<td>12401</td>
</tr>
<tr>
<td>172.16.192.47</td>
<td>44818</td>
</tr>
<tr>
<td>172.16.192.48</td>
<td>44818</td>
</tr>
<tr>
<td>172.16.192.49</td>
<td>44818</td>
</tr>
<tr>
<td>172.16.192.50</td>
<td>44818</td>
</tr>
<tr>
<td>172.16.192.51</td>
<td>49525</td>
</tr>
<tr>
<td>172.16.192.52</td>
<td>49526</td>
</tr>
</tbody>
</table>

Know Topologies

Collect

Analyze

Detect
### Incident Response

1. **Plan and Train**
2. **Scope the Infection**
3. **Collect Forensic Data**
4. **Maintain Safe and Reliable Operations**
5. **Make Suggestions During Cleanup**

### Table

<table>
<thead>
<tr>
<th>PID</th>
<th>Path</th>
<th>State</th>
<th>Local IP Address</th>
<th>Local Port</th>
<th>Remote IP Address</th>
<th>Remote Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>172</td>
<td>172.16.192.200</td>
<td>SYN_SENT</td>
<td>172.16.192.200</td>
<td>51287</td>
<td>172.16.192.41</td>
<td>12401</td>
<td>TCP</td>
</tr>
<tr>
<td>172</td>
<td>172.16.192.200</td>
<td>SYN_SENT</td>
<td>172.16.192.200</td>
<td>51288</td>
<td>172.16.192.88</td>
<td>44818</td>
<td>TCP</td>
</tr>
<tr>
<td>172</td>
<td>172.16.192.200</td>
<td>SYN_SENT</td>
<td>172.16.192.200</td>
<td>51288</td>
<td>172.16.192.88</td>
<td>44818</td>
<td>TCP</td>
</tr>
</tbody>
</table>
Threat and Environment Manipulation

De-Conflict

Timely Malware Analysis

Architecture Recommendations

### 2.b) bddd4e2b84.exe - File Activities

**Files Created:**
- C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\~tracedscn.yls

**Files Modified:**
- C:\DOCUME~1\ADMINI~1\Device\Afd\Endpoint
- C:\DOCUME~1\ADMINI~1\Device\RasAcd

**File System Control Commands:**

<table>
<thead>
<tr>
<th>Command</th>
<th>File System Control Command</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device\KsecDD</td>
<td></td>
<td>0x00390008</td>
</tr>
<tr>
<td>Device\RasAcd</td>
<td></td>
<td>0x00F14014</td>
</tr>
<tr>
<td>Device\Afd\Endpoint</td>
<td>AFD_GET_INFO</td>
<td>2</td>
</tr>
<tr>
<td>Device\Afd\Endpoint</td>
<td>AFD_SET_CONTEXT</td>
<td>60</td>
</tr>
<tr>
<td>Device\Afd\Endpoint</td>
<td>AFD_BIND</td>
<td>30</td>
</tr>
<tr>
<td>Device\Afd\Endpoint</td>
<td>AFD_GET_TDI_HAND</td>
<td>80</td>
</tr>
<tr>
<td>Device\Afd\Endpoint</td>
<td>AFD_CONNECT</td>
<td>30</td>
</tr>
</tbody>
</table>
IOCs and TTPs reflecting "tracedscn.yls", OPC, and ICS protocol scanning led to identifying compromised organizations.
Observable Steps to an ICS Attack [HAVEX]

**STAGE 1 - Intrusion**

- Reconnaissance
- Weaponization
- Targeting
- Delivery
- Exploit
- Install / Modify
- C2
- Act

**STAGE 2 – ICS Attack**

- Develop
- Test
- Deliver
- Install / Modify
- Execute ICS Attack

Attack with Impact
The Ukraine Attack

LITTLE BOBBY
I HEARD THERE WAS AN ATTACK IN UKRAINE ON THE POWER GRID!

YES--A CYBER ATTACK THAT ACTUALLY CAUSED A POWER OUTAGE.

GOOD THING THAT CAN'T HAPPEN HERE!

THE IMPACT WOULD BE DIFFERENT--BUT IT CAN DEFINITELY HAPPEN HERE.

NOT IF I CHOOSE TO BELIEVE IT CAN'T!

THAT'S NOT HOW REALITY WORKS.

by Robert M. Lee and Jeff Haas
Active Cyber Defense Cycle
• Identify an Indicator of Compromise (IOC) from iSight
• Search in your network
NSM -> Incident Response (IR)

- Incident responders identifying the infected system collect samples in tools such as Redline or FTK.

Searching for pieces of malware that use the same C2 can sometimes reveal additional variants and indicators.

- In this case the 64[.]4[.]10[.]33 IP address led to another BE2 sample which also used 46[.]165[.]222[.]6.
• Malware analysis can reveal additional indicators of compromise
• Collecting internal intrusion data from the various teams gives better threat insight

• Threat Intelligence Consumption personnel can share to learn and help others
Observable Steps to an ICS Attack [BE3]

**STAGE 1 - Intrusion**
- Reconnaissance
- Weaponization
- Targeting
- Delivery
- Exploit
- Install / Modify
- C2
- Act

**STAGE 2 – ICS Attack**
- Develop
- Test
- Deliver
- Install / Modify
- Execute ICS Attack

**Observable Steps**

**External Network Hosts** (Business or Plant Network)

**DMZ Applications**

**Supervisory Control Elements** (Network, Applications, Servers)

**Control Elements** (PLCs, RTUs, SIS)

**Sensors & Actuators**

**IO**

**Fieldbus using Industrial Protocols**
- Integrated Attack
- Highly Coordinated
- Logistic Sophistication
- Used Tools to Enable
- 6+ Months in the Environment
Takeaways

**LITTLE BOBBY**

**IS IT UNFAIR THAT CHINA ALWAYS GETS BLAMED FOR COMPUTER BREACHES?**

**YES -- OTHER COUNTRIES DO THE SAME OR SIMILAR ACTIVITIES. WE HAVE TO KEEP AN OPEN MIND AND REMAIN CRITICAL OF THE EVIDENCE.**

**OKAY, SO WHICH COUNTRY IS MOSTLY RESPONSIBLE THEN?**

**CHINA.**

*by Robert M. Lee and Jeff Haas*
What I Want You To Do After the Conference

Strategic Players
- Communicate about Real Threats and Impact
- Set the Culture
- Demand Value Add

Operational Players
- Empower Your People
- Get them Trained
- Developer Partnerships

Tactical Players
- Infrastructure Preparation
- Baseline the Environment
- Start Monitoring the Environment
Questions?

Visit us at SANS ICS to keep up with our latest research, classes, and more:
http://ics.sans.org/

Keep in Touch with the Community with the SANS ICS Alumni Email Distro:
https://lists.sans.org/mailman/listinfo/