Cyber Incident: Ras Abu Desalination Plant

Where Doha, Qatar

When November 21, 2022

What
- Short-term water supply disruptions inciting brief panic in local populace
- Displays at plant listed names of migrant worker known to have died
- Water supply nominal after a few days

How
- Alleged exploits (as assessed by Chinese IRC)
- STANDINGPALM – backdoor inserted via update in Yuma software used at desalination plants, attributed to USG by Chinese IRC
- ROCKSHOT – caused malfunction in temperature control sensors

Who
- Unassessed based on current reporting, uncertainties and intelligence gaps
- Chinese IRC attributed STANDINGPALM to USG
- Private researcher attributed ROCKSHOT to UAE

Assessment Currently multiple critical uncertainties and intelligence gaps; reliance on uncorroborated third-party claims and analysis; STANDINGPALM and ROCKSHOT not definitively known to originate from same threat source or to operate as package

Risks to CNI

Reactions of allies

Chinese role in Qatar

Other actors

Implications and Considerations

NSC Strategic Objectives

Decrease uncertainty, know the risks	Demonstrate U.S. as a responsible cyber actor	Limit China's ability to exploit situation

APT 2785 aka PURPLE APPLE

Recommended Actions

Understand

1. USCYBERCOM and CIA to conduct internal review of cyber operations to understand origin of STANDINGPALM and extent of any possible USG utilization of it
   By December 11
2. DNI to analyze and assess perpetrator of Ras Abu Fontas cyber incident and origin of ROCKSHOT malware and to develop options for public attribution based on level of confidence and classification of supporting intelligence
   By December 14

Prepare

3. CISA and EPA, with support from relevant private sector coordinating councils, to conduct domestic vulnerability assessment of Yuma software and specific ICS exploits and, where relevant, provide prioritized remediation strategy – to be supported by general information campaign, promoted by EPA (e.g. "desalinate the network")
   By end December

Reassure

4. With FBI in lead via UAE LEGAT relationships, CISA to publicly offer technical support to Qatar to collect technical evidence and assist with remediation, while simultaneously requesting Fenghuang Labs to publicly share evidence used for analysis
   By December 15
5. USG to use non-public classified military and diplomatic channels to reassure FVEY and NATO allies regarding its alleged involvement in incident and will share information when available
   Ongoing

Gather, Assess, Consider, Act, Review

IRC – Internet Research Company CNI – Critical National Infrastructure LEGAT – Legal Attaché

10 DECEMBER 2022