AU Cyber sQuad Decision Document

Laila Abdelaziz
Kady Hammer
Taylor Kerr
Alex Neubecker

Bottom Line Up Front:

A USG-developed backdoor in Yuma software was exploited by an unknown actor to attack a QEWC plant. Qatar received an *unintended* installation of the backdoor, which the USG developed to conduct Chinese intelligence. A Beijing-based firm publicly attributed the backdoor to the USG. China deployed a patch domestically but is facing issues rolling out the patch to affected BRI firms across Asia and Africa, which are experiencing active threats and disruptions. Qatari authorities arrested a US national and QEWC employee alleged to have participated in the attack.

The NSC should — (1) create and deploy a patch for the backdoor (which no longer serves an intelligence purpose); (2) protect US critical infrastructure (CI); (3) support allies and restore relationships; and (4) communicate assistance rather than deny attribution. Finally, the President should reassure allies, specifically Emir Tamim of Qatar and President Macron of France.

Policy Recommendations

Recommended options should occur simultaneously within given time frames.
High risk options will be adopted at the discretion of the NSC

	Investigate	Remediate	Anticipate
Immediate (within 72 hrs)	- DOJ/FBI: liaise with Qatari law enforcement on QEWC insider - FBI: investigate People's Militia and other US threat actors - ODNI: task IC to investigate foreign threat actors and attribute malware - ODNI: obtain copy of malware for patching from Qatar/China *Risk: HIGH*	-DHS/NSA: coordinate patch development -US CERT/CISA: send patch to US/foreign CI -CISA: engage ISACs and National Guard to spread patch to State/Local governments and CI - CIA: extract Nikara asset - POTUS: reach out to Emir Tamim of Qatar - SecDef & SecState: emphasize US support of Taiwan - POTUS: reach out to President Macron of France	- Offer CYBERCOM Protection Teams and Cyber Mission Assistance Teams to affected nations - Alert FEMA/National Guard for domestic disaster response - Alert USAID for potential international disaster response - CISA: issue alert to CI and private sector with resilience measures - ODNI: lead counter-espionage response for Chinese retaliation
Near-Term (within 3-14 days)	- FBI: monitor People's Militia/other criminal actors - FBI: lead on foreign law enforcement coordination - ODNI: monitor foreign threat actors - ODNI: re-establish strategic collection capabilities against PLA *Risk: HIGH*	- Encourage, through State and Commerce, repudiation of attribution in media outlets, specifically Al Jazeera - State: engage Gulf Cooperation Council to mitigate regional tensions	- NSC: prepare to invoke PPD-41 and convene UCG *Conditional on threat assessment; we are on the verge of invoking*
Long Term (within 2+ weeks)	- DOJ/State: strengthen information-sharing agreements with partner and allied nations	- Engage US-French cyber dialogue - Promote acceptance of UN GGE 2021 report on responsible state cyber behavior	- Create cyber impact assessment as part of VEP balance considerations - Promote cybersecurity investment tax credits for key critical infrastructure to improve resilience