STERLING
INFORMATION TECHNOLOGIES INC

University of Windsor
School of Computer Science

Mapping a Target

Attacker's Perspective

Presented by: Nathan Serre
Date: January 21, 2026

Operation Absolute Resolve

- Full Disclosure: Most details are classified
- This is a speculative reconstruction
- The ideas and methodology presented here are based on public reports where possible
- Where facts regarding this specific case end we fill those gaps with knowledge about similar attacks

Operation Absolute Resolve

- On January 3rd this year the US government launched an invasive strike on the capital of Venezuela, Caracas
- “The lights of Caracas were largely turned off due to a certain expertise that we have”
- This quote along with public reports from Caracas at the time of the attack heavily point to a cyber attack by the US government

GLOSSARY

- ICS (Industrial Control System)
- SCADA (Supervisory Control and Data Transmission)
- PLC (Programmable Logic Controller)
- OT (Operational Technology)
- IT (Information Technology)
- RTO (Regional Transmission Operator)

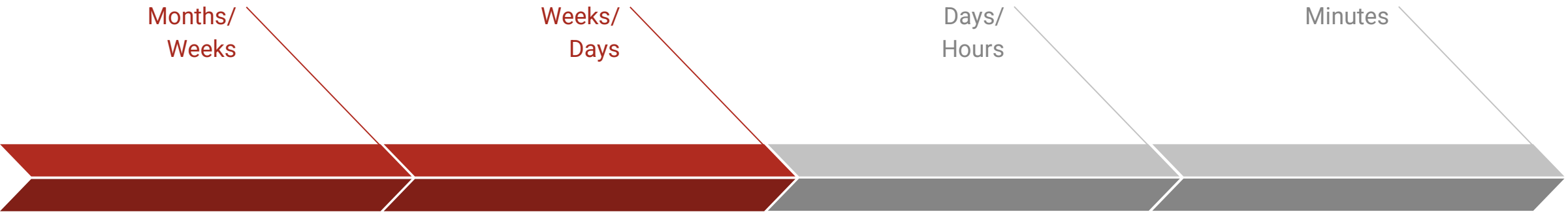
Red Team Targets

- Regional transmission operator overseeing multi-state load balancing
- Hybrid IT/OT environment with shared identity services
- Third-party vendors with remote access

Blue Team Defenses

- Segment systems whenever possible
- Do not use shared credentials across systems whenever possible
- Least privileges at all times
- Zero Trust No Access

TIMELINE



Reconnaissance & OSINT

Initial Access

IT -> OT Pivot

Grid Disruption

OSINT

- Open Source Intelligence
- What to look for in a human access point
- OT Network Engineer
- 10+ years ICS experience
- Vendor facing/Client facing responsibilities
- PLC and SCADA experience
- LinkedIn Profile Scraping

Comparable Infrastructure

- Ukrainian regional distribution grids (2015-2016)
- North American RTOs
- Publicly documented substation and control centers

Phase Defense: Recon & OSINT

- Avoid oversharing on LinkedIn
- Pay attention to profile scraping or unusual access patterns
- Limit public accessibility of grid topology documents

Initial Access

- Spear-Phishing
- Social Engineering
- Messages are made to require action (Urgency and familiarity)
- Used to gain access through valid credentials
- Hybrid IT/OT targets

Phase Defense: Initial Access

- Educate employees on cybersecurity
- Do not trust emails, links, QR codes
- Every file contains potential malware
- “Success breeds complacency. Complacency breeds failure. Only the paranoid survive.” - Andy Grove
- Enforce Multi Factor Authentication for remote access
- Heavily restrict third party and vendor access

Living off the land

- Use only what is at your disposal
- Native admin tools
- Downloads attract attention
- Malware attracts attention
- Observation and persistence

RED TEAM OPSEC: LOTL

- Avoid noisy tools
- Blend with normal admin activity
- Minimize contact with OT until final phases

Blue Team Defense: LOTL

- Compare activity with baseline administrative behavior
- Watch for unusual use of native tools (PowerShell, WMI)
- Apply least privileges to IT admins

IT -> OT Pivot

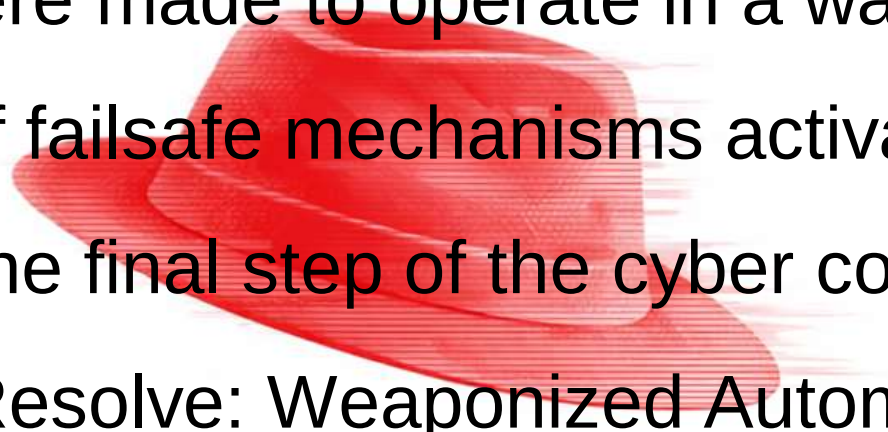
- Making the jump from IT to OT using shared credentials
- Shared network resources between IT and OT
- IT administrative access
- Abusing SCADA software to map out grid topology and PLC behavior

Phase Defense: IT -> OT Pivot

- Enforce network segmentation
- Alerts on abnormal authentication attempts
- Block direct IT -> OT administrative access
- Logs and reports on OT asset scans
- Treat all remote desktops as high risk
- All IT access to OT assets should be heavily monitored and controlled

GRID DISRUPTION

- Attackers used existing architecture to trigger an automated shutdown
- System failsafes were mapped thoroughly
- System were made to operate in a way that would trigger a cascade of failsafe mechanisms activating
- This was the final step of the cyber component of Operation Absolute Resolve: Weaponized Automation



Phase Defense: Grid disruption

- Critical actions such as automated shutdowns and fail safe mechanisms require human validation
- System monitoring for abnormal commands
- Regular training on OT response drills

Conclusion

- Every phase exploited things systems administrators take for granted
- Public Information
- Trusted Users
- Admin tools
- Network Convenience
- Automated protections
- These are architectural failures, not technical

QUESTIONS

- What defensive measure would most effectively have prevented initial access?
- Why did the attackers not choose to attack OT systems directly?
- Why did the attack not aim to cause lasting damage like the 2015 Russia power grids attacks on Ukraine?

Thank You!