TLP: CLEAR

UNIFIED THREAT ADVISORY

Iran-linked hackers access U.S Water Utilities East Coast

2026-04-10T01:35:42.106Z

RANSOM-ISAC [DEFUSED] detections.ai

Introduction

The Unified Threat Advisory is a coordinated Cyber Intelligence effort co-authored by **Ransom-ISAC** *an Information Sharing and Analysis Center dedicated to emerging ransomware analysis, collective defense strategies, and global threat intelligence sharing.* **Defused** *a sophisticated cyber deception platform detecting early warning emerging threats such as 0/N-day vulnerabilities, and* **Detections.ai** *a community driven platform for sharing high-fidelity detection rules across integrated environments.*

Overview

The **Unified Threat Advisory** *group is dessiminating details regarding* **Iran-linked hackers** *tied to the ongoing conflicts in the Middle East Theatre and previous actors from Pro-Russian groups attempting to target and compromise small* **U.S based water utilities** *located on the East Coast. The attackers compromised small flushing pumps attached to water hydrants or tap into mains used for maintaining water quaility from underground water distribution system via* **Eclipse 9800i series** *tampered the PLC for maintaining the Chlorine residual levels known as* ***Intelligent Monitoring and Flushing station.***

*In addition, we are sharing technical details regarding a sophisticated and malicious Python-based Graphical User Interface (GUI) Industrial Control System (ICS) reconaissance and data exfiltration tool known as "***TRK25-ADVANCED***" - a similar functionality to a previous predecessor* **Kurtlar_SCADA.exe** *used by the groups such as Z-Pentest and* **CAR - Cyber Army of Russia** *allied with Pro-Palestine groups during the Israel-HAMAS conflict taught to enumerate and hack into exposed industrial control systems.*

Technical Details

The **TRK25-ADVANCED** *is an advanced Industrial Control System (ICS) reconaissance and data exfiltratration tool powered with a Graphical User Interface (GU) based on* **PyQt5**. *Successor to the widely used* **Kurtlar_SCADA.exe** *with over* **900+** *lines of Python code which begins by actively scanning pre-defined hardcoded network blocks from Russia, Ukraine, Germany, USA, and China. It utilizes a dictionary of ICS/SCADA ports via industrial_ports function including* **VNC, RDP, SSH**. *Once a host is discovered the code uses a risk scoring system labeling* **SCADA 90 points**, *Siemens S7 95 points, Modbus 80. After successfully* **banner grabbing** *live hosts it then activates a class called* **"Automatic Vulnerability exploitation"** *which automates low-hanging fruits such as the hardcoded default credentials in code listed below as indicators. Once exploited the tool installs* **persistence** *via dataexfiltration and exfiltration_package, where it aggregates HMI Operator screenshots, fingerprints IP, country, ports, and system classification into a JSON transmitted via* ***Base-64 encoded*** *format.*

Indicators & C2 domains

cd261f739ad950bacadd8ce66bb31672c91cb708cde977b48f24b9666afaac16 **Infrastructure Destruction Squad.py**
61219ea5cd69fb4fbf20cb304673cecfd42d2251aa3b4c7e6f6b36a52ba9013e **kurtlar.exe**
1b39f9b2b96a6586c4a11ab2fdbff8fdf16ba5a0ac7603149023d73f33b84498 **iocontrol malware**
'password', '123456', 'admin', 'root', '1234', default','operator', 'user','guest','scada', 'plc','hmi','control','factory',industrial'