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 composed of both a ransomware and malware that targets global shipping software.

- BASKERVILLE: Ransomware that affects email software, access control, and cargo manifests at shipping ports.
- CHIMERA: Malware that allows actors to edit bills of lading and container tags at shipping ports.

The WCTF has a high level of confidence, based on HUMINT and SIGINT reporting, that BASKERVILLE has been deployed at several ports in the United States and abroad and works tangentially with CHIMERA, allowing actors to camouflage data manipulation in TidalWaves, a port management system used by government agencies and private industry. The WCTF has a moderate level of confidence, based on reliable HUMINT, that the aim of the cyber-attackers is to disrupt global trade; however, escalation of the cyber incident is possible. Any escalation could severely impact U.S. economic interests domestically and abroad.

Response Goals:
The WCTF recommends that policies approved by the NSC follow a framework that includes several primary goals:
- Determine immediate mitigation plan for both Texas ports.
- Assess the damage of BASKERVILLE and CHIMERA on ports, government agencies, and private industry.
- Coordinate with affected countries to assess and mitigate the impacts of BASKERVILLE and CHIMERA to global trade.
- Maintain contingency plans for escalation of software deployment.

Policy & Response Options:

NATIONAL RESPONSE

- FBI and DHS will coordinate immediate intelligence gathering priorities with relevant parties.
  - FBI Houston Field Office and Field Intelligence Group will work with the Houston DHS Fusion Center, TidalWaves, local law enforcement, and Maritime Transportation System ISAC to collect information at the Port of Houston and Port of Corpus Christi and assess the impact of BASKERVILLE and CHIMERA.
- Issue CISA Traffic Light Protocol: AMBER (TLP: AMBER) to the Maritime Transportation System ISAC members regarding BASKERVILLE and CHIMERA.
- Instruct CISA to deploy and operate technology to assist affected government agencies and issue mitigation protocols to other impacted entities under 44 U.S. Code § 3553 (h).
- Establish national cyber taskforce led by the FBI National Cyber Investigative Joint Task Force and assisted by CISA that includes: IT/IS staff from the Port of Houston and Port of Corpus Christi, TidalWaves IT/IS support staff, Maritime Transportation System ISAC representatives, and cyber specialists from the Rabinara Group; in accordance with principles outlined in the Cyberspace Solarium Commission.
  - Assess damage and implement immediate mitigation plan for Port of Houston and Port of Corpus Christi.
  - Establish working groups to prioritize analysis of CHIMERA lateral movement potential, reverse-engineer BASKERVILLE and CHIMERA, and identify actors for attribution.
- Prioritize intelligence collection on 1881 COLECTIV and MANTICORE within the NSA, CIA, and FBI.
  - Contact Romanian and Interpol authorities through the FBI Legal Attaché in Bucharest, which covers Romania, in order to question 1881 COLECTIV SUBJECT in custody. Coordinate with DOJ's Office of International Affairs to request Romanian assitance via MLAT, if needed.

INTERNATIONAL RESPONSE

- Establish immediate international lines of communication with relevant partners.
  - Coordinate through CISA with international CERTs to determine relevant international cyber-response.
  - Instruct State Department RSO to notify OSAC members of malicious IOCs.
- Establish an international cyber taskforce with Nigeria, Australia, Brazil, France, and India to assess and mitigate the continuous impact from BASKERVILLE and CHIMERA.
  - Establish collaboration between USAID and the Ministry of Foreign Affairs in Nigeria to coordinate and address ongoing needs due to the situation at the Port of Harcourt.
- Create economic outlook report that describes potential outcomes of a disruption of global trade as a result of the cyberattack, collaborating with the WTO and Financial Services ISAC.

ESCALATION CONTINGENCIES

- Put CYBERCOM on alert to develop potential OCO response options authorized by Section 1642 of the 2019 NDAA.
- Prepare a public statement in order to mitigate negative PR, acknowledging that the U.S. Federal Government is coordinating with local Texas government, state Texas government, and private sector actors in order to assess and mitigate the impact of BASKERVILLE and CHIMERA.
  - Establish a PR strategy with DOJ Office of Public Affairs, CISA, social media, and news media companies to counter misinformation and potential disinformation.