CYBER KNIGHT RIDERS

SIPA **HANDOUT – DAY 1**

TO: National Security Council | **FROM**: Cyber Knight Riders, SIPA / Columbia University

SUBJECT: Ransomware & supply chain attacks against US ports with links to Romania and Iran

EXECUTIVE SUMMARY: In response to the ransomware and supply chain attacks on two US and seven international ports, we identify these US strategic objectives: (1) Maintain/Re-establish Openness & Combat Port Shortages, (2) Facilitate Technical Mitigation and Investigation, (3) Ensure Operational Readiness, (4) Establish International Cooperation, (5) Formulate Appropriate US Response.

ASSESSMENT

1. Medium confidence: **Romanian cybercrime group** launched the **ransomware attack**
2. Medium confidence: **One or more Iranian-linked APT(s)** launched TW **supply chain attack**
3. Low-medium confidence: The **ransomware and the supply chain attacks are coordinated**
4. First indication: Possible longer-term objective is **attack against US energy/oil supply**

POLICY OPTIONS ***(Future Options in italic grey, marked F, if situation deteriorates)***

1. Corroborate Intelligence on Incidents (Impact: Improve understanding, Risk: None)

- 1.1 Consult with US IC, Five Eyes and international partners
- 1.2 Advise FBI to investigate ransomware attack in cooperation with ENISA (EU-CERTs)
- 1.3 Collect information with US and International Port Authorities

2. Facilitate Technical Mitigation (Impact: Defensive assessment, investigation and expulsion of intruders, Risk: Unclear willingness to cooperate with TW proprietor)

- 2.1 Advise CISA/FBI to investigate extent and depth of TW intrusion with TW SOC
- 2.2 Advise CISA/US-CERT to cooperate with TW for technical mitigation (patches, NCAS/CISA warning, additional vulnerabilities)

3. Establish Crisis Management (Impact: Involve all stakeholders, ensure port safety, Risk: None)

- 3.1 Coordinate with CISA's NCCIC, FBI's CyWatch and Coast Guard's NRC, relevant COTP and port operators to secure dangerous goods, prioritize outstanding network updates, increase ports' physical security, coordinate public/internal crisis communication, review current cyber defense plans and exercises at unaffected US ports
- 3.2 Coordinate with ISACs, SCCs and GCCs (DHS NIPP for DOT), TSA and CBP *(F: Include NIPP for DOE)*
- *3.F F: Set up international maritime crisis response unit with ENISA, IMO's ISPS, DHS/CISA, Coast Guard and FBI*

4. Secure Transportation of Critical Supplies and Energy Sector (Impact: Preparing options to secure oil and energy provision, Risk: None)

- 4.1 Coordinate with DOT/DOE for possible deterioration and attack on energy supply: (1) review plans on prioritizing energy-related trade, (2) reroute critical supplies, (3) increased cyber monitoring and threat hunting
- *4.F F: Coordinate with DOT/DOE for individual/joint protection measures to secure US oil and energy supply and begin coordination with allies for potential port access*

5. Explore Diplomatic Options (Impact: Coordination with partners, preparing for deterioration without current escalation; Risk: Overestimation of threat level, unintended self-escalation)

- 5.1 Advise DOS to (1) address Romania, EU and NATO for cooperation on investigation and disruption of cybercrime group, (2) to assess and reinforcement backchannels to Iran for potential future use
- *5.F F: Advise (1) DOS and DOT/OFAC to assess options for (economic) sanctions against Iran/associated groups, (2) DOS and CIA to establish Iranian backchannel, (3) DOS to reach out to Israel to inform and coordinate joint response, Prepare (4) public statement and attribution of attacks to Iran and Romania and (5) media disclosure*

6. Assess DF/PE-aligned Military Measures (Impact: Prepare for potential deterioration without escalating at the moment, Risk: Unintended escalation due to leak of preparation)

- 6.1 Address USCYBERCOM to assess disruption and preemptive defense options through DF/PE hard evidence
- *6.F F: USCYBERCOM/FBI to implement (1) disruption operations (2) DF operations against Iran/associated groups*