EVENT SUMMARY UPDATE

Recent intelligence updates show that PENSIVEPENGUIN, a backdoor into Yuma software originally created by a CIA asset to provide intel on PRC military infrastructure, was obtained by a non-USG actor who used it to create the destructive payload which was activated within QEWC. The vulnerability has led other malicious actors to enact attacks against other Yuma users. China-based company Nikara Solutions, the creators of Yuma software, have developed and begun to deploy a patch within Chinese critical infrastructure. Deployment of the Nikara Solutions patch has not been widely deployed outside of China. An American citizen with an alleged connection to the QEWC cyberattack has been detained in Qatar.

Intelligence Remediation

Recommended

Risk Level: Low

- Task **CIA** to establish contact with Nikara Solutions asset to ensure asset's safety and ability to continue mission.
- Continue IC assessments of short-term and long-term effects on national collection objectives due to high likelihood of Chinese discovery of PENSIVEPENGUIN.

↓

Risk Level: Medium

- *Evacuate **CIA** asset due to risk of discovery by PRC.
- *Remove PENSIVEPENGUIN to limit risk of blowback and discovery; forfeit collection ability
- Onboard allied and partner countries earlier in development of cyber operations.

↓

Risk Level: High

- *Leave **CIA** asset in place and continue collection efforts.
- *Activate PENSIVEPENGUIN capabilities to install malicious payload on PLA networks.

Building Global Resilience

Recommended

Risk Level: Low

- Expand **NIST**'s work in cybersecurity and privacy with a focus on the National Vulnerability Database.
- **CISA** through **US-CERT** to work with CERTs/CSIRTS internationally to secure critical infrastructure owners abroad.
- **DOS** and **USAID** offer long-term workforce development international capacity building support.

↓

Recommended

Risk Level: Medium

- Develop a "counter-bug" bounty program led by **NCD** to develop an open-source Yuma patch.
- Host Yuma vulnerability patch with Apache Software Foundation and/or code.gov.

Legend

FL= Fenghuang Labs
PRC = People's Republic of China
PLA = People's Liberation Army (China)
*These options should be considered as alternatives to one another, as opposed to additive.

Communications Plan

Recommended

Risk Level: Low

- **White House Press Secretary:**
  - The US did not implement malware.
  - The US is bolstering cyber security to protect US assets.
- Global Engagement Center in **DOS** to engage in messaging that denies FL attribution claim.
- **DOS** press release reaffirms commitment to relationship with Qatar and international allies, including France.
- **CISA**, **EPA** and **FBI** to form task force for information sharing and coordination purposes with water sector.

↓

Risk Level: Medium

- Deny any US responsibility in attack via **DOS** and **White House Press Secretary** press release.
- **DOS** and **FBI** to offer ongoing investigative support with regard to American citizen in custody in Qatar.

↓

Risk Level: High

- Release **DOS** statement condemning Chinese responsibility in causing regional instability via software vulnerabilities in the BRI.