Situation Assessment

On March 19, 2021, ransomware attacks were reported in 7 international ports, including 2 U.S. ports: Port of Houston and Port of Corpus Christi in Texas. The ransomware, dubbed Baskerville, has reportedly compromised Port of Houston's operations. While vessels can dock, goods cannot be unloaded due to the inability to access data, including cargo manifest systems and email resulting in shipping issues. The full extent of the data integrity manipulation is unknown. International media has reported that TidalWaves, a widely used cargo management system, was the victim of a cyber attack that we believe to be caused by or related to Baskerville.

This task force understands that the shipping industry is a broad, critical, and vulnerable target. The FBI and CIA have picked up chatter that corresponds with current port and data disruptions The chatter suggests that entities/groups with potential links to state-backed actors may be involved in the Baskerville ransomware attack and TidalWaves compromise. It also suggests that ransomware may not be the primary purpose of the Baskerville malware. While the main actors and motivations are unattributed, the Baskerville and TidalWaves compromise could have secondary effects outside of the shipping sector. For instance, slowed shipping and missing cargo could undermine market confidence, resulting in negative economic impacts. As another example, there are reports of a brewing humanitarian crisis in Nigeria should shipping operations not resume quickly. Additionally, missing goods may have security implications depending on the nature of the cargo. Further investigation is needed to understand the nature and extent of the Baskerville malware, TidalWaves compromise, and the threat actors involved.

Summary of Impacts & Risks

Shipping Delays - Tracking data for shipments in 7 reported ports have been corrupted by Baskerville. How can Baskerville be mitigated and/or removed to resume regular shipping operations?

- Known Impacts
  - Missing cargo is marked in manifests as "delivered," leading to delays and confusion of goods transportation.
  - Ships cannot unload cargo in ports affected by Baskerville, leading to delays in the transportation of goods.
  - Energy exports and foreign aid have been disrupted in Nigeria and possibly around the world.
- Potential Impacts & Risks
  - There will likely be a negative economic impact from lack of goods distribution and dip in market confidence.
  - The Covid Pandemic may intensify from probable losses and delays of Covid vaccines and related materials.
  - Adversarial States may circumvent sanctions and move weapons or people across U.S. and/or foreign borders.

Spread of Malware - It is unclear how the Baskerville malware spreads and under what parameters it executes. How can Baskerville be contained?

- Known Impacts
  - Ports in North America, South America, Europe, Africa, Asia, and Australia are infected with Baskerville.
  - Goods ranging from food to oil refinery equipment are missing.
  - Ships cannot plug into the IT infrastructure of infected ports, causing delays.
- Potential Impacts & Risks
  - Baskerville is likely to spread to new ports beyond the reported 7 and may cross into other critical sectors like healthcare, energy, and finance.
  - Failure to deliver time-sensitive and volatile shipments may pose risks to U.S. economic interests and security.

Overview of Policy Options:

Given the impacts on global shipping, it is critical to collaborate with international, governmental, and private sector partners in the response to Baskerville. It is important to consider short term policy options to address the immediate problem and long-term policy options to prevent it from happening again. The focus is on *containing* the malware, *mitigating* the impact on shipping while simultaneously *investigating* the origins.

Mitigate Impact on Shipping

- Priority 1: Revert to analog shipping measures.
- Priority 2: Deploy U.S. Coast Guard to all ports, starting with infected ports.

Contain the Malware

- Priority 1: Leverage CISA via US-CERT to issue alerts and coordinate government, private, and international response.

Investigate Origins

- Priority 1: Digital forensics and patch creation.
- Priority 2: Use law enforcement and the intelligence community (IC) to investigate missing goods and second-order effects.

Policy Options:

These are a range of options to consider. They are not mutually exclusive and this task force believes that the combined policies create a comprehensive strategy to combat Baskerville.

Mitigate the Impact on Shipping: Temporary action must immediately be taken to mitigate the economic, humanitarian, and security risks associated with interrupted shipping. This will cause delays but is likely to ease long term impact.

- Short Term: Policy options below to be started immediately.
  - DHS should work with impacted shipping companies to develop analog shipping methods to promote continuity of shipping operations.
    - Orders should be placed by phone and tracked in Excel spreadsheets on new, unused computers.
    - Current cargo should be manually verified and physically marked by each shipping company.
    - Ongoing communications should go through encrypted channels such as Whatsapp or Signal.
  - The U.S. Coast Guard (USCG) should be deployed to all U.S. ports to conduct maritime traffic management and

facilitate the needs of ships in holding patterns.

        - USCG should contact the International Maritime Organization and U.S. Merchant Marine support to assist in coordinating U.S. and international response.
        - Ships should not plug into port IT infrastructure with Baskerville; they should reroute or anchor in place.
        - In ports that are confirmed to NOT have Baskerville, USCG should partner with US-CERT and the U.S. Digital Service to check ships for Baskerville before allowing them to use said port's IT infrastructure.
    - Shipping companies should explore alternative means of moving goods through air or ground transportation.
    - Should the stock market show dangerous volatility, SEC should implement trading suspension on affected stocks.
- Mid Term: These policy options may take about 6 months-1 year.
    - The Department of Commerce issues subsidies to U.S.-based businesses that are on the brink of financial collapse due to the impact of Baskerville.

Advantages: Lessening the impacts of shipping disruption will allow the U.S. to economically rebound more quickly. Utilizing USCG to coordinate logistics can quell panic and give DOD direct access to ports as-needed. A fast response utilizing public and private partners will project leadership in this crisis and allow the U.S. to influence responses moving forward.

Disadvantages: Coordinating analog tracking across ports and companies will be difficult. Goods will be delayed. Focusing on shipping impacts will not address malware spread, the specific zero-days exploited, or yield information to stop Baskerville.

Contain the Malware: The first priority should be to contain the spread of Baskerville so further resources can focus on the mitigation of negative impacts and recovery.

- Short Term: Policy options below to be started immediately.
    - The Cybersecurity Infrastructure Security Agency (CISA) via U.S. Computer Emergency Readiness Team (US-CERT) should be declared the incident response coordinator. With assistance from Maritime Transportation System ISAC (MTS-ISAC), US-CERT should issue an alert to all ports, shipping industry stakeholders, allied international partners, and critical infrastructure operators warning of potential impacts.
        - US-CERT should coordinate with CERT-EU, CERT-CA, AusCERT and MTS-ISAC to communicate and collect information on Baskerville, develop temporary workarounds, and move towards a patch.
- Long Term: Policy option below may take 1 plus years.
    - It is recommended that DHS update guidance on best cybersecurity practices for ports, including suggestions to employ Disaster Recovery as a Service (DRaaS) and to obtain a cybersecurity certification. Such guidance would help incentivize proactive steps toward mitigating risk of future cargo manifest corruption.
    - DHS should explore funding Distributed Ledger Technology (DLT) research by contracting academic and private companies in order to improve integrity and reliability of cargo shipping manifests in the future.

Advantages: Government coordination with the private sector creates a more efficient, comprehensive response to Baskerville. In the long term, cybersecurity certification of ports creates IT system adherence to cyber best practices, reducing cyber risks. However, all threats cannot ever be fully mitigated. Therefore, we suggest funding DLT research to improve shipping manifest resiliency.

Disadvantages: As the government shares information, threat actors may manipulate information or change tactics to adapt to our methods. DLT implementation would take global cooperation, which may be difficult among competing trade partners.

Investigate Origins: Investigate the components of Baskerville and the parties responsible for the development and deployment of the malware.

- Short Term: Policy options below to be started immediately.
    - CISA should contract a cybersecurity firm (e.g., FireEye or Crowdstrike) to conduct independent analysis of Baskerville, how it spreads, affects ports, and best methods for neutralizing the malware and patching it.
    - The Office of Foreign Asset Control, the U.S. Intelligence Community, DHS, and Interpol should investigate missing goods that could pose a danger to citizens.
- Mid Term: These policy options may take about 6 month-1 year.
    - TidalWaves should work with trusted cybersecurity contractors and US-CERT to develop and deploy a patch
    - US IC & Five Eyes should continue intelligence gathering on suspected threat actors' (Manticore APT and Colectiv 1881) network communications to explore leads for attribution.

Advantages: Conducting digital forensics will help patch development and mitigate further vulnerabilities. We also need an understanding of the techniques, tactics, and procedures used in Baskerville and who used them to deter future attacks.

Disadvantages: The timetable for developing a patch is unclear. Moreover, since the full nature of the hack is unknown, investigators may be hindered by unseen challenges such as insider threats. Additionally, committing resources to finding lost items may not yield proportional results.