



MAWAC-ENA WORKSHOP

PARIS

November
2025





Cybersecurity Practices in Water and Industrial Systems

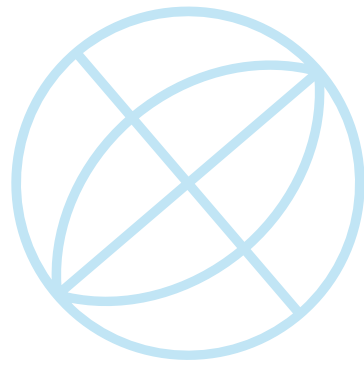
Rigel Gjomemo

Research Scientist, DPI

Venkat Venkatakrishnan

Professor, University of Illinois at Chicago

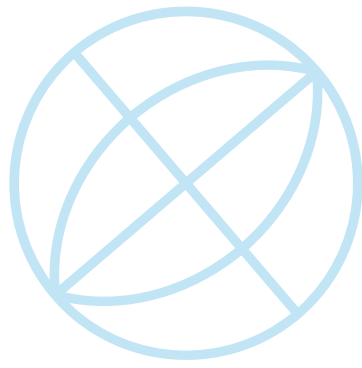
Water Systems in the US



- 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.



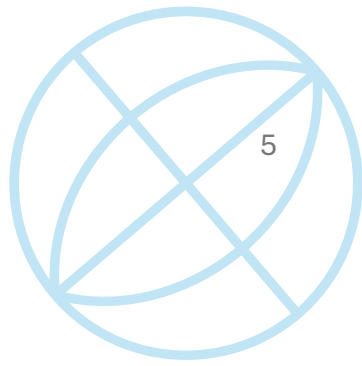
Water Systems IT in the US : Issues



- 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

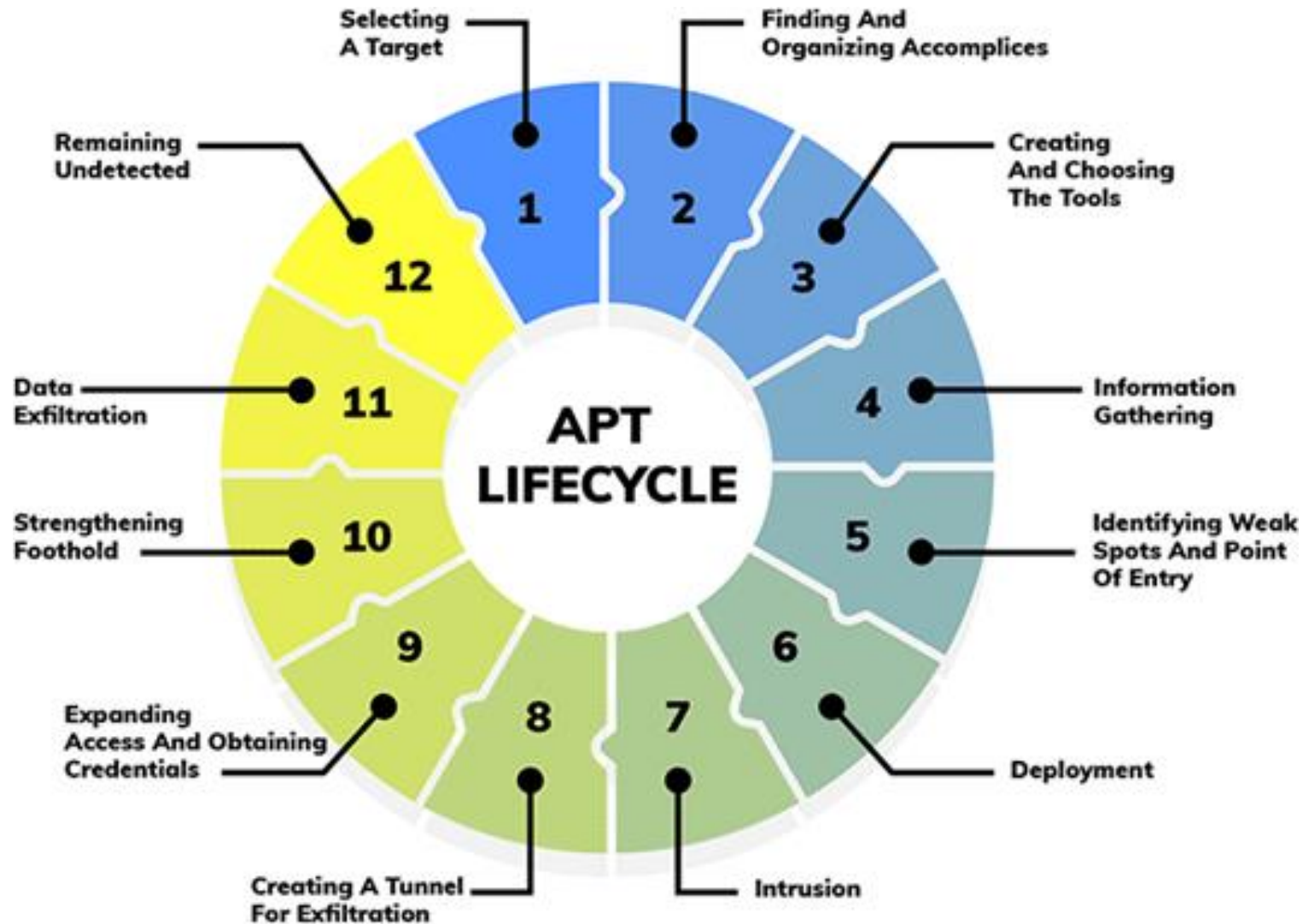
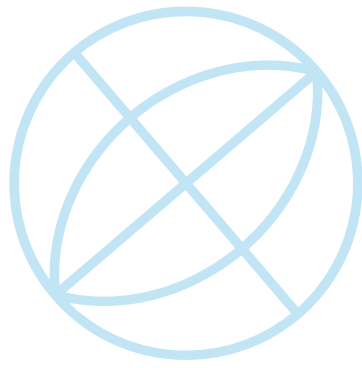
👤 Pierluigi Paganini 🕒 June 21, 2021

Kansas Man Pleads Guilty to Water Facility Tampering

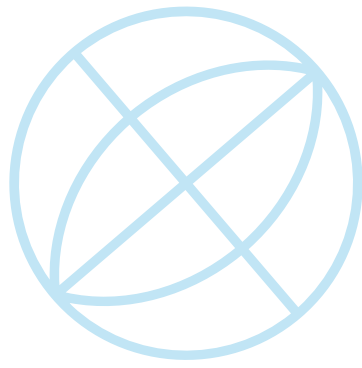
Thursday, October 21, 2021

For Immediate Release

The lifecycle of a cyber-attack



Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	7 techniques	9 techniques	12 techniques	19 techniques	13 techniques	39 techniques	15 techniques	27 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Active Scanning (2)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administrative Command	BITS Jobs	Access Token Manipulation (3)	Access Token Manipulation (3)	Credentials from Password Stores (3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (8)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (8)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (3)	Boot or Logon Initialization Scripts (3)	Build Image on Host	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Clipboard Data	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (1)	Browser Extensions	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Dashboard	Remote Services (6)	Data from Cloud Storage Object	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (8)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (2)	Deploy Container	Input Capture (4)	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository (2)	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (7)	Create Account (3)	Execution Guardrails (1)	Direct Volume Access	Man-in-the-Middle (2)	Container and Resource Discovery	Software Deployment Tools	Data from Information Repositories (2)	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Search Open Technical Databases (3)		Trusted Relationship	Shared Modules	Create or Modify System Process (4)	Event Triggered Execution (15)	Domain Policy Modification (2)	Modify Authentication Process (4)	Domain Trust Discovery	Taint Shared Content	Data from Local System	Ingress Tool Transfer	Exfiltration Over Other Network Medium (1)	Firmware Corruption
Search Open Websites/Domains (2)		Valid Accounts (4)	Software Deployment Tools	Event Triggered Execution (15)	Event Triggered Execution (15)	Execution Guardrails (1)	Network Sniffing	File and Directory Discovery	Use Alternate Authentication Material (4)	Data from Network Shared Drive	Multi-Stage Channels	Exfiltration Over Web Service (2)	Inhibit System Recovery
Search Victim-Owned Websites			System Services (2)	External Remote Services	Exploitation for Privilege Escalation	File and Directory Permissions Modification (2)	OS Credential Dumping (8)	Network Service Scanning		Data from Removable Media	Non-Application Layer Protocol	Scheduled Transfer	Resource Hijacking
			User Execution (3)	Hijack Execution Flow (11)	Hijack Execution Flow (11)	Hide Artifacts (7)	Steal Application Access Token	Network Share Discovery		Proxy (4)	Remote Access Software	Transfer Data to Cloud Account	Service Stop
			Windows Management Instrumentation	Process Injection (11)	Process Injection (11)	Impair Defenses (7)	Steal or Forge Kerberos Tickets (4)	Password Policy Discovery		Screen Capture	Traffic Signaling (1)	System Shutdown/Reboot	
				Scheduled Task/Job (7)	Scheduled Task/Job (7)	Indicate Removal on Host (8)	Steal Web Session Cookie	Peripheral Device Discovery		Video Capture	Web Service (3)		
				Valid Accounts (4)	Valid Accounts (4)	Indirect Command Execution	Two-Factor Authentication Interception	Permission Groups Discovery (3)					
							Unsecured Credentials (7)	Process Discovery					
								Query Registry					
								Remote System Discovery					
								Software Discovery (1)					
								System Information Discovery					
								System Location Discovery					
								System Network Configuration Discovery (1)					
								System Network Connections Discovery					
								System Owner/User Discovery					
								System Service Discovery					
								System Time Discovery					
								Virtualization/Sandbox					



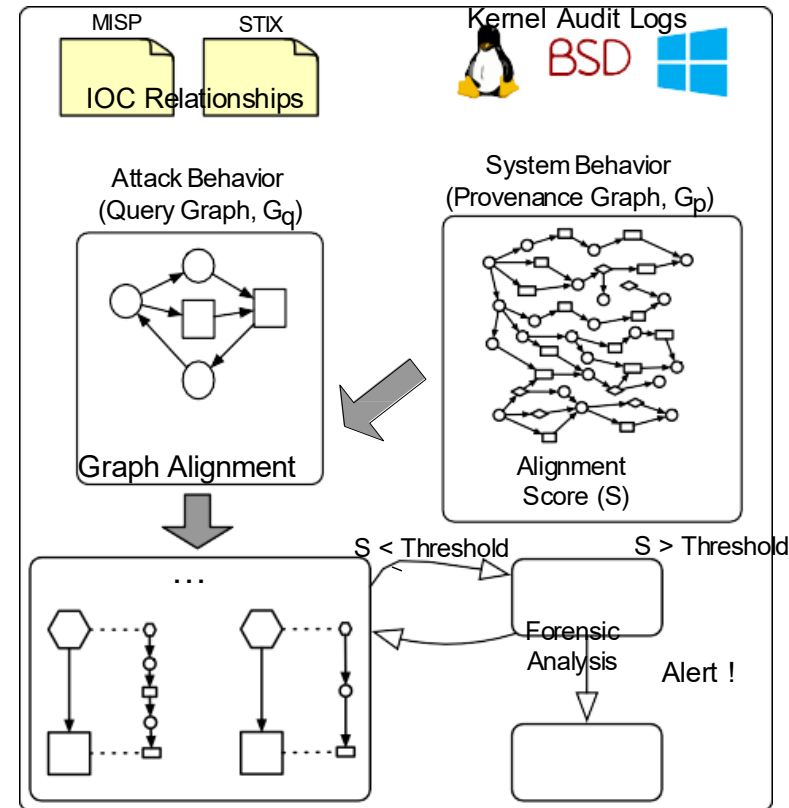
Our work: Cyber Threat Hunting

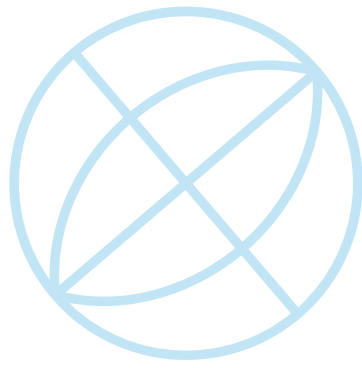
- Cybersecurity labs discover new threats
- The details released as Threat Intelligence Reports
 - Structured reports OpenIOC, STIX, MISP
 - Unstructured: Natural Language Description
- *Enterprise question:* Has my enterprise been the target of this threat?
- State of the art: Looking for fragmented 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



Métropole
du Grand Paris



SEINE
GRANDS
LACS



AGENCE
eau
seine
NORMANDIE



Water Security Management
Assessment, Research & Technology

MAWAC- ENA PARIS 2025

