DECISION DOCUMENT

AU CYBER SQUAD

Laila Abdelaziz
Kady Hammer
Taylor Kerr
Alex Neubecker

Bottom Line Up Front *(what we know now)*

On November 21, 2022, the first day of the FIFA World Cup, a Qatar Electricity & Water Co. (QEWC) desalination plant was disrupted by malware (ROCKSHOT) that was effectuated via a backdoor (STANDINGPALM). QEWC was using a compromised version of Yuma ICS software containing the backdoor; that software version was also pushed out to Chile, China, and Morocco. QEWC hired a **Chinese firm, Fenghuang Labs, to investigate. Fenghuang Labs attributed the backdoor to the USG.** This attack may damage US foreign relations, particularly with France, in the realm of cybercrime cooperation. Proliferation threatens US national & economic security and could create humanitarian crises abroad.

Potential Scenarios *(why this matters to the USG)*

Degree of US involvement is currently unclear. Potential scenarios include:

- USG-developed backdoor was stolen or otherwise misappropriated
- Malicious actors repurposed US code to create a false flag deflection
- Chinese company wrongly attributed backdoor to US; correct attribution unknown

The ROCKSHOT malware is alarming because it affects the integrity of the safety systems used in everything from water treatment facilities to transportation systems to nuclear power.

Courses of Action *(what we want to achieve)**

INVESTIGATE actors, IOCs, and TTPs associated with the backdoor and malware, leveraging diplomatic and intelligence capabilities

MITIGATE vulnerabilities in USG and private sector systems, and offer assistance to build resilience of affected countries

COMMUNICATE via CISA, State Department, and others with private sector, global partners, and the public to share information, raise awareness of potential threats, and safeguard systems

ANTICIPATE and minimize emergent technical, policy, humanitarian, and diplomatic risks

Recommendations (*how we should respond)*

Recommendations will vary depending on USG involvement with, or knowledge of, backdoor & malware

Immediate to Long Term Recommendations

	Immediate (72 hours)	Short Term (1 – 6 weeks)	Long Term (2+ months)
Investigate	Coordinate whole of government investigation of backdoor and malware origins (ODNI lead)‡	NSA: Analyze logs and code to assess attribution‡	Refer to Cyber Safety Review Board for "lessons learned"
Mitigate	CISA: Mitigate potential spread or impact of backdoor and malware in CI	US CERT & CISA: Provide open-source patches to affected parties	Improve resilience of, and cooperation with critical infrastructure including cybersecurity investment tax credit
Communicate	State Dept: Address allies, partners and public concerns and prevent degradation of trust	Encourage media and ally caution/ corroboration prior to attribution	Promote cyber norms for responsible state behavior
Anticipate	Alert relevant resources in the event the malware spreads or backdoor compromises CI systems	Ready CYBERCOM Protection Teams in case of further attacks	Improve global information-sharing partnerships

**Courses of action should occur simultaneously within given time frames*

‡*Clandestine intelligence-gathering risks detection, global backlash, and retaliation*