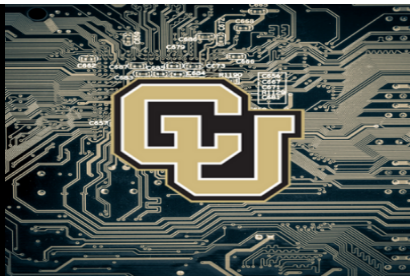
ZERO DARK NERDY



Executive Summary

On 21 November, 2022, Qatar Electricity & Water Co. (QEWC) suffered from a cyberattack targeting water industrial control systems (ICS) which resulted in lower water yield. Consequently, QEWC was not able to meet increased water consumption demand, and accessed reserve water resources in order to supply its consumers. To investigate the incident, QEWC hired Fenghuang Labs (a Beijing-based incident response firm) which identified that the water plant used a compromised version of Yuma software that included a backdoor (dubbed as STANDINGPALM), as well as destructive malware at the affected water plant (dubbed as ROCKSHOT). Several other potential victims using the compromised software were identified in China, Morocco, and Chile, and the report from Fenghuang Labs named the US government as the perpetrator of the backdoor cyberattack.

In response to the cyberattack and accusations against the US, we propose the NSC (1) address the spread of malware and threat to US infrastructure; (2) address attribution claims against the US, encourage multilateral efforts in order to strengthen the credibility of the US internationally, and identify the malign actor responsible; (3) work to encourage regional stability in the Middle East and Gulf region; (4) provide US citizens and installations in Qatar with information and resources related to the cyberattack and its local impacts; and (5) reinforce commitment to Qatar in the wake of the cyberattack and to bolstering human rights on a global scale through multilateral efforts.

Risk and Severity Assessment

According to the Cyber Incident Severity Schema released in Presidential Policy Directive 41, the cyber incident severity is considered a level 3 high impact for Qatar because the incident is likely to impact public health and safety, foreign relations, and public confidence. As for the United States, the incident is considered a level 2 medium impact because the incident may impact domestic public health and safety, as well as foreign relations. Threats and potential impacts include:

Spread of Malware/Threat to US Infrastructure

- The potential exploitation of vulnerabilities in the Yuma software could spread to US critical infrastructure, presenting a threat to US domestic public health and safety. The discovery of additional victims (China, Morocco, and Chile) emphasizes this risk of proliferation.

International Reputational Impacts

- Fenghuang Labs accused the United States of perpetrating the cyberattack. This could affect US and Qatar's long-standing diplomatic relations.
- The reputation and credibility of the United States on the global stage could be at risk from the accusations.

Regional Stability

- Historical precedent indicates that the current crisis may have a destabilizing impact. The 2017 Qatar diplomatic crisis resulted in the UAE cutting diplomatic ties with Qatar. This diplomatic relationship has since been restored in 2021, but those gains may be lost due to speculation about the UAE being the perpetrator. Conversely, regional stability may also suffer if the speculation proves true.

US Citizens and Installations in Qatar

- Qatar's population is 2.5 million, but only 11.6% are Qatari nationals. A majority of the population are foreigners. Accordingly, if there is a recurrence of the attack on the water system in Qatar, US nationals may be at risk, especially due to their increased presence in the country for the 2022 FIFA World Cup in Doha.
- The Al Udeid Air Base in Qatar establishes vital footing for the US in the Middle East region due to the air base hosting US Central Command in the region. So, if OT software components are compromised, issues would arise with basic functions in the military base.

Humanitarian Concerns

- The 2022 World Cup has increased the demand for water due to foreigners traveling to Qatar for the games. This context introduces the risk of the water shortage having a potentially negative impact on migrant worker communities.

POLICY RECOMMENDATIONS

	Short Term	Long Term

Spread of Malware & Threat to US Infrastructure	• To address concerns from the US public about this attack, direct **DHS Office of Public Affairs** to issue a statement emphasizing that the US is not responsible for this attack, that we are committed to finding the responsible party, and that we are bolstering our own cyber security to protect US assets.
	• The US must work with the private sector to audit domestic water infrastructure to ensure the vulnerabilities to Yuma software are not present in American infrastructure.
	• Utilize **CISA** to ensure that US critical infrastructure is enhancing its security protocols during this time.
		• The US must secure its own critical infrastructure from future attacks.
		  ○ Utilize **CISA** and the **EPA** (as the SRMA for the water sector) to investigate the risks that IT and OT convergence present to US assets.
		  ○ Direct **CISA** to develop a contingency plan to ensure the US could fend off a similar attack in the future.
		  ○ Task **CISA's JCDC** to coordinate with the private sector to establish risk and response plans regarding water infrastructure and potential vulnerabilities in Yuma software.
		  ○ Create a workforce development program by **CISA** to educate on vulnerabilities of water infrastructure

International Reputational Impacts	• Direct the **State Department Bureau of Cyberspace and Digital Policy** to continue to deny attribution of attack to US by Fenghuang Labs, reaffirming that the US was NOT involved in the QEWC cyberattack. • Direct the intelligence community to investigate connections between CCP and Fenghuang Labs given the legal access the CCP has to the private sector within China • Continue to work with OCLCTIC to establish the US was not involved in the cyberattack.	**State Department**, in coordination with **DHS**, **FBI**, and others: • Provide the international community with technical details of future cyber attacks against the US to establish a norm of information sharing. • Establish an ad hoc joint-multilateral, multistakeholder investigative committee to address the cyberattack in Qatar. • Engage in diplomatic relations and remind China of the 2015 UN GGE norm of considering all data prior to attribution.
Regional Stability	• Propose a Cyber Coalition within the Gulf Cooperation Council, with the initial steps being general information sharing, establishing confidence building measures, and repairing relations between the Gulf states. • Provide immediate investigative support to Qatar from the US.	Direct the **State Department** to work with Qatar to: • Further the Cyber Coalition within GCC to result in an integrated intelligence community between GCC members. • Offer capacity building resources to heighten security of critical infrastructure during high volume usage of resources. • Encourage Qatar's NCA to ensure adequate separation between IT and OT systems in critical infrastructure.
US Citizens and Installations in Qatar	• **State Department** will inform US citizens currently in Qatar of potential resource scarcity of critical infrastructure in Qatar. • Al Udeid Air Base will ensure their own reserves of resources within their critical infrastructure.	• Direct the **Department of Defense** to audit the Al Udeid Air Base's critical infrastructure to ensure there is no Yuma backdoor in their own software. • Instruct Al Udeid Air Base to ensure adequate separation between IT and OT systems of the airbase.
Humanitarian Concerns	• Direct the **White House Press Secretary** to address domestic and international concerns about human rights abuses by reinforcing commitment to Qatar while making a commitment to bolstering human rights on the global scale through multilateral efforts.	• Encourage **US sporting organizations** to publicly release their own statements of the importance of labor rights and safety.