MAWAC-ENA WORKSHOP

PARIS

November
2025

Cybersecurity Practices in Water and Industrial Systems

Rigel Gjomemo
Research Scientist, DPI
Venkat Venkatakrishnan
Professor, University of Illinois at Chicago

Water Systems in the US

- 52,000 community water systems
- 16,000 wastewater systems
- Water industry is a Critical National Infrastructure (CNI)
- **Survey**: 15.8% of the systems experienced 1 to 4 IT cybersecurity incidents over 12 months. 4.7% reported 1 OT cybersecurity incident over 12 months.

Water Systems IT in the US : Issues

- Major challenges
  - Awareness of threats and best practices
  - IT and OT identification and remote access control
  - Lack of cybersecurity training and workforce
  - Economic disadvantages

- In sum, the national systems are in dire need of cybersecurity improvement capabilities

Cybersecurity Incidents

Ongoing Cyber Threats to U.S. Water and Wastewater Systems

Last Revised: October 25, 2021 **Alert Code:** AA21-287A

Federal agencies warn of ransomware targeting water, wastewater treatment plants

Published Oct. 18, 2021

Ransomware Hit SCADA Systems at 3 Water Facilities in U.S.

U.S. Warns of Attacks Targeting IT and OT Systems in Water Facilities

EPA Webinar on Recent Unitronics Programmable Logic Controllers Hacked at US Water and Wastewater Systems

THREAT ACTORS IN JANUARY ATTEMPTED TO POISON THE WATER AT A US FACILITY

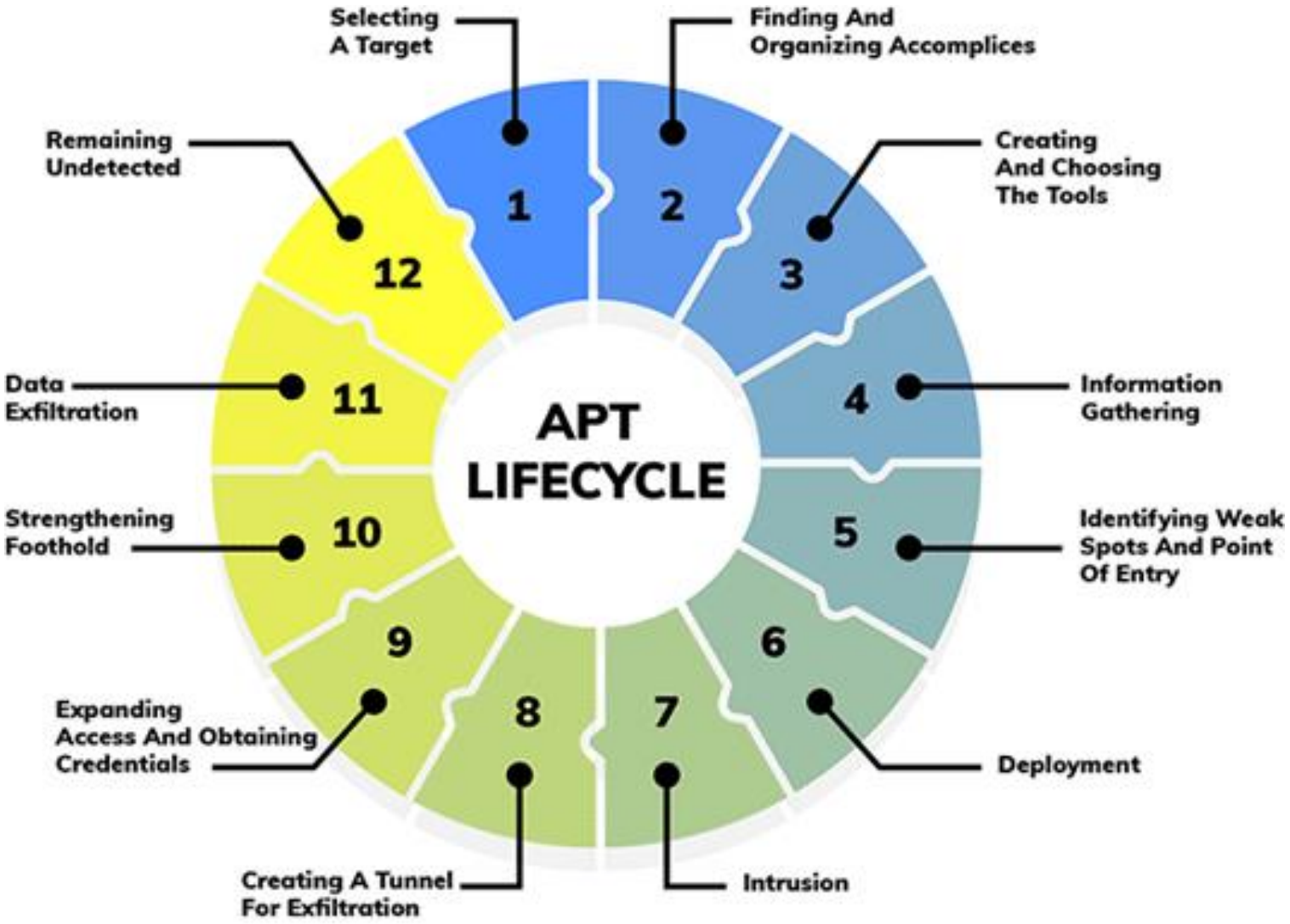
Pierluigi Paganini June 21, 2021

Kansas Man Pleads Guilty to Water Facility Tampering

Thursday, October 21, 2021

For Immediate Release

The lifecycle of a cyber-attack



ATT&CK Matrix

Our work: Cyber Threat Hunting

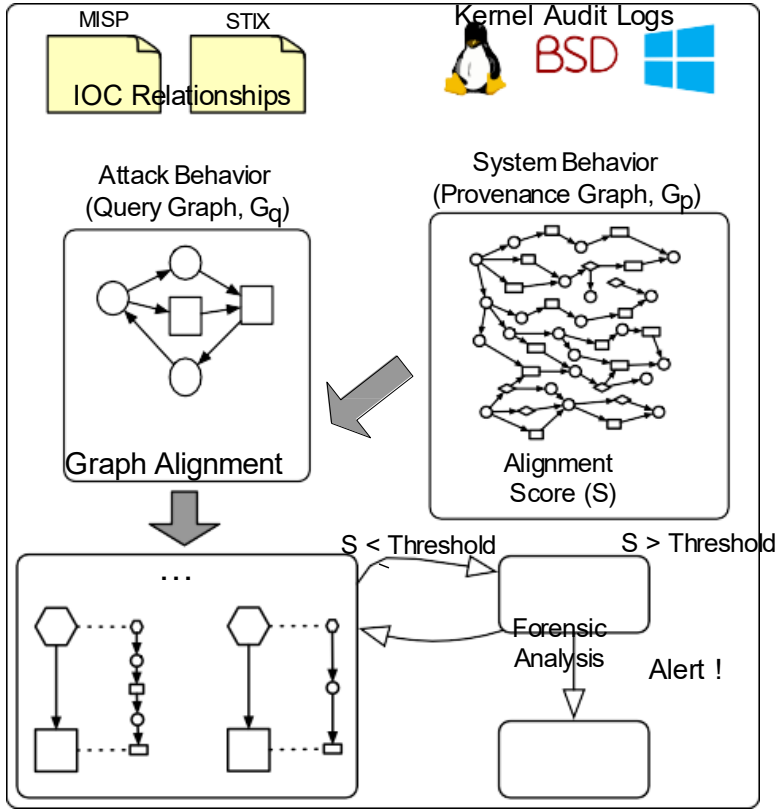
- Cybersecurity labs discover new threats
- The details released as Threat Intelligence Reports
  - Structured reports OpenIOC, STIX, MISP
  - Unstructured: Natural Language Description

    Enterprise question: Has my enterprise been the target of this threat?
- State of the art: Looking for fragmented Indicators of Compromise (IOC)
  - hash values, file/process names, IP addresses, domain names
  - Very fragile

Automate Approach to Threat-Hunting:

(USENIX 2017, IEEE S&P 2019, CCS 2019, ESORICS 22, ICICS 22)

- Modeling Threat Hunting as finding an embedding of a query graph in a much larger provenance graph
  - G_p: audit logs modeled as a graph
  - G_q: attack behavior modeled as a graph
  - Both labeled, typed, and directed
  - Inexact matching



Call for Action

- Pilot cyber-threat hunting project
  - Partner with utilities on cybersecurity
- We have the ”pilot ready” solution
- Need operational environment partner for pilot
- Next stage to be pitched to US federal funding (DARPA, NSF, DOE)

Thank you for your attention

NAME : Venkat Venkatakrishnan

INSTITUTION : University of Illinois at Chicago

MEGACITY : Chicago

MAWAC- ENA PARIS
2025