**Summary and Synopsis:**

Significant Cyber Incident halting global port operations creates profound economic implications; Actors gained access through TidalWaves software to manipulate data and deploy ransomware; Threat actors are Romanian cybercriminals (*moderate confidence*) hired by Iranian APT (*low confidence*).

**Policy Recommendations:**

| Risk Level | Priority | | | |
|---|---|---|---|---|
| | Contain Malware | Attribute Actors | Act Multilaterally | Communicate Effectively |
| Highly Recommended | **- FBI led task force responding to ports (local FBI CTFs, CISA, CBP, ICE, US-CERT, M-CERT, USCG)**<br><br>**- FBI OPS reach out to TidalWaves to identify and notify breached customers**<br>*Cost: Resistance from private sector* | **- Task intelligence community with investigating the relationship between 1881 Colectiv and Manticore**<br><br>**- Find missing cargo using NGA**<br><br>**- DOJ opens case against 1881 Colectiv members and Manticore**<br>*Cost: Investigative resources* | **- Alert international allies to discovery of malware and port data manipulation**<br><br>**- Direct embassies to offer U.S. assistance to impacted nations' port malware response through our ALAT expertise and Secret Service CFTFs.**<br>Cost: *Investigative resources* | **- Centralize all communication from NSC**<br>*Cost: May overwhelm the White House Press Office*<br><br>**- Disseminate technical findings (M-ISAC, MTS-ISAC, MPS-ISAO, VirusTotal)** |
| Recommended With Caution | - Engage private-sector security firms to assist in technical investigation and forensic analysis of port breaches<br><br>- FBI led task force urges ports to initiate Disaster Recovery plans<br>*Cost: Investigative resources* | - Arrest known 1881 Colectiv members in international operation coordinated by INTERPOL-USNCB and DOJ OIA<br>*Cost: Constrain Intelligence Collection*<br><br>- USCYBERCOM / NSA propaganda campaign against actor(s)' leadership<br>*Cost: May escalate geopolitical issues* | - Emergency session of the UN Security Council and International Maritime Organization<br>*Cost: Bureaucracy may cause delay*<br><br>- Advise international allies to increase their own port security if near conflict areas<br>*Cost: State may have limited resources* | - CISA Representative interviews with major news network |
| Higher Risk Considerations | - Securing the ecosystem<br>*Cost: Monetary* | - CYBERCOM / NSA operation against actor(s)' critical infrastructure.<br>*Cost: May escalate geopolitical issues*<br><br>- CYBERCOM / NSA threat hunt forward into Iranian networks<br>*Cost: Intelligence Gain/Loss* | - Sanctions towards actors(s) involved for their involvement with the ransomware attacks<br>*Cost: May escalate geopolitical issues*<br><br>- Defend forward with NATO's RRT<br>*Cost: May escalate geopolitical issues* | - Panel of U.S. government officials from impacted sectors hold a press conference on attack's implication |

To build long-term capacity , we recommend prioritizing the establishment of the National Cyber Director to oversee the following: investment in research and development of technological security solutions, updates to maritime security frameworks, expanding international training and assistance programs, and the enactment of supply chain regulations.

**#CtrlAltElite:** Evan Gertler. Arsene Frederic Jr., Elizabeth Marge, Christopher Rodriguez-Molina