

The Worst ICS/OT Cybersecurity Love Story

Mike Holcomb

Disclaimer

- ❑ The information provided in this presentation is for educational purposes only.
- ❑ All knowledge obtained must be used for legitimate, authorized purposes.
- ❑ The views written and discussed in this course are those of the presenter and not that of their employers or other affiliated organizations.

© 2025 Mike Holcomb

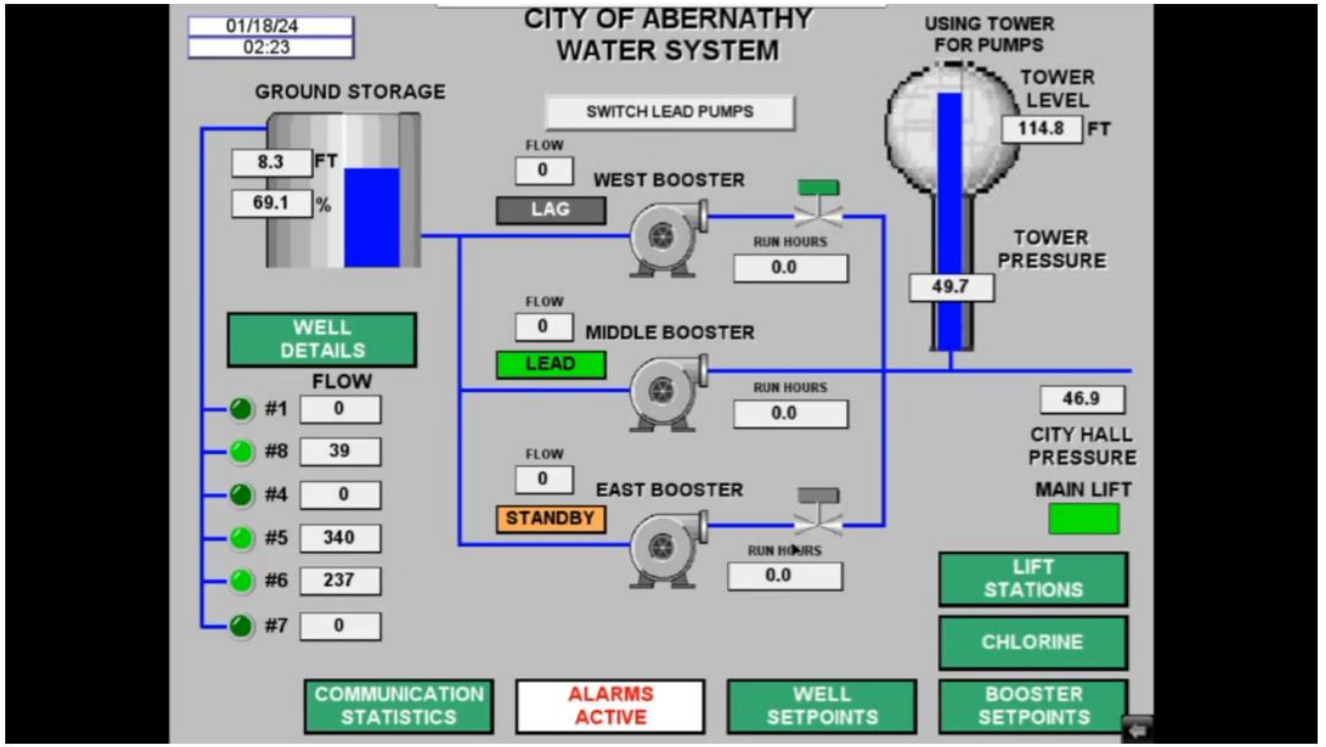
About Mike



- Fellow for Cyber Security at Fluor
- ICS/OT Cybersecurity Global Lead
- Founder of BSidesICS and BSidesGreenville
- CISSP, GRID, GICSP, ISA 62443, GPEN, GCIH, etc.
- Master's degree from SANS Technology Institute
- Posts on LinkedIn and YouTube on OT/ICS Cybersecurity

Agenda

- ❑ The Greatest ICS/OT Cybersecurity Love Story
- ❑ Findings from Dragos' Year in Review Report
- ❑ State Adversaries & Hacktivists Converge
- ❑ Why Does It Matter?



A screen recording shows Cyber Army of Russian Reborn clicking buttons on the interface of a water utility in Texas. CYBER ARMY OF RUSSIA REBORN VIA TELEGRAM

Source: https://www.wired.com/story/cyber-army-of-russia-reborn-sandworm-us-cyberattacks/

© 2025 Mike Holcomb

The Greatest ICS/OT Cybersecurity Love Story



Source: https://editorial.rottentomatoes.com/article/hear-us-out-hackers-was-the-best-cyber-thriller-in-a-year-chock-full-of-them/

© 2025 Mike Holcomb

ICS/OT Threat Intel: Dragos' Year in Review Report

- ❑ Considered mandatory reading for those working in ICS/OT environments
- ❑ World leading ICS/OT cyber threat intelligence
- ❑ Provides real world insights along with practical tactics for defense



© 2025 Mike Holcomb

Findings from Dragos' Year in Review Report



↑ **87%**

Ransomware attacks against industrial organizations **increased 87 percent** over the previous year.



60%

Dragos tracked **60 percent more ransomware groups** impacting OT/ICS in 2024.



69%

of all ransomware attacks targeted **1,171 manufacturing entities** in **26 unique manufacturing subsectors**.

Source: Dragos 8th Annual Year in Review 2025 - OT/ICS Cybersecurity Report

© 2025 Mike Holcomb

Findings from Dragos' Year in Review Report (cont.)

65%

of sites Dragos assessed had insecure remote conditions. This includes insecure configurations, unpatched systems, and poor network architecture related to remote access appliances and applications.



45%

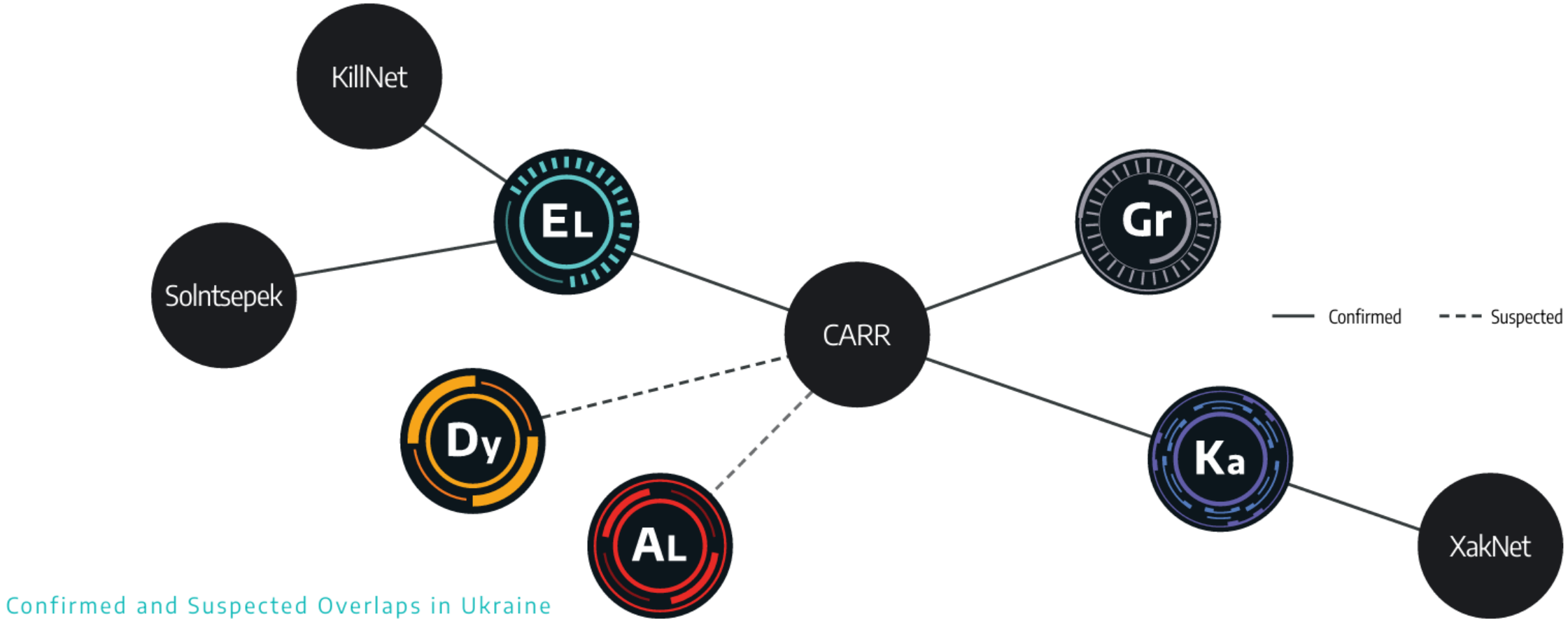
of OT Watch customers have SSH communicating to publicly routable addresses. Dragos penetration testers leverage existing SSH paths for general purpose encrypted communication including demonstrating C2 tunnels and proxies.

*A minor portion of these environments are untuned.

Source: Dragos 8th Annual Year in Review 2025 - OT/ICS Cybersecurity Report

© 2025 Mike Holcomb

State Adversaries & Hacktivists Converge



Confirmed and Suspected Overlaps in Ukraine

Source: Dragos 8th Annual Year in Review 2025 - OT/ICS Cybersecurity Report

© 2025 Mike Holcomb

State Adversaries & Hacktivists Converge

WHY Does It Matter?

© 2025 Mike Holcomb

State Adversaries & Hacktivists Converge

- State Adversaries
  - Low Volume / Low Visibility
  - High Impact Incidents
- Hacktivists
  - High Volume / High Visibility
  - Low Impact Incidents



© 2025 Mike Holcomb

KAMACITE

- ❑ “Technical overlaps” with ELECTRUM and Sandworm (APT44)
- ❑ Focuses on Phase 1 attacks to infiltrate IT networks and associated OT/ICS infrastructure
- ❑ Hands off initial OT/ICS network foothold to ELECTRUM
- ❑ Examples include CrashOverride (2016) which was responsible for the 2016 Ukrainian blackout
- ❑ Has targeted entities in the United States and the United Kingdom since as early as 2017



© 2025 Mike Holcomb

ELECTRUM

- ❑ “Technical overlaps” with KAMACITE and Sandworm (APT44)
- ❑ Focuses on Phase 2 attacks in OT/ICS infrastructure with initial access provided by KAMACITE
- ❑ Includes data wiping capabilities
- ❑ Evidence of using hacktivist groups as cover for cyber attacks
- ❑ Also has targeted entities in the United States and the United Kingdom



© 2025 Mike Holcomb

GRAPHITE

- ❑ New group first discovered by Dragos in 2024
- ❑ Aligns with APT28 (Russia's Fancy Bear)
- ❑ Like KAMACITE, focuses on Stage 1 attacks against IT infrastructure
- ❑ Has burned several zero-day attacks
- ❑ Known for targeting industrial organizations in Eastern Europe and the Middle East for credential harvesting

© 2025 Mike Holcomb

Cyber Army of Russia Reborn (CARR)

- ❑ One of the most prolific Russian hacktivists groups that appeared in 2022 with the Russian invasion of Ukraine
- ❑ Known for data leaks, DDoS attacks and targeting critical infrastructure
- ❑ Strongly suspected of being created by Sandworm (APT44) in support of Russia's GRU

© 2025 Mike Holcomb

KillNet & XakNet

- KillNet
  - Russia-aligned hacktivist group known for DDoS, website defacements and data leaks
  - Targets Ukraine and its allies, including NATO countries
  - Coordinated attacks with other Russian-aligned hacktivists groups
- XakNet
  - Russian-aligned hacktivist group known for strong political rhetoric
  - Primarily known for DDoS and data leaks

© 2025 Mike Holcomb

Solntsepek (Scorching Sun)

- Hacktivists with claim strong alignment with CARR
  - More aligned operationally with Russian state adversaries
- Known for targeting Ukrainian ISPs and data leaks against Ukraine and their allies
- Evidence demonstrates that some attacks were cover for Sandworm (APT44) activity
- Information warfare conducted over Telegram, social media and other disinformation channels

© 2025 Mike Holcomb

Why Does It Matter?

- ❑ Geopolitical considerations can no longer be removed from cybersecurity discussions
- ❑ We need to move beyond traditional threat models of OT/ICS adversaries
- ❑ Could hacktivist activity that's easy to detect be cover for more advanced attacks?
- ❑ Attribution still doesn't matter
  - ❑ But also matters at the same time

© 2025 Mike Holcomb

THANK YOU!

- Please don’t hesitate to reach out!

linkedin.com/in/mikeholcomb
mikeholcomb.com
mike@mikeholcomb.com
youtube.com/@utilsec
github.com/utilsec



Mike Holcomb
Helping YOU Secure ICS/OT

© 2025 Mike Holcomb