CYBER KNIGHT RIDERS

SIPA **SITUATION ASSESSMENT AND POLICY BRIEF**

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: Ongoing ransomware attacks with links to Romanian cybercrime and possibly extensive supply chain attacks with links to Iranian APT group(s) affected two US ports and seven international ports. In response, we propose the NSC (1) urgently corroborates intelligence on incidents with our international partners, (2) thwarts the ongoing attacks and patch affected systems with CISA/US-CERT, (3) establishes joint crisis management and communication between US agencies and public partners, (4) preventively secures the transportation of critical supplies and the energy sector, (5) engages in diplomatic communication with partners and prepares backchannels to our adversaries and (6) assesses military and/or cyber disruptive measures if the situation deteriorates.

FACTS – US ports of Houston and Corpus Christi as well as seven international ports were **hit by a coordinated, international ransomware attack** from Romania. Simultaneously a possibly Iranian-backed **APT group(s) compromised the port management software** "TidalWaves" in a months-old supply chain attack. The **extent and depth of infiltration is still unknown** (no. of ports / persistence).

March 19, 2021: Texas ports and seven international ports (FRA, BRA, IND, AUS) were hit by a coordinated, international ransomware attack out of Romania named "BASKERVILLE". The is linked to the Romanian hacking collective "1881 Colectiv". INTERPOL arrested Mihai IORDAN, a member of the collective, on March 23 with potentially relevant insider information. The attack stalled trade on a variety of goods, incl. oil refinery equipment in the US and oil deliveries from Nigeria. The Port of Houston (No. 2 in US) predominantly trades crude oil and oil products. At Port of Corpus Christi, oil-based products make up 76% of all commodities traded.

March 23, 2021: CISA confirmed the compromise of the port management software "TidalWaves" (TW) in an ongoing supply chain attack. US IC picked up noise that hints toward a long-term planning of the attack with entry over a month ago. The supply chain attack shows a possible connection to the Iranian APT group "Manticore" with a minimum of four operating members including Kian AHMADI alias "Klaw".

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 supply** with oil

US intelligence reports and the origin of the ransomware "BASKERVILLE" attribute the Romanian cybercrime group "1881 Colectiv" with high confidence to the ransomware attack. The TidalWaves intrusion exhibits TTPs (advanced combination of delivery, exploitation, C2 and exfiltration/payload activation) of an Advanced Persistent Threat (APT) execution. The long-term operation indicates persistence: it may lead to a substantial threat to US economic interests. The vulnerabilities may be exploited by other US adversaries.

Intelligence so far suggests some degree of Iranian involvement, possibly motivated by retaliation for the killing of Iranian General Soleimani in Jan 2020 and friction in JCPOA / Nuclear Deal. Iran has previously demonstrated persistent threats to US critical infrastructure, e.g., in the Rye Brook, NY dam attack in 2013.

It is likely that the ransomware and the supply chain attack are coordinated with the ransomware possibly contracted as a "for-hire service" from the Romanian group. The largest concern at the moment is furthered economic damage to US shipping and transportation. The longer-term objective of the attack may be US energy supply as the ports targeted are crucial for oil-related trade, the effects on refinery equipment and the Nigerian oil trade cut.

STRATEGIC OBJECTIVES

1. **Maintain/Re-establish Openness and Combat Port Shortages** (Ensure continued operability for US transportation system, in particular for ports and energy sector supplies)

2. **Facilitate Technical Mitigation and Investigation** (Mitigate negative effects of ransomware and supply chain attacks, assess extent and depth of ongoing intrusions, investigate attribution)
3. **Ensure Operational Readiness** (Coordinate with US agencies, port authorities and private sector to prevent further deterioration and damage to US companies)
4. **Establish International Cooperation** (Establish robust communication and cooperation with international partners to mitigate damages and future risk and to investigate responsible threat actors)
5. **Formulate Appropriate US Response** (Assess diplomatic and possibly military options of response)

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

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/US-CERT to investigate extent and depth of TW intrusion with TW SOC
   - 2.2 Cooperate with TW to issue patches, coordinate NCAS/CISA warning, assess additional unpatched vulnerabilities, determine potential for exploitation by other threat actors.
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 Coast Guard Captains of the Port (COTP) and port operators to locate and secure dangerous goods in affected ports, prioritize outstanding network update, increase ports' physical security, coordinate public and internal crisis communication, reviews 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 to share information and raise awareness level *(future option: Include NIPP for DOE)*
   - *3.F Future option: 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 and DOE to prepare for possible deterioration of situation and potential attack on energy supply, especially petroleum, including (1) review plans on prioritizing unloading/trade of energy-related trade, (2) reroute critical supplies, (3) increased cyber monitoring and threat hunting
   - *4.F Future option: Coordinate with DOT and DOE to execute individual or 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 Future options: (1) Advise DOS and DOT/OFAC to assess options for (economic) sanctions against Iran/associated groups, (2) Advise DOS and CIA to establish backchannel communication with Iran, (3) Advise DOS to reach out to Israel to inform and coordinate joint response, (4) Prepare public statement and attribution of attacks to Iran and Romania, (5) Share information on attribution with journalists*
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 cyber disruption options against cybercrime group and preemptive defense options through DF/PE hard evidence against Iran
   - *6.F Future options: Advise USCYBERCOM and/or FBI to implement (1) disruption measure against cybercrime group, (2) Defend Forward operation against Iran/associated groups*