CONFIDENTIAL

TO: National Security Council
FROM: APT 2785 aka PURPLE APPLE
DATE: December 10, 2022

CYBER INCIDENT AT RAS ABU FONTAS DESALINATION PLANT IN QATAR

Executive Summary

A recent incident at a desalination plant in Doha, Qatar during the start of the 2022 World Cup is potentially linked to a cyber operation or operations exploiting vulnerabilities in the water and wastewater sector. Currently there are significant intelligence gaps around the alleged incident, effects, threat actors, and possible intentions. The recommended actions, therefore, aim to bring the position of the USG to one of greater certainty before taking further action.

Situation Update

On November 21, 2022, during the FIFA World Cup in Doha, Qatar, the Ras Abu Fontas water desalination plant was allegedly targeted by malware that caused the plant's temperature control sensors to malfunction, affecting its production capacity. During the incident, digital displays at the plant listed names that included a Pakistani migrant construction worker known to have died from dehydration. The incident resulted in short-term water supply disruptions, inciting brief panic in the local populace, and reportedly caused a few migrant worker hospitalizations from loss of access to water. Water supply returned to normal after a few days. No impact was reported at Al Udeid Air Base (AB).

On December 5, Fenghuang Labs, a Chinese cyber incident response company, alleged that a backdoor (named STANDINGPALM) had been inserted via an update in the Yuma software used at the Ras Abu Fontas plant, and that malware (named ROCKSHOT) discovered in the plant's systems had caused the malfunction. Fenghuang Labs attributed STANDINGPALM to USG, citing sophisticated tactics, techniques, and procedure. Yuma is common in desalination and other water plants, and Fenghuang Labs reported that plants in China, Morocco, and Chile have also received the compromised update.

Qatar stated on December 6 that it is considering its response options given Fenghuang Labs' attribution to USG, and diplomatic cables indicate that France has privately expressed concerns. On December 7, a private researcher attributed ROCKSHOT to the United Arab Emirates (UAE). UAE dismissed this as speculation on December 8 in a short statement. USDOS issued an NCND statement on December 9, noting the assistance provided to Qatar in relation to the security of its desalination plants.

Assessment

This is an ongoing incident with multiple critical uncertainties and intelligence gaps, including the current reliance on uncorroborated third-party claims and analysis. According to this analysis, STANDINGPALM indicates a sophisticated cyber operation (i.e. covertly inserting an exploit via a software update), whereas ROCKSHOT indicates a detailed understanding of desalination plant industrial control systems (ICS) (i.e. impacting production via an operational technology exploitation). Although both pieces of malware were allegedly discovered in Ras Abu Fontas's system, they are not definitively known to originate from the same threat source – noting that the current public narrative conflates them as a package.

It is assessed that the aim of ROCKSHOT was to disrupt the water supply coinciding with the start of the World Cup, likely to cause public embarrassment to Qatar, but it is not certain if any collateral harm, including to migrant workers, was intended. With the ongoing proliferation of cyber capabilities to state and non-state actors, it is uncertain whether a nation-state may have directed this alleged cyber operation or operations, and any attribution would be speculative at this stage unless and until verifiable first-order analysis of the technical exploits and threat source and vector has been completed.

In strategic terms, there are multiple competing interests in the situation around Qatar, which includes China and the UAE (e.g. with intent to influence political and economic outcomes in the region), and also

non-nation-state actors (e.g. with concerns regarding abuse of migrant workers in Qatar), all of which will be kept under assessment as understanding of the incident progresses. It is not currently possible to assess the credibility and accuracy of Fenghuang Labs or the private researcher's analysis given the limited public detail, but it is assessed that Fenghuang Labs would not have issued their statement without the approval of the Chinese government.

Issues for Consideration

The situation poses a range of risks critical to U.S. security interests. First, there is a wider but unknown risk from STANDINGPALM and ROCKSHOT proliferating and being exploited by other actors to harm U.S. and global critical infrastructure should there be related vulnerabilities in ICS components. It is not known if any current U.S. cyber operations have been compromised by this incident. Given Fenghuang Labs' attribution of the incident, managing public messaging, congressional responses and reactions, and equities with France and other allies will be critical to preserving international relationships and USG reputation as a responsible cyber actor. There is also a risk of socio-economic unrest in Qatar stemming from ongoing water shortages, which are reported to be especially acute around migrant worker communities. This may subsequently affect CENTCOM's ability to operate in the greater Gulf region via interruption of services to Al Udeid AB.

Given the low levels of confidence and information available, the most pressing strategic objective for the NSC's response is to task USIC, law enforcement, and where possible the private sector to verify and analyze the incident in order to gain clarity on the likely perpetrator or perpetrators and the risks to domestic U.S. infrastructure. A fuller assessment of the cyber operations involved will help to calibrate and enable a coordinated USG response, reflecting the second strategic objective of demonstrating with confidence that the U.S. does not condone this activity and is ready to uphold cyber norms and laws. However, it is not recommended that the U.S. adopts a firm posture publicly before more is known, given the risks of making assumptions that subsequently prove to be incorrect. The third strategic objective should be to limit China's ability to exploit the situation given its known strategic partnership and infrastructure investment with Qatar, and to ensure the protection of U.S. equities with Qatar and regional allies.

The USG should be prepared for a sudden escalation of the situation as clarity is gained, but the recommended actions are intended to adopt a multi-pronged, strategic approach to prepare for a range of outcomes.

Recommended Actions

1. USCYBERCOM to conduct an internal review of cyber operations to understand the origin of STANDINGPALM and extent of any possible USG utilization of it. (By December 11)
2. DNI to analyze and assess the perpetrator of the Ras Abu Fontas cyber incident and the origin of the ROCKSHOT malware and to develop options for public attribution based on the level of confidence and classification of supporting intelligence. (By December 14)
3. CISA and EPA, with support from Water Information Sharing and Analysis Center and Water Sector Coordinating Council, to conduct a domestic vulnerability assessment of Yuma software and specific ICS exploits and, where relevant, provide a prioritized remediation strategy. This is to be supported by a general information campaign, promoted by EPA (e.g. "desalinate the network"). (By end December)
4. With FBI in the lead via its 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 the evidence used for attribution. (By December 15)
5. While confidence in the assessment is improved, USG to use non-public classified military and diplomatic channels to reassure FVEY and NATO allies regarding its alleged involvement in the incident and that it will share information when available. (Ongoing)