UTAH VALLEY UNIVERSITY W0LV3R1NES:
MARK DRIGGS, ALEC HEITZMANN, ANDREW JENSEN, HUNTER KARR

SITUATION SUMMARY:
On 23 March 2021, the W0LV3R1NES Cybersecurity Task Force (WCTF) received notice of a cyberattack that targets global shipping software. Since then, the situation has escalated to impact US national security interests. The malware, codenamed BASKERVILLE, has spread to 43 ports across the globe, instigated by an initial cyberattack against the TidalWaves port management system. The current impacts of BASKERVILLE include:

- Missing SAM equipment and medical supplies.
- 74 cargo ships backlogged in Houston.
- 46% reduction in oil production at Corpus Christi.
- Nigeria regional energy crisis and food shortage.

In total, BASKERVILLE currently stands at a cost of $950B. The complete attribution continues to be unclear, however, the WTCF is confident that 1881 COLECTIV is working with an adversary with top-tier offensive capabilities. The immediate priority of the NSC should be to stop the spread of malware, locate immediate shipped goods that may threaten US national security, and normalize the global shipping industry. The WCTF has a strong level of confidence that the aim of the malicious cyber-attackers is to disrupt global trade.

RESPONSE GOALS:
The WCTF recommends that policies approved by the NSC follow a framework that includes several primary goals:

- Mitigate immediate impacts of the ransomware attack and resume normal port operations.
- Track down and identify missing cargo, with the highest priority on cargo posing a threat to national security.
- Establish complete attribution for the cyberattack, including potential partners to 1881 COLECTIV.
- Maintain contingency plans for escalation of software development.

POLICY & RESPONSE OPTIONS:

SHORT-TERM RESPONSE

- Establish Unified Coordination Group (UCG) under PPD 41 to coordinate between government and private entities to accomplish the following tasks:
  - Identify potential for BASKERVILLE to laterally move to other industries and establish connection to other malware.
  - Reverse-engineer BASKERVILLE and attribute actors.
  - Identify and shutdown 1881 COLECTIV nodes/servers.
- Instruct CISA to coordinate with Rabinara Group to provide effective mitigation strategies and workarounds for affected systems, to include providing YARA rules to those affected.
- US Coast Guard works with the Port Authority to allow for safe docking and unloading to help resume normal port operations.
- Task CIA and NGA, working with impacted US defense contractors, to continue targeted surveillance, prioritizing SAM missile components.
- Prioritize DOJ indictments of 1881 COLECTIV members in custody and MANTICORE.
  - FBI Legal Attaché coordinate with Europol EC3 in Bucharest to issue indictment.
- Establish domestic economic damage assessment:
  - DoT FinCEN collect, analyze, and disseminate data on financial transactions to established beneficiaries of economic impropriety related to stock manipulation and identify potential attribution to report to UCG.
  - FinCEN works alongside ongoing SEC operation to identify any potential commonalities.
- FBI Cybercrime Center continues to establish direct attribution between 1881 COLECTIV and MANTICORE.

LONG-TERM RESPONSE

- Task US Coast Guard and the US Maritime Administration to monitor AIS tracking systems to identify and track ransomware-affected ships.
- TidalWaves, working with CISA and the FBI National Cyber Investigative Joint Task Force to ensure proprietary sensitivity, will encourage full rollout of the TidalWaves software patch.
- Coordinate through CISA with FIRST CSIRTs to share Baskerville TTPs with the intention to halt the spread of BASKERVILLE.
- Coordinate with the UN Humanitarian Air Service (UNHAS) in Nigeria to deliver USAID shipments until the Port of Harcourt is secured.
- Instruct CISA to work with DoS to prepare a proposal for the requested Nigeria assistance package.

ESCALATION CONTINGENCIES

- Put CYBERCOM on alert to develop potential OCO response options authorized by 2019 NDAA.
- NSA/CYBERCOM Integrated Cyber Center works with private industry including ISPs, technology firms, and cybersecurity research firms to identify possible contingencies should BASKERVILLE or associated malware move laterally.
- DoT OFAC prepares list of potential sanction targets based on attribution.
- Notify CENTCOM of missing SAM components in the event that CIA and NGA cannot provide actionable intelligence.