When Your OT Support... Supports the APT :(  

Jake Williams  
Rendition Infosec  
www.rsec.us  
@MalwareJake
$whoami

- Founder and President of Rendition Infosec
- IANS Faculty
- Rally Security Co-Host
- SANS Senior Instructor and Course Author
- Former NSA hacker, Master CNE operator, recipient of the DoD Exception Civilian Service Medal
- **Dislikes:** those who call themselves “thought leaders,” “crypto bros,” and anyone who **needlessly adds blockchain** to a software solution
• What is OT really anyway?
• Remote Administration – Do we need it?
• OT Security Models
• Remote Support Software
• OT Compromise Case Studies
• Takeaways
What’s considered Operational Technology (OT)?

We’re talking about WAY more than just utilities here...
We all know what IT is, but when does IT cross the line into OT?

Operational Technology (OT) – the hardware and software dedicated to detecting or causing changes in physical processes through direct monitoring and/or control of physical devices such as valves, pumps, etc. (Wikipedia)

If a computer has an impact on the operation or monitoring of a physical device or process, then it’s OT
Where do we find OT?

• A few places we find OT include:
  – Assembly lines
  – Healthcare
  – Utilities
  – Chemical manufacturing
  – Transportation
  – Scientific instruments (e.g. laboratories)

• OT is so much more than just utilities
  – Much of your daily life is controlled behind the scenes by OT
When you get an MRI, there’s a computer that controls the sled moving you in and out of the apparatus.

If a patient needs to be removed quickly (e.g. heart attack) and the controller isn’t sending the appropriate commands, valuable time can be lost with a manual extraction.
OT Examples (2)

- Increasingly, robotic instruments are used for manufacturing

- An out of control robotic arm can harm people nearby by exceeding the design limitations

- Even if safety controls keep the device from harming humans, malfunctioning OT can cause a line stoppage or substandard product
OT Examples (3)

• Optical scanners, weight, and size sensors may are used to sort goods to their appropriate destination by controlling a sorting conveyor.

• Inappropriate controls may cause damage to parcels and financial loss due to late or expired goods.
We don’t like to think about it, but drugs and other chemicals are regularly tested on animals.

The tests and data collection are regulated by OT devices.

An OT service interruption invalidates the test, meaning these animals are killed for absolutely no gain.
Could we just do it ourselves?

Who better to administer the device than the manufacturer?
Why 100% vendor support?

• We are very unlikely to be able to correctly configure and administer highly specialized equipment

• The equipment may be leased
  – You touch, you break, you buy...

• Configuration options are often undocumented
  – And contracts may prohibit reverse engineering the software

• Software patches need to be deployed
  – Don’t just think security, patches are often needed to deal with operational issues as well
The OT security paradox

• Security would prefer to install all of our endpoint security controls on the OT device/controller
  – That’s often not allowed by the vendor
  – Hardware is usually spec’d to the exact requirements needed to run the controller software

• There’s not room to add a few more security agents

• Ever been working when the EDR does an IOC sweep?
  – Sometimes my GUI gets choppy
  – Imagine the impact if that GUI is a robotic welding arm...
Most orgs we work with that have OT devices have multiple different vendors and models
– In most cases, deploying a field tech for every checkup or software update is simply impractical

Corporate firewalls prevent simply listening on a port for connections from remote support
– This makes remote support programs like TeamViewer useful
– Because they call out through the firewall, eliminating the need for firewall changes
OT Security Models

Yes, we need to threat model OT too...
Do OT devices get patches?

• Unfortunately, many OT devices don’t receive regular operating system patches
  – If they receive any at all...

• Very often, we see OT devices being run on obsolete operating systems with publicly known vulnerabilities
  – Attackers know that OT is a target rich environment
Good ICS security demands the logical network segmentation between Information Technology (IT) and Operational Technology (OT) networks. Separation can be performed using:

- Air gaps (no connection between networks)
- Firewalls
- Cross domain solutions

When architecting security, think prevention AND detection!
Separation: Air Gap

- “Air gap” is a physical separation between networks
- These are often touted as the most secure option
- In my experience air gap networks:
  - Often aren’t really separated
  - Are poorly patched and poorly monitored
- There’s no monitoring choke point in this architecture, making it less than ideal for hunt operations
- Ed Skoudis famously said “There’s no such thing as an air gapped network. At best they all just end up being really high latency.”
• Using firewalls to separate IT and OT is a good start, but it doesn’t offer a true separation
  – Most firewalls can’t inspect encrypted data
  – Most firewalls decode (at most) a limited number of protocols
• Firewalls do offer an ideal choke point where events can be logged and used to hunt
  – Hunt operations are however limited to the usefulness of logs, which due to limitations noted above are often incomplete
A cross domain solution that understands protocols used in the operational environment is the ideal architecture for security.

- Because logs are richer in nature, this solution is also the most useful for hunting.

Attackers wishing to compromise OT networks with true separation MUST transit the cross domain solution.

- This makes the cross domain solution an ideal monitoring point.
- All logs are not created equally - the cross domain solution logs are extremely high value.
So what gets used?

- The case for remote vendor support is well established
  - The separation methodology must work with remote support constraints

- Air gap – removes the possibility of remote support

  - **Firewall** – as long as a few ports (usually just DNS and HTTPS) are allowed, remote support works fine

- Cross domain solution (e.g. smart diode) – As long as the diode vendor handles the remote support solution, all is well
  - Unfortunately, different vendors use different programs and diode vendors have trouble keeping pace with external software changes
Who needs protection from who?

OT Environment

- Windows 2000
- Solaris 8
- Linux 2.6
- OpenVMS (Alpha)
- Windows XP
- Windows 7

IT Environment

- Windows 2000
- Solaris 8
- Linux 2.6
- OpenVMS (Alpha)
- Windows XP
- Windows 7
- Windows Server 2019
- Linux 4.14
- Windows 10
- Windows Server 2016
- Windows 10
- Windows 10

Many operational models all most (or all) traffic out of the OT environment while limiting what traffic can ingress.
Remote support compromise target?

• OT security is about more than availability and integrity

• OT equipment may be used to pivot to the IT network to compromise confidentiality
  – OT devices may themselves have valuable intelligence data
Remote Support Software

It’s FAR more than just TeamViewer...
Features attackers love

• Most remote support software supports:
  – Chat functionality with the victim (rarely needed)
  – Full remote keyboard and mouse control
  – File transfer in both directions (malware in, data exfil out)
  – Full encryption support (a few use certificate pinning)

• The encryption support is particularly difficult for data diodes that now can’t see what’s being transferred
TeamViewer

- Allows file transfer and remote control
- Attackers use this in phishing attacks due to the availability of (nearly) unlimited use free trials
- Some organizations have moved from TeamViewer due to cost, but it continues to be a favorite of attackers due to flexibility
LogMeIn Rescue

• Unlike regular LogMeIn, this doesn’t require an install and can simply run from a portable application
GoToAssist

• A few customers have assets managed using GoToAssist
• The most often cited reasons from vendors are:
  – Service desk integration
  – Mobile device interfaces
OT Remote Compromise Case Studies

The names have been changed (because lawyers...)
Case Study: Surgical Center

- **Victim**: Surgical center with 20+ locations
- **Initial OT Equipment Compromised**: Gas Spectrometer
- **Other OT assets impacted**: Yes
- **IT network breach**: Yes

- The attacker piggybacked on a legitimate support session
- This was a high security network, admins would only enable remote support when requested through email and verified with a callback
Case Study: Surgical Center (2)

• Each laboratory had a separate OT and IT network

• Site to site VPNs were relatively locked down and well instrumented, aiding in detection and investigation
  – Physical disconnection of sites created the choke points that led to relatively early detection

• All threat modeling had been performed assuming IT would breach OT, not the other way around
Case Study: Manufacturing

- **Victim**: Heavy machinery manufacturer
- **Initial OT Equipment Compromised**: Vending machine for small parts and hand tools
- **Other OT assets impacted**: Yes
- **IT network breach**: No

- The attacker compromised the vendor, who had an the ability to connect to remote devices whenever needed
- There was no legitimate support activity occurring at the time the attacker took control of the device
Case Study: Manufacturing (2)

• The attacker deployed the AES-NI ransomware, which was configured with ETERNALBLUE

• Once a few machines inside the OT network were compromised, the scanning activity (plus line stoppages) led IT to quickly sever the IT/OT connection

• We don’t assess the attacker realized they were in an OT environment – probably just looking for a payday
Case Study: Chemical Processing

• **Victim**: Chemical Processing Plant
• **Initial OT Equipment Compromised**: Mixer/Extruder
• **Other OT assets impacted**: Yes
• **IT network breach**: Yes

• The attacker piggybacked on a legitimate support session, delivering a RAT (Remote Administration Tool) to the HMI (Human Machine Interface)
Case Study: Chemical Processing (2)

- The attacker pivoted to the IT network using an SMB server with weak security
  - Poor security settings were required due to legacy OT devices connecting to it
- The attacker laterally moved off the file server to a server that sits only in the IT network and set off alerts for application whitelisting
  - The attacker (probably?) assumed that lax security found in the OT environment would permeate into the IT environment
Conclusion

Takeaways!
Need MOAR takeaways!
1. Remote support isn’t going away anytime soon (and that hurts me to say as a security professional)

2. You’re only as secure as your remote support

3. Threat model the OT network targeting the IT network

4. Instrument your OT environment – there’s less variation of traffic in OT than IT, attacks are easier to discover if you listen
5. Create choke points for traversal from OT to IT
   – This is your BEST opportunity to find a supply chain compromise from remote support

6. Consider dedicated Internet (with monitoring) for OT remote support – allows restricting any IT/OT connection further

7. Segmentation **within** OT networks is crucial, particularly for unsupported operating systems

8. I don’t have the answer
   But I’m 100% positive it isn’t **blockchain**
Questions?

Jake Williams
Rendition Infosec
@malwareJake
rsec.us