Threat Activity Alert: English-Speaking Group 'Force Electronic Quds' Claims Hacking of Water System and Thermal Pump in Israel

Cyber Crime (CC)

Critical Infrastructure (CI)

Fusion (FS)

Hacktivism (HK)

November 30, 2022 08:32:07 AM, 22-00026526, Version: 1

Executive Summary

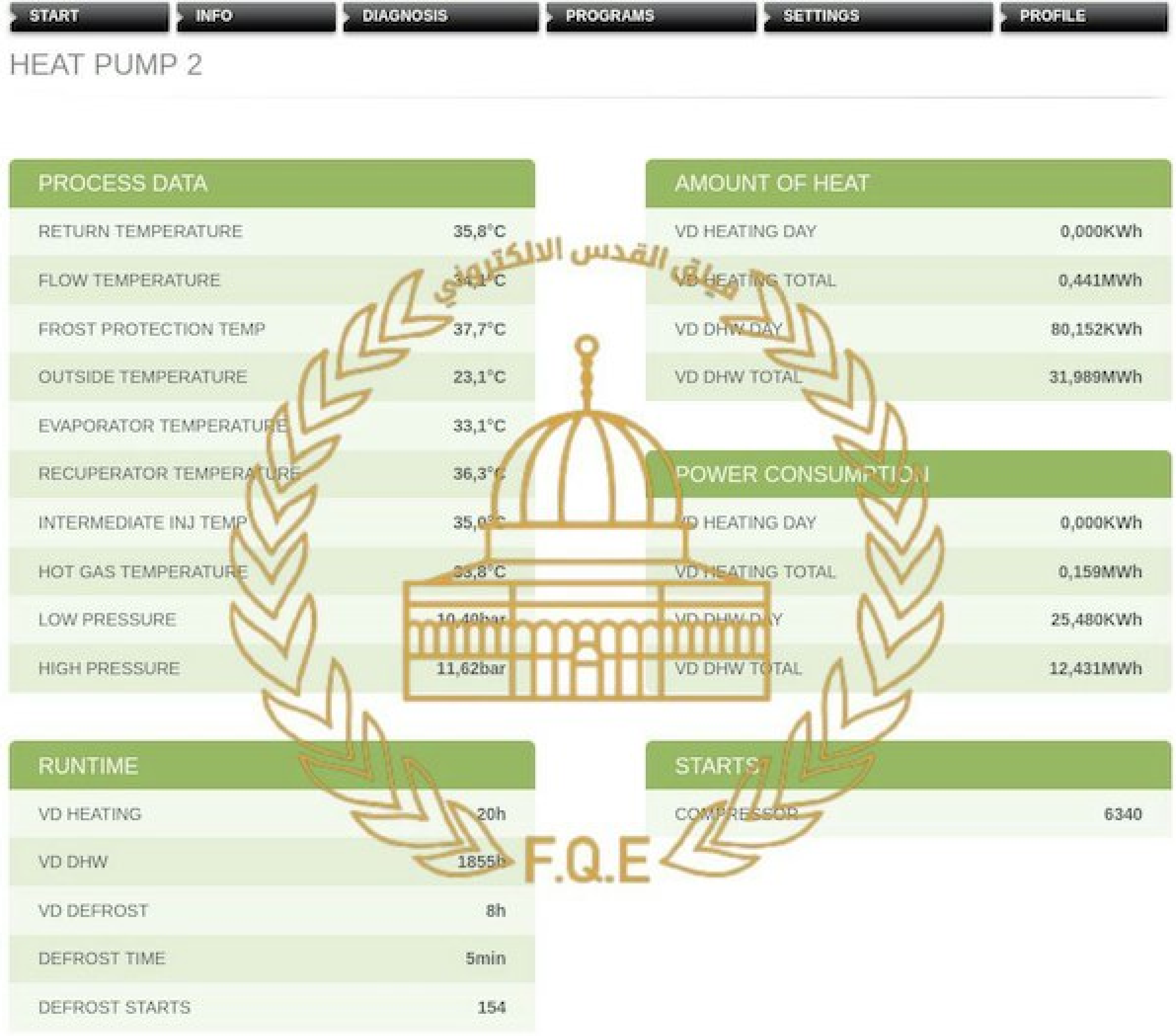
Threat Activity Alerts relay immediate observations of notable activities within the cyber threat environment. Activities continue to be monitored and may result in additional alerts or reports if anything significant occurs, or the issue warrants further analysis.

Threat Detail

Date: Sep. 4, 2022

Source: Telegram. Force Electronic Quds's Telegram channel.

Sep. 4 - Actor: Force Electronic Quds



HEAT PUMP 2

PROCESS DATA	
RETURN TEMPERATURE	35,8°C
FLOW TEMPERATURE	34,1°C
FROST PROTECTION TEMP	37,7°C
OUTSIDE TEMPERATURE	23,1°C
EVAPORATOR TEMPERATURE	33,1°C
RECUPERATOR TEMPERATURE	36,3°C
INTERMEDIATE INJ TEMP	35,0°C
HOT GAS TEMPERATURE	33,8°C
LOW PRESSURE	10,40bar
HIGH PRESSURE	11,62bar

AMOUNT OF HEAT	
VD HEATING DAY	0,000KWh
VD HEATING TOTAL	0,441MWh
VD DHW DAY	80,152KWh
VD DHW TOTAL	31,989MWh

POWER CONSUMPTION	
VD HEATING DAY	0,000KWh
VD HEATING TOTAL	0,159MWh
VD DHW DAY	25,480KWh
VD DHW TOTAL	12,431MWh

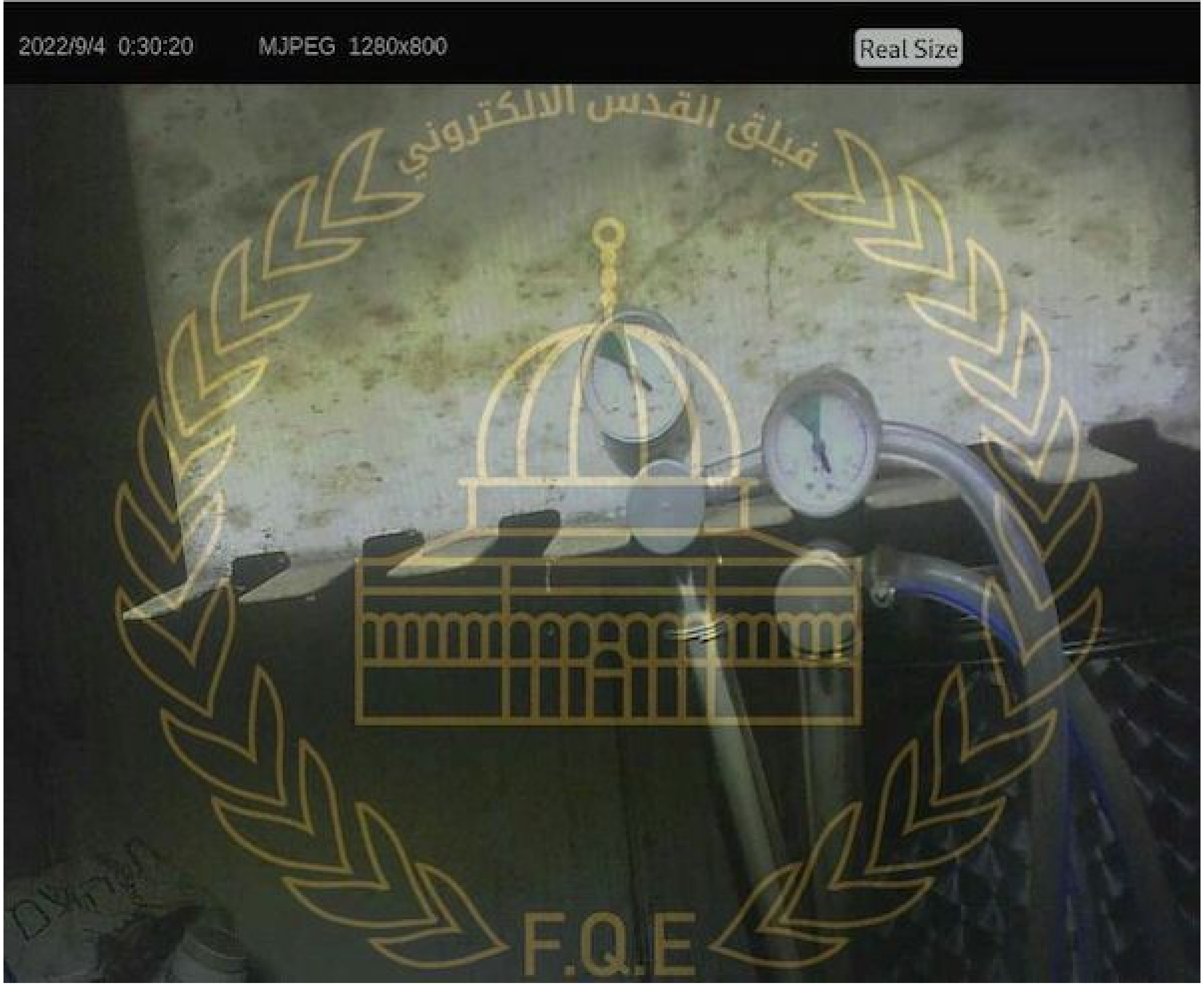
RUNTIME	
VD HEATING	20h
VD DHW	1855h
VD DEFROST	8h
DEFROST TIME	5min
DEFROST STARTS	154

STARTS	
COMPRESSOR	6340

The water systems and thermal pumps inside (Nakhal Yekhi'am Reserve), located in the Kilil Rape, are under our control, and we control and raise the temperatures as we wish.

#Force_Electronic_Quds

Sep. 4 - Actor: Force Electronic Quds



water systems...

#Force_Electronic_Quds

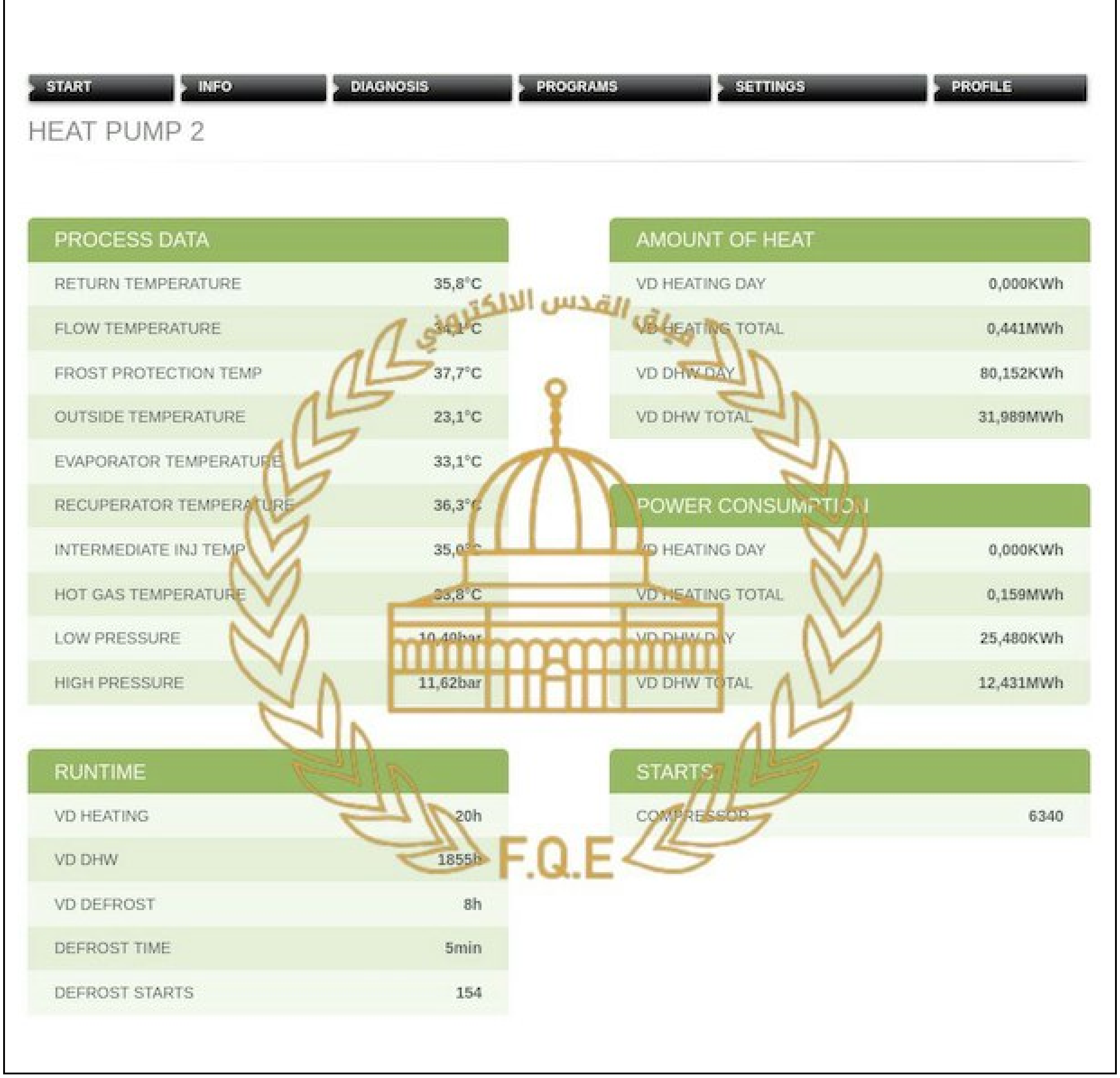
Nov. 29 - Actor: Force Electronic Quds

The zionist enemy is closing one of the control panels for the water systems that we have been accessing for 5 continuous months!!!

#Cyber_Unit

#Force_Electronic_Quds (hxxps://t[.]me/ForceElectronicQuds)

Nov. 30 - Actor: Force Electronic Quds



HEAT PUMP 2

PROCESS DATA	
RETURN TEMPERATURE	35,8°C
FLOW TEMPERATURE	34,1°C
FROST PROTECTION TEMP	37,7°C
OUTSIDE TEMPERATURE	23,1°C
EVAPORATOR TEMPERATURE	33,1°C
RECUPERATOR TEMPERATURE	36,3°C
INTERMEDIATE INJ TEMP	35,0°C
HOT GAS TEMPERATURE	33,8°C
LOW PRESSURE	10,40bar
HIGH PRESSURE	11,62bar

AMOUNT OF HEAT	
VD HEATING DAY	0,000KWh
VD HEATING TOTAL	0,441MWh
VD DHW DAY	80,152KWh
VD DHW TOTAL	31,989MWh

POWER CONSUMPTION	
VD HEATING DAY	0,000KWh
VD HEATING TOTAL	0,159MWh
VD DHW DAY	25,480KWh
VD DHW TOTAL	12,431MWh

RUNTIME	
VD HEATING	20h
VD DHW	1855h
VD DEFROST	8h
DEFROST TIME	5min
DEFROST STARTS	154

STARTS	
COMPRESSOR	6340

Researcher Comments

Overview

On September 04, November 29 and November 30, 2022, the threat actor group "Force Electronic Quds" posted on their Telegram channel claiming to attack water systems and thermal pumps inside (Nakhal Yekhi'am Reserve), located in the Kilil Rape, Israel. The actor group did not share information on the tactics, techniques, and procedures (TTPs) used in the attack. The victim appear associated with the forest and tourism industry.

Actor Background

Force Electronic Quds is an English-Arabic speaking actor group active in the hacktivism space primarily opposing Israel. We have primarily observed this actor targeting internet-exposed assets and leveraging known exploits to gain initial access. This actor appears explicitly interested in targeting OT, but we suggest they have an beginner level capability related to compromising web applications.

Threat Activity Alerts relay initial findings within the cyber threat environment. The content is a faithful representation of an actor's communication, original or translated when possible. If present, reliability (A-F) and credibility (1-6) scores are based on the NATO System and reflects source confidence based on prior history, not judgements about the veracity of any specific claims. We welcome feedback with questions, additional findings, or simply an indication of interest.

Please rate this product by taking a short four question survey

First Version Publish Date

November 30, 2022 08:32:07 AM

Threat Intelligence Tags

Tactics, Techniques And Procedures (TTPs)

- Enabling Infrastructures

Target Geographies

- Israel

Version Information

Version:1, November 30, 2022 08:32:07 AM

MANDIANT ADVANTAGE