



# Cyber 9/12 Strategy Challenge

## Intelligence Report I

### INSTRUCTIONS

**Please read these instructions carefully. They have changed from previous years.**

Your team will take on the role of experienced policy advisers, part of a hypothetical cybersecurity task force, preparing to brief the National Security Council (NSC). This packet contains fictional information on the background and current situation involving a major cyber incident affecting US systems. The attacks notionally take place in Spring 2021 in a world where the **SolarWinds compromise never occurred**. The scenario presents a fictional account of political developments and public reporting surrounding the cyber incident.

The NSC needs information on the full range of response options available regarding this incident. Your team has been tasked with developing an appropriate course of action for recommending to the NSC.

You are to consider as facts the following pages for formulating your response.

**You will use the fictional scenario material presented to perform three tasks:**

**Written Situation Assessment and Policy Brief:** Your first task is to write an analytical policy brief that provides a concise assessment of the situation, addresses potential impacts and risks, and discusses the implications of the cyber incident. Describe policy considerations for different potential state and non-state actors. Be clear regarding the advantages and disadvantages of various policy options and explore the course of action you are recommending in depth. **The length of the brief is limited to two single-sided pages.**

**Oral Policy Brief (Day 1):** For the first day of the competition, prepare a ten-minute oral presentation outlining your impact and risk assessment, as well as your suggested course of action. You will present to a panel of judges playing the role of the NSC.

**Decision Document (Day 1):** Teams will also be required to submit a “decision document” accompanying their oral presentation at the beginning of the competition round. The “decision document” will be a maximum of one single-sided page in length, outlining the team’s response options, decision process, and recommendations. The teams should note that the document is not intended to summarize every detail of the recommendations, but to help the judges follow the oral presentation, and the judges will be given only 2 minutes to read it before the presentation begins. The document should be written

with the goal of assisting busy senior officials to quickly grasp your team's recommendations and analysis.

**Keep these tips in mind as you are reading and considering your policy response alternatives:**

- *Analyze the issues.* The goal of the competition is for competitors to grapple with complex issues and weigh the strengths and weaknesses of potentially conflicting interests. Priority should be given to analysis of the issues and not to listing all possible issues or solutions.
- *Engage the scenario.* Believe that the universe we have created is plausible and that the events that happen in it are realistic. Nevertheless, remember to think critically about the intelligence you have been provided and its provenance.
- *Think multi-dimensionally.* When analyzing the scenario, remember to consider implications for other organizations and domains (e.g. private sector, military, law enforcement, different levels of government, diplomatic) and incorporate these insights along with cybersecurity.
- *Consider who you are, and who you're briefing.* You are experienced cyber policy professionals briefing the National Security Council. As such, you should be ready to answer questions on agency responsibility, provide justifications for your recommendations, and have potential alternatives ready.
- *Be creative.* Cyber policy is an evolving discourse, and there is no single correct course of action to the scenario information provided. There are many ideas to experiment with in responding to the crisis.
- *Don't fight the scenario.* Unless stated otherwise, assume all inter-state relations, policies, and treaties have remained the same as they were in February 2021. Explore the implications of that information, not the plausibility. **The only exception to this is that in this scenario, students should work with the assumption that the SolarWinds hack never occurred.**

Given the unclear nature of the threat, the NSC requests that your team prepare a concise assessment of the ongoing situation and reporting. Your assessment should include:

- How or where the relevant systems could be vulnerable to exploit, and what steps can be made to mitigate these vulnerabilities;
- An assessment of potential risks and impacts to consider if the vulnerabilities are successfully exploited; and
- Responses the NSC can or should consider addressing these vulnerabilities, taking into account the severity and likelihood of the threat.

To provide this assessment and policy recommendations, you will apply your understanding of the technologies involved, cybersecurity, law, foreign policy, international relations, and security theory to synthesize useful policy measures from limited information. Your recommendation must analyze the possible strengths, weaknesses, opportunities, and threats of your proposed response.

In formulating your response, you will be expected to have considered, at a minimum:

- All stakeholders when determining an action or recommendation, including the role of the government and private sector;
- The long and short-term impacts of your recommendation;
- Which agency will be responsible for the action you have recommended;
- Appropriate recommendations for local vs. federal government;
- Whether you can, or should, attribute the threat; and
- The covert or overt nature of your response.

Additionally, this message is accompanied by several documents that may assist your team in preparing the assessment and policy brief for the NSC:

- **Tab 1** – DarkNode Forum Thread
- **Tab 2** – CIA Surveillance Record
- **Tab 3** – Port Operator Email Chain
- **Tab 4** – Washington Post Article
- **Tab 5** – Rabinara Group Report
- **Tab 6** – Internal FBI Memo
- **Tab 7** – Premium Times News Article
- **Tab 8** – Tweets

## Tab 1 – DarkNode Forum Thread

Intelligence Packet: NSA Market Monitor Program

ID #103012205

<b>Threat Level</b>	<b>Moderate (2/5)</b>
<b>Admiralty Code</b>	<b>C4</b>
<b>Event Date</b>	<b>17 May 2020</b>
<b>Source</b>	<b>DarkNode “Cash L4b” Forum</b>
<b>Threat Actor (TA)</b>	<b>Manticore, 1881 Colectiv</b>
<b>TA's Language</b>	<b>English</b>
<b>Targeted Geography</b>	<b>Iran, Romania</b>
<b>Analysts</b>	<b>Alex Turner</b>

### Key Points

1. **Abstract:** During routine network monitoring, analysts came across an English language thread on a dark web forum, DarkNode, hosted in the Asia-Pacific. The thread linked to coordination between Manticore, an Iranian state-sponsored APT, and 1881 Colectiv, a Romanian organized cyber-criminal group. An operative representing Manticore notified its 1881 Colectiv counterpart of a malware payload to enable the modification of bills of lading and container tags in TidalWaves, a cargo management software used by port facilities and shipping operators.

1881 Colectiv operative is instructed by the Manticore operative to install ransomware onto key port systems to camouflage the data manipulation of bills of lading and container tags. The Manticore operative assures its counterpart that there is an opportunity for financial gain in this operation.

This thread might provide insight into Manticore and 1881 Colectiv’s future joint operations.

2. **Audience:** U.S. law enforcement agencies, U.S. and international intelligence agencies.

3. **Source and Validation:** DarkNode has a mixed record of providing actionable information. It has been used as a marketplace for malware and credit card information before, and it has hosted forums used to coordinate illegal online activity. However, it is also a popular

anonymous message board for privacy minded internet users and has hosted discussions from 1881 Colectiv in the past, often focused on stolen credit card credentials and identity theft.

4. Mitigation Summary: We suggest increased monitoring of known Manticore and 1881 Colectiv networks and malware marketplaces to identify targeting or active exploitation of port and maritime infrastructure.

5. IOCs and Attachments: No Relevant IOCs were found.

Source Report: Text of DarkNode forum discussion

1. TA's post on 17 March 2021:

*17/03/2021 0413EST*

**huma79**> are you there?

**zmeu00**> of course

**huma79**> i have some good news. we've developed a way to edit port bills and tags on TW

**huma79**> could be useful in rerouting goods

**zmeu00**> aiurea! are you serious?

**huma79**> you know i don't joke

**huma79**> could you all assist in covering the edits?

*17/03/2021 0438EST*

**zmeu00**> i think so. we could arrange for operators to be barred access

**zmeu00**> of course that would require compensation

**huma79**> oh there's potential for that

**Tab 2 – CIA Field Record**



**SUSPECT:** Klaw aka Kian Ahmadi

**AFFILIATION:** Speculated affiliation with MANTICORE and Iranian state-backed cyber espionage group.

**LAST SIGHTING:** Krakow, Poland on 10/23/2020.

**OPERATOR NOTES:** Identified MANTICORE members are speculated to communicate using in-game chat features in a popular MMO videogame.

User	Message
Klaw	<Klaw has joined the channel by invitation>
Stinger	Kian is here, we can start the game
Sher	Why are we not using VC?
Stinger	Nets too slow for VC
Klaw	Bishoor! Its klaw
Fang	Who made the mistake?
Sher	Klaw has the report
Klaw	Someone tried to activate 2FA
Klaw	They started looking for us on network
Fang	Have they discovered us?
Sher	No
Sher	They’ve been looking for weeks. They don’t realize that we’re in their code
Fang	Klaw how could you be this reckless?
Sher	We have had incredible success jenaab – from BitHub till now no one has caught on
Fang	Yes. A year of diligent work in honor of Suleimani ... wasted
Fang	Are the other pieces in place?
Klaw	Yes. This was a secondary target. They had stronger protections
Fang	Stronger than PoH?
Klaw	PoH had some external protections. Internally? It was super easy, barely an inconvenience to compromise the whole system
Sher	Klaws genius was infecting TWs BitHub. From that success TW gave us access to everything
Stinger	And from everything weve gone to everywhere jenaab. TW is in so many systems, so many ports, even they don’t realize.
Stinger	We have been in hundreds of port systems and have been hard at work with the others
Fang	Until Klaws idiot...
Klaw	Jenaab, He knows his mistake. He was one of the 1881 and has been cut out
Sher	Jenaab we knew this was likely when we brought in others. Perhaps the risk was not worth it
Sher	Spoils are already arriving at home, they suspect nothing. This will be a victory that Suleimani would be proud of
Fang	We aimed beyond their ships and ports.
Stinger	Why? We will steal and cripple their trade – lets see how they like it
Fang	You are right. This was to teach them the pain they gave us
Stinger	Jenaab, we should launch the last update
Klaw	There’s another update?
Fang	Yes, our friends are arranging it. Not your team.
Sher	Stinger stop requesting items from me

Cyber 9/12 Strategy Challenge | Intelligence Report

*Note: All materials included are fictional, unless otherwise marked, and were created for the purpose of this competition. Any resemblance to real persons, organizations, or events is coincidental. All scenario content is the intellectual property of the Atlantic Council unless otherwise specified in writing. This content is licensed for use by our Cyber 9/12 competition partners and students competing in our Cyber 9/12 competitions without fee or compensation, and to all other parties with the written consent of the Atlantic Council. This scenario is developed for academic purposes and is not meant to represent the views of the competition organizers, authors, or any affiliated organizations.*

Fang	S – bia berim get them ready. K – you’ll be informed of when to start the attack
Stinger	Closing lobby and DCing

*// Recorded on 2/26/2021 //*

### Tab 3 – Port Operator Email Chain

**From:** Samantha Gaffer  
**Sent:** Monday, March 8, 2021 at 10:36 a.m.  
**To:** Rose Barleyman  
**Subject:** Possible data degradation

Hi Rose,

I hope you had a nice weekend.

I am reaching out because I noticed some irregularities in our tracking data. I have received a substantial number of emails in the past couple of weeks from distributors complaining that portions of their shipments have failed to be delivered.

This number of failed deliveries suggests that there is likely an error in our tracking data. I have attached these specific complaints, could you look into this problem and compare it to our existing tracking data?

Sincerely,  
Sam

**Samantha Gaffer**  
Head, Customer Relations  
Port of Houston  
Samantha.Gaffer@PortHouston.com

---

**From:** Rose Barleyman  
**Sent:** Monday, March 8, 2021 at 12:17 p.m.  
**To:** Samantha Gaffer  
**Cc:** Ted Sandyman; Fred Bolger  
**Subject:** Re: Possible data degradation

Hi Sam,

Thanks for flagging this for me, as you mentioned our database shows these specific shipments as complete.

I have passed this along to two of my colleagues, who will be looking into the situation on the ground.

Cyber 9/12 Strategy Challenge | Intelligence Report

*Note: All materials included are fictional, unless otherwise marked, and were created for the purpose of this competition. Any resemblance to real persons, organizations, or events is coincidental. All scenario content is the intellectual property of the Atlantic Council unless otherwise specified in writing. This content is licensed for use by our Cyber 9/12 competition partners and students competing in our Cyber 9/12 competitions without fee or compensation, and to all other parties with the written consent of the Atlantic Council. This scenario is developed for academic purposes and is not meant to represent the views of the competition organizers, authors, or any affiliated organizations.*



Ta,  
Rose

**Rose Barleyman**  
Director of Operations  
Port of Houston  
Rose.Barleyman@PortHouston.com

---

**From:** Rose Barleyman  
**Sent:** Monday, March 8, 2021 at 12:26 p.m.  
**To:** Bob Sandyman; Donna Bolger  
**Subject:** Fw: Possible data degradation

Hi Bob and Donna,

Samantha Gaffer emailed me regarding possible irregularities in our tracking data. We have received a significant number of complaints and I worry that this may point to a systemic problem.

I have done some initial research and our data conflicts with the statements of several of our distributors, who claim that their shipments never arrived.

Please look into this.

Ta,  
Rose

**Rose Barleyman**  
Director of Operations  
Port of Houston  
Rose.Barleyman@PortHouston.com

-BEGIN FORWARDED EMAIL-

**From:** Samantha Gaffer  
**Sent:** Monday, March 8, 2021 at 10:36 a.m.  
**To:** Rose Barleyman  
**Subject:** Possible data degradation

Cyber 9/12 Strategy Challenge | Intelligence Report

---

*Note: All materials included are fictional, unless otherwise marked, and were created for the purpose of this competition. Any resemblance to real persons, organizations, or events is coincidental. All scenario content is the intellectual property of the Atlantic Council unless otherwise specified in writing. This content is licensed for use by our Cyber 9/12 competition partners and students competing in our Cyber 9/12 competitions without fee or compensation, and to all other parties with the written consent of the Atlantic Council. This scenario is developed for academic purposes and is not meant to represent the views of the competition organizers, authors, or any affiliated organizations.*

...

---

**From:** Donna Bolger  
**Sent:** Monday, March 8, 2021 at 7:26 p.m.  
**To:** Rose Barleyman  
**CC:** Bob Sandyman  
**Subject:** Fw: Possible data degradation

Hi Rose,

Thank you for sending over the complete list of alleged mismatches in our data.

Bob is looking into data tracking software to trace activity on the dates in question to determine what the cause of these irregularities might be.

We have also evaluated the alleged contents of the disputed shipments to determine if there was a pattern to the missing data. The missing items cover a wide range, from oil refinery equipment to food.

I will keep you updated as our evaluation continues.

Best,  
Donna

# The Washington Post

National Security

Foreign Policy

Justice

Military

## Biden Sanctions Iran After Nuclear Negotiations Fail



By [Omar Rahman](#)

Mar. 16, 2021 at 11:15 EST

Negotiations between Tehran and Washington came to a halt after the Rouhani regime decided to continue their nuclear enrichment efforts. Iranian leadership claims the US is too untrustworthy to commit to a new joint agreement limiting enrichment, to which the US responded to by reinstating sanctions.

Cyber 9/12 Strategy Challenge | Intelligence Report

*Note: All materials included are fictional, unless otherwise marked, and were created for the purpose of this competition. Any resemblance to real persons, organizations, or events is coincidental. All scenario content is the intellectual property of the Atlantic Council unless otherwise specified in writing. This content is licensed for use by our Cyber 9/12 competition partners and students competing in our Cyber 9/12 competitions without fee or compensation, and to all other parties with the written consent of the Atlantic Council. This scenario is developed for academic purposes and is not meant to represent the views of the competition organizers, authors, or any affiliated organizations.*

After oscillating expectations on nuclear compliance from the Obama, Trump, and now Biden Administrations, Iran refused to reenter commitments with the US that could be dismantled by a subsequent presidential administration. In 2015 the Obama Administration successfully implemented the Joint Comprehensive Plan of Action (JCPOA), better known as the Iran Nuclear Deal, which aimed to limit enrichment, increase international oversight, and slow the development of Iran's nuclear capabilities. In exchange for complete compliance, the United Nations, European Union, and US agreed to lift sanctions on Tehran.



In 2018, the US unilaterally left the JCPOA and reinstated sanctions due to Iran's violations of the agreement. Following the 2020 Presidential election, President Biden discussed creating a new nuclear framework with Iran but pledged that national security would remain the highest priority.

Top national security officials are unsurprised by the stalemate. During January 2021's confirmation hearings, Secretary of State Antony Blinken, Secretary of Defense Gen. Lloyd Austin, and Director of National Intelligence Avril Haines all affirmed Iran was far from compliance with the standards set in 2015. They insisted any nuclear deal would depend on the Iranian regime's strict adherence to the former JCPOA's requirements.

Unfortunately, the nuclear enrichment is only one source of tension between Iran and the US. More than a year ago, a US air strike killed top Iranian General Qasem Soleimani as part of the Trump Administration's maximum pressure campaign. Enraged, Iran swore revenge, and analysts say Tehran is still contemplating its response. Recently, a [Twitter](#) account connected to the Iranian Supreme Leader Ayatollah Ali Khamenei was banned for posting a video that appeared to portray former President Trump being killed in an air strike.

The looming threat was accompanied by cyber campaigns intending to disrupt the 2020 US Presidential election. Iranian hackers allegedly published a hit list of US election officials, hoping to intimidate election officials and deter them from working at the polls. If history is any indication, President Biden's Administration can anticipate more Iranian cyber campaigns against the US like those seen in 2015. Without a doubt, US relations with Iran will continue to be shaped by former President Trump's actions.

Another wave of sanctions, a failed nuclear deal, and impending retaliation do not mix well. Iran will remain a top priority for the Biden Administration as they balance maintaining pressure without pushing Iran to a red line.

## Tab 5 – Rabinara Group Report



### MEMBER ALERT: COORDINATED PORT RANSOMWARE

19-Mar-2021

Hello <[REDACTED]>,

Rabinara Group has confirmed ongoing ransomware attacks in the Port of Houston, USA; Port of Corpus Christi, USA and Port of Harcourt, Nigeria.

Rabinara Group amongst its list of services offers expertise in handling maritime cyber incidents. Rabinara Group was first contacted on March 19, 2021 by Port of Houston and Port of Corpus Christi, within minutes of each other and was contacted by Port of Harcourt an hour later.

Rabinara Group's industry partners have reported ongoing campaigns in at least 4 additional ports in South America, Europe, Asia and Australia.



Digital Forensics and Incident Response teams have only just begun their work. Rabinara Group looks to provide its members with 24/7 alerts on issues what we have **confidence** in, which is why you are receiving this alert.

### **Threat actor**

The BASKERVILLE ransomware deployed in affected targets is a known ransomware attributed to the 1881 Colectiv, a ransomware crew that operates out of Romania. Rabinara Group has tracked their activity before and has advised clients on how to prevent exploitation.

### **Impact**

Initial findings from our Austin team that was deployed to the Port of Houston confirmed that BASKERVILLE has compromised entire port systems most critically, email services and cargo manifest systems – including digital backups. Other impacted systems include access management software preventing easy access to secure facilities and gated areas.

Port Traffic Control, Gantry and Trolley systems remain online and active, allowing vessels to berth.

Cargo cannot be unloaded due to the ransomware that has impacted the cargo manifest systems.

### **Implications**

Rabinara Group has long advocated for stronger cybersecurity at ports and across maritime systems. Maritime commerce accounts for 90% of all global trade tonnage, yet these systems continue to remain woefully open to exploitation and are hamstrung by poor network segmentation and cybersecurity practices allowing adversaries widespread access to port systems.

Due to these systemic vulnerabilities, Rabinara Group cannot confidently account the degree of damage and is committed to providing both a determination on the origin of this breach, as well as securing our client systems from further exploitation.

The Rabinara Group will continue working round the clock to resolve this situation for our clients in the US and internationally.

Best,  
Jose Mancía  
Co-Founder, Rabinara Group



Rabinara Group  
770 Broadway, New York, NY 10003  
*Gold Award, Threat Intel | Fortune 500 Clients | Exceptional People, Exceptional Results*

## Tab 6 – Internal FBI Memo

**TOP SECRET// HCS-O// REL TO USA FVEY//**



**TO:** CHRISTOPHER GALLAGHER, DIRECTOR  
FEDERAL BUREAU OF INVESTIGATION,  
WASHINGTON DC

**DATE:** MAR 23 2021

**FROM:** ESTE KARO, ASSISTANT DIRECTOR, CYBER DIVISION  
CRIMINAL, CYBER, RESPONSE, AND SERVICES BRANCH  
FEDERAL BUREAU OF INVESTIGATION  
WASHINGTON DC

**RE:** INTERPOL ARRESTS '1881 COLECTIV' MEMBER

**TS//HCS-O//OC/REL TO USA, FVEY**

(U//FOUO) INTELLIGENCE PURPOSES ONLY: (U//FOUO) The information in this report is provided for intelligence purposes only but may be used to develop potential investigative leads. No information contained in this report, nor any information derived therefrom, may be used in any proceeding (whether criminal or civil), to include any trial, hearing, or other proceeding before any court, department, agency, regulatory body, or other authority of the United States without the advance approval of the Attorney General and/or the agency or department that originated the information contained in this report. These restrictions apply to any information extracted from this document and used in derivative publications or briefings.

(TS//FVEY) The purpose of this memorandum is to advise you of a recent arrest of Mihai Iordan (SUBJECT) made by Interpol in Romania. SUBJECT was identified as a key member of the Romanian cyber-criminal group 1881 Colectiv by an international intelligence database. Information gathered from SUBJECT throughout questioning suggests SUBJECT may be connected to a recent pattern of short selling of shipping and petroleum companies flagged by the US Securities and Exchange Commission (SEC). Suspecting criminal activity based on the persistent and targeted nature of this activity, the SEC notified FBI White Collar Crime Division of these activities. In coordination with the SEC, FBI Cyber Division launched an investigation into the alleged criminal activity.

(TS//FVEY) SUBJECT was arrested by Romanian police on FEB 27 2021 on charges of drunk and disorderly conduct. INTERPOL flagged his arrest and connected him to a series of ransomware attacks against Romanian and Hungarian healthcare facilities in 2019/2020, which were tied to the Romanian cyber-crime group 1881 Colectiv. SUBJECT was then transferred to the custody of INTERPOL in Romania.

Cyber 9/12 Strategy Challenge | Intelligence Report

*Note: All materials included are fictional, unless otherwise marked, and were created for the purpose of this competition. Any resemblance to real persons, organizations, or events is coincidental. All scenario content is the intellectual property of the Atlantic Council unless otherwise specified in writing. This content is licensed for use by our Cyber 9/12 competition partners and students competing in our Cyber 9/12 competitions without fee or compensation, and to all other parties with the written consent of the Atlantic Council. This scenario is developed for academic purposes and is not meant to represent the views of the competition organizers, authors, or any affiliated organizations.*

(S// FVEY) Due to SUBJECT's work with 1881 Colectiv, INTERPOL, in coordination with Romanian Police, detained and charged SUBJECT for conspiracy to commit wire fraud, illegal access to information systems and illegal system interference in connection with recent ransomware attacks.

(S//FVEY) While questioning SUBJECT, officers leveraged their knowledge of his activities relating to the ransomware cases to press for information regarding 1881 Colectiv. SUBJECT implied he had valuable information regarding the current workings of 1881 Colectiv and would pass on this information in exchange for a significantly reduced punishment in a minimum-security prison. Law enforcement agreed to a deal depending on the value of SUBJECT's information.

(TS// FVEY) Under further interrogation, SUBJECT confessed "a recent mistake" terminated his work with 1881 Colectiv, but swore he had information on "game-changing developments" 1881 Colectiv is involved in. SUBJECT boasted of his role in executing BASKERVILLE but promised "the worst was yet to come."

(TS// FVEY) INTERPOL learned 1881 Colectiv was actively shorting shipping and petroleum company stocks by orders from anonymous partners and cutouts. Stock manipulation followed by BASKERVILLE attacks on the same companies, earned 1881 Colectiv millions. SUBJECT expressed medium confidence a small portion of those profits were transferred to their anonymous partner. INTERPOL attributes stock manipulation to odd bribery efforts.

(S//FVEY) INTERPOL officers immediately investigated the validity of these claims and found a pattern of suspicious trading and ransomware attacks against these sectors across the globe in the previous weeks, matching SUBJECT's statement. Several of the companies targeted are based in or operate within the United States, thus the full report, including the complete Interpol and Romanian police files on 1881 Colectiv and SUBJECT's full statement, was sent to the FBI Cyber Division.

(S//FVEY) FBI Cyber Division launched an investigation into SUBJECT's claims and the intelligence provided by our INTERPOL partners. FBI Cyber Division is also in close coordination with contacts at the SEC in the ongoing investigation of suspicious trading patterns. FBI Cyber Division will provide updates as the investigation continues and welcomes all feedback and direction.

**CLASSIFIED UNTIL: MAR 23, 2071**

**TOP SECRET// HCS-O// REL TO USA. FVEY//**

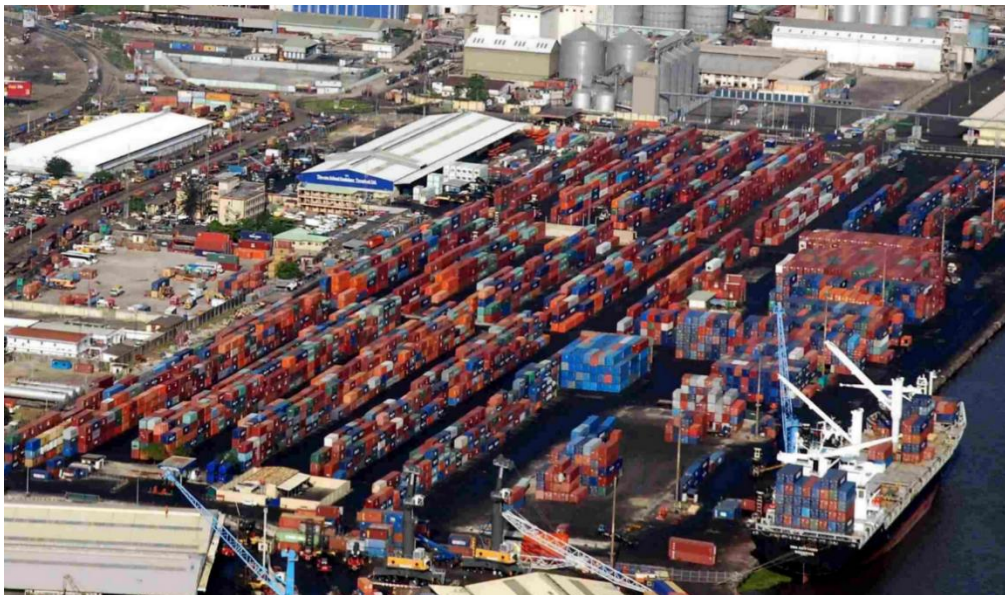
Cyber 9/12 Strategy Challenge | Intelligence Report

*Note: All materials included are fictional, unless otherwise marked, and were created for the purpose of this competition. Any resemblance to real persons, organizations, or events is coincidental. All scenario content is the intellectual property of the Atlantic Council unless otherwise specified in writing. This content is licensed for use by our Cyber 9/12 competition partners and students competing in our Cyber 9/12 competitions without fee or compensation, and to all other parties with the written consent of the Atlantic Council. This scenario is developed for academic purposes and is not meant to represent the views of the competition organizers, authors, or any affiliated organizations.*





## Ransomware Campaign Spells Trouble in Port Harcourt



*A ransomware attack has brought operations in Port Harcourt and other ports around the world to a standstill.*

By **Omolola Boafa** – March 25, 2021 4 min read

On March 19, operators in the Port of Harcourt detected unusual activity on port networks. At Port Harcourt, basic operations can be difficult on a normal day, the last thing port operators and managers needed was ransomware attack.

Since then, energy exports have been most immediately impacted. The Ministry of Energy predicts this cyberattack may result in a regional energy crisis as Port Harcourt's two refineries have a combined capacity of 210,000 barrels per day.

“While port operations have come to a standstill, Port Harcourt’s IT and Security teams are hard at work responding to the incident,” said Executive Director of the Port of Harcourt, Nigella Adewunmi. “Staff are working around the clock to resume port operations and alleviate congestion along the Bonny River.”

To complicate matters further, tens of millions of metric tons of food aid from the USAID Food for Peace program is received through Port Harcourt. This aid ensures that some 1.8 million Nigerians displaced by Boko Haram in the Adamawa, Borno, and Yobe states can have meet their daily food needs.

“Northeastern Nigeria has been gripped by conflict for over a decade now,” says Alison Mosshart, spokesperson for USAID’s Office of Food for Peace (FFP). “This conflict has displaced Nigerians and ravaged their livelihoods as well. USAID’s FFP offers life-saving assistance to millions. Any delays will be felt immediately by those who are the most vulnerable in Nigeria.

Delays in food shipments will result in millions of Nigerians experiencing acute food insecurity, especially in regions already experiencing violence and instability at the hands of Boko Haram.

## Tab 8 – Tweets



CNN Breaking News

@cnnbrk



(1/3) BREAKING: TidalWaves, a Port Management System with “clients in every country where ships carry cargo,” was compromised by a potentially devastating cyber-attack. Officials are still scrambling to recover from large ransomware attack on Texas and Nigerian Ports earlier...

8:38 AM · Mar 23, 2021

79.5K Retweets 1.2K Quote Tweets 17.2K Likes



CNN Breaking News

@cnnbrk



(2/3) ...this month. Port workers are searching for missing cargo impacted by the attack. TidalWaves attackers are unknown, but many customers, including government agencies, are likely compromised. Cybersecurity experts believe this is a supply chain attack and intruders have...

8:39 AM · Mar 23, 2021

73.6K Retweets 31.1K Quote Tweets 79.3K Likes





CNN Breaking News   
@cnnbrk




(3/3)...been in the system for months, slowly expanding access. Full extent of infiltration is unclear but the attack could impact customers worldwide. A senior CISA official confirmed TidalWaves breach is responsible for shipment issues at US and Nigerian Ports.

8:39 AM · Mar 23, 2021

73.3K Retweets 22.3K Quote Tweets 75.4K Likes



Rep. Dallas Briscoe   
@DallasfromHtown



Despite the attacker's best efforts, attacks on the Port of Houston were unsuccessful. I personally visited the Marina today and can confirm all boats, including mine, are undamaged! We are [#HoustonStrong](#).

12:00 PM · Mar 25, 2021

8.8K Retweets 416 Quote Tweets 7.9K Likes





TIDAL  
@TIDAL



TIDAL is NOT AFFILATED with TidalWaves or the recent cyber-attacks. Our unlimited music and videos are safe for streaming right now!

5:56 PM · Mar 26, 2021

108 Retweets 21 Quote Tweets 2.6K Likes



The Weather Channel  
@weatherchannel



There is NO extreme weather expected in Houston or anywhere on the Texas coast. TidalWaves is a software company that is UNRELATED to potential tsunamis, tidal waves, or dangerous weather.

10:22 PM · Mar 26, 2021

108 Retweets 21 Quote Tweets 2.6K Likes



# Cyber 9/12 Strategy Challenge

## Intelligence Report II

### INSTRUCTIONS

**Please read these instructions carefully. They have changed from previous years.**

Your team will take on the role of experienced policy advisers, part of a hypothetical cybersecurity task force, preparing to brief the National Security Council (NSC). This packet contains fictional information on the background and current situation involving a major cyber incident affecting US systems. The attacks notionally take place in Spring 2021 in a world where the **SolarWinds compromise never occurred**. The scenario presents a fictional account of political developments and public reporting surrounding the cyber incident.

The NSC needs information on the full range of response options available regarding this incident. Your team has been tasked with developing an appropriate course of action for recommending to the NSC.

You are to consider as facts the following pages for formulating your response.

**You will use the fictional scenario material presented to perform two tasks:**

**Oral Policy Brief (Day 2):** For the first day of the competition, prepare a ten-minute oral presentation outlining your impact and risk assessment, as well as your suggested course of action. You will present to a panel of judges playing the role of the NSC.

**Decision Document (Day 2):** Teams will also be required to submit a “decision document” accompanying their oral presentation at the beginning of the competition round. The “decision document” will be a maximum of one single-sided page in length, outlining the team’s response options, decision process, and recommendations. The teams should note that the document is not intended to summarize every detail of the recommendations, but to help the judges follow the oral presentation, and the judges will be given only 2 minutes to read it before the presentation begins. The document should be written with the goal of assisting busy senior officials to quickly grasp your team’s recommendations and analysis.

**Keep these tips in mind as you are reading and considering your policy response alternatives:**

- *Analyze the issues.* The goal of the competition is for competitors to grapple with complex issues and weigh the strengths and weaknesses of potentially conflicting interests. Priority should be given to analysis of the issues and not to listing all possible issues or solutions.
- *Engage the scenario.* Believe that the universe we have created is plausible and that the events that happen in it are realistic. Nevertheless, remember to think critically about the intelligence you have been provided and its provenance.
- *Think multi-dimensionally.* When analyzing the scenario, remember to consider implications for other organizations and domains (e.g. private sector, military, law enforcement, different levels of government, diplomatic) and incorporate these insights along with cybersecurity.

Cyber 9/12 Strategy Challenge | Intelligence Report

*Note: All materials included are fictional, unless otherwise marked, and were created for the purpose of this competition. Any resemblance to real persons, organizations, or events is coincidental. All scenario content is the intellectual property of the Atlantic Council unless otherwise specified in writing. This content is licensed for use by our Cyber 9/12 competition partners and students competing in our Cyber 9/12 competitions without fee or compensation, and to all other parties with the written consent of the Atlantic Council. This scenario is developed for academic purposes and is not meant to represent the views of the competition organizers, authors, or any affiliated organizations.*

- *Consider who you are, and who you're briefing.* You are experienced cyber policy professionals briefing the National Security Council. As such, you should be ready to answer questions on agency responsibility, provide justifications for your recommendations, and have potential alternatives ready.
- *Be creative.* Cyber policy is an evolving discourse, and there is no single correct course of action to the scenario information provided. There are many ideas to experiment with in responding to the crisis.
- *Don't fight the scenario.* Unless stated otherwise, assume all inter-state relations, policies, and treaties have remained the same as they were in March 2021. Explore the implications of that information, not the plausibility. **The only exception to this is that in this scenario, students should work with the assumption that the SolarWinds hack never occurred.**

Given the unclear nature of the threat, the NSC requests that your team prepare a concise assessment of the ongoing situation and reporting. Your assessment should include:

- How or where the relevant systems could be vulnerable to exploit, and what steps can be made to mitigate these vulnerabilities;
- An assessment of potential risks and impacts to consider if the vulnerabilities are successfully exploited; and
- Responses the NSC can or should consider addressing these vulnerabilities, taking into account the severity and likelihood of the threat.

To provide this assessment and policy recommendations, you will apply your understanding of the technologies involved, cybersecurity, law, foreign policy, international relations, and security theory to synthesize useful policy measures from limited information. Your recommendation must analyze the possible strengths, weaknesses, opportunities, and threats of your proposed response.

In formulating your response, you will be expected to have considered, at a minimum:

- All stakeholders when determining an action or recommendation, including the role of the government and private sector;
- The long and short-term impacts of your recommendation;
- Which agency will be responsible for the action you have recommended;
- Appropriate recommendations for local vs. federal government;
- Whether you can, or should, attribute the threat; and
- The covert or overt nature of your response.

Additionally, this message is accompanied by several documents that may assist your team in preparing the assessment and policy brief for the NSC:

- **Tab 1** – Mariner GChat
- **Tab 2** – US Coast Guard Memorandum
- **Tab 3** – Atlantic Council Fast Thinking Post
- **Tab 4** – US Embassy in Abuja Press Release
- **Tab 5** – Social Media Post
- **Tab 6** – Reuters News Article

Cyber 9/12 Strategy Challenge | Intelligence Report

*Note: All materials included are fictional, unless otherwise marked, and were created for the purpose of this competition. Any resemblance to real persons, organizations, or events is coincidental. All scenario content is the intellectual property of the Atlantic Council unless otherwise specified in writing. This content is licensed for use by our Cyber 9/12 competition partners and students competing in our Cyber 9/12 competitions without fee or compensation, and to all other parties with the written consent of the Atlantic Council. This scenario is developed for academic purposes and is not meant to represent the views of the competition organizers, authors, or any affiliated organizations.*

- **Tab 7** – Press Release from MTS-ISAC
- **Tab 8** – Email Exchange between EC3 and FBI
- **Tab 9** – ODNI Report to the NSC



## Tab 1 – Mariner GChat



### Party on Garth

6 members

Thu, Sep 10, 2020

#### Will Swann

I can't believe that the new Nicholas Cage movie finally came out and there's no way to watch it – most advanced navy my ass. My gf has almost spoiled it for me twice.

#### Keira Gibbs

What movie, Tenet? And yea seriously, I can't wait to gtfo this ship

#### Will Swann

Hell yea, it looks sweet

#### Jack Pearl

I saw it! It was surprisingly good. I have a buddy at Houston who sends me new movies and TV shows. I could pass along his info if y'all want?

**Will Swann**

That would be awesome dude, I need to get back in the loop of things. Can we get them on USB? I need something that'll work while I'm stuck at the engineering deck

**Keira Gibbs**

Could I get those copies as well? Does he have The Boys? my little brother and I watched the first season together and he really wants to talk to me about it

**Jack Pearl**

Yea, no prob guys, he can probably get you some USBs next time we're in Houston

**Will Swann**

Do you mind if I tell my bunkmates? I'm sure they'll wanna know where I got the goods haha

**Jack Pearl**

Fine by me, just no narcing lol

## Tab 2 – US Coast Guard Memorandum

U.S. Department of  
Homeland Security

United States  
Coast Guard



### MEMORANDUM

April 2, 2021

**From:** Rebecca Tova, CMDR  
First Coast Guard District

**To:** Samuel Teek, RDML  
COMDT (CG-2)

**Subj:** MALWARE DISCOVERED AT PORT OF NEW YORK – INVESTIGATION UNDERWAY

1.Purpose. Malware was discovered during a routine scan of an incoming cargo ship at the Port of New York. Further investigation concluded that this malware was inactive. At this time, attribution is uncertain, but an investigation is underway to determine the spread and possible impact of this malware.

2.Situation. On the morning of April 1, 2021, US Coast Guard personnel at the Port of New York conducted an inspection of the cargo ship, Obsidian Sun. The inspection produced evidence that the ship's networks were infected with malware.

In response, Coast Guard personnel onsite contacted the FBI and sent an incident response team to assess the situation. During the course of this investigation, the Port of New York Harbormaster determined that the Obsidian Sun should be prevented from docking at Port in order to limit the opportunity for the malware to spread. This decision was made in coordination with the US Coast Guard.

The response team determined that the ship was infected with an unknown variant of malware, with fingerprints evidenced throughout the network. Analysts determined that this malware is currently inactive, with no evidence of communication with an external command-and-control server. The malware appears to have been introduced to the ship's system directly, though it is unclear exactly how the initial infection occurred and whether it was a single incident.

Analysis of the tactic, tools, and procedures (TTP) that we are aware of at this point, including the malware itself, do not point conclusively to an attributable actor. However, some markers match intelligence on several international cybercriminal groups, including 1881 Colectiv, based in Romania.

Cyber 9/12 Strategy Challenge | Intelligence Report

*Note: All materials included are fictional, unless otherwise marked, and were created for the purpose of this competition. Any resemblance to real persons, organizations, or events is coincidental. All scenario content is the intellectual property of the Atlantic Council unless otherwise specified in writing. This content is licensed for use by our Cyber 9/12 competition partners and students competing in our Cyber 9/12 competitions without fee or compensation, and to all other parties with the written consent of the Atlantic Council. This scenario is developed for academic purposes and is not meant to represent the views of the competition organizers, authors, or any affiliated organizations.*

This group is primarily known for executing ransomware attacks against hospitals in Eastern Europe, and it is unclear what connection this group would have with Obsidian Sun.

Obsidian Sun is operated by Naranpa Shipping Ltd, based in Hong Kong. The company was initially cooperative in our investigation, however, this morning communications directly from the company ceased and instead have been routed through the prominent law firm, Xiala. The ship flies under the Liberian flag, a common practice used to avoid taxes and regulation.

Before entering New York Harbor, the Obsidian Sun made one stop in the Port of Miami, after having crossed the Atlantic Ocean from the Port of Harcourt, in Nigeria. Because of this route and stops, at this moment, it is not possible to determine where the malware was introduced to the ship's system.

Coast Guardsmen and Port of New York staff are implementing safeguards to prevent the spread of this malware and continue to encourage best cyber safety practices. Scans of incoming ships, especially from the Port of Miami and the Port of Harcourt have been increased until the conclusion of this investigation.

## Tab 3 – Atlantic Council Fast Thinking Post



### JUST IN

Beijing has offered Port Harcourt operators incident response support as the Nigerian port grapples with an unprecedented ransomware attack. The attack first disclosed late last month, has sparked a regional energy crisis and food shortages across the Adamawa, Borno, and Yobe states in Nigeria—states already destabilized and vulnerable due to activities of the insurgent group Boko Haram.

Jupitech 360, a Chinese cybersecurity firm, has published a report on the attack, highlighting an exploit used and linking it to the leaked cache of data and vulnerabilities orchestrated by the Shadow Brokers in 2016.

### TODAY'S EXPERT REACTION COURTESY OF

- **Dr. Mabel Edwards**, Resident Fellow

### GREAT POWER COMPETITION IN NIGERIA

Historically, Chinese soft power in Nigeria has taken the form of investments in the Nigerian energy sector and infrastructure. As Abuja responds to this debilitating cyberattack, we could see increased competition between the United States and China, both seeking to offer incident response support and information to help Nigerian authorities recover from the attack and identify the perpetrators. Washington's interests so far have been tied to USAID Food for Peace shipments that have been delayed by the ransomware attacks. Whichever direction Abuja decides to move, the Nigerian government should be wary of Chinese support and intelligence. After all, Beijing has a [track record](#) of politicizing cyber incidents and intelligence as well as [spying](#) on its nominal friends in the region.

## Tab 4 – US Embassy in Abuja Press Release



U.S. Embassy & Consulate  
in Nigeria



### U.S. Statement on Port Harcourt Ransomware Attacks, Affirms Commitment to Partnership with Nigeria

On April 8, 2021 Ambassador Adrienne Hardaway issued a statement reaffirming the United States’ support of Nigeria amid the instability caused by ransomware attacks on the Port of Harcourt.

Ambassador Hardaway remarked, “Washington is standing by Abuja as Port Harcourt operators and the government of Nigeria work tirelessly to respond to the ransomware attack that has precipitated an energy crisis across Western Africa and accelerated food insecurity among Nigeria’s most vulnerable populations, already experiencing violence and displacement from Boko Haram.

As we celebrate 60 years of U.S.-Nigeria diplomatic relations, we look forward to continued collaboration on transnational cyber threats and offer our Nigerian partners our technical expertise, operational support and information sharing capabilities through our Cybersecurity and Infrastructure Security Agency wherever they may be of most use. Certain companies’ assessments of the incident at Port Harcourt threaten to politicize threat intelligence and adversely impact critical relationships across an already inflamed situation and an important region of the world. We hope all parties will focus on collaborating with speed and apolitical intentions so as to recover this critical facility and avoid unwarranted tension.”

USAID’s Office of Food for Peace (FFP) provides assistance for millions of Nigerians impacted by the ongoing conflict with Boko Haram. The slowdown in Port Harcourt has caused delays for FFP shipments, threatening acute food instability across the parts of the region.

“We stand ready to support Nigerian authorities in whatever way we can to remedy this terrible crime and support our two nations continued journey towards stable peace and prosperity,” said Ambassador Hardaway.

---

By U.S. Mission Nigeria | 8 April 2021 | Topics: Ambassador, News, Press Releases |  
Tags: Cybersecurity

## Tab 5 – Social Media Post

↑  
39.4k  
↓

 **r/PoliticalHumor** · Posted by [u/DaFunkJunkie](#) 4 hours ago  9  3  13  7

**Finally, someone speaking out on the REAL threat to Nigeria. Ghana must be held accountable #ExposeGhana**



**Musa**  
@MrGwagwalada

Why are these Nigerian Ports bearing the brunt of these cyberattacks? Ghana is mobilizing their growing cybercriminal network to undermine the Nigerian energy sector. It's time to WAKE UP! This is an intentional move at stifling the Nigerian energy industry and harming citizens.

3:10 PM · Apr 15, 2021

315 Retweets 124 Quote Tweets 1.4K Likes

2.2k Comments Share ... 84% Upvoted

Log in or sign up to leave a comment

Log In

Sign Up

SORT BY BEST

[View discussions in 3 other communities](#)



**Blackcat9285** 14 hours ago

Nigerians must unite to speak out against Ghanaian attacks on our country! We must use our voices to incite change.

Many of us are gathering in front of the Embassy of Ghana in Abuja this weekend to protest. Join us, we are stronger together! Smaller protests will be carried out at Port Harcourt and Tin Can Island Port as well! Come ready to use your voice and make our leaders listen! Nigerians must come together and show we will not tolerate such blatant attacks.



**Ibrahim505** 13 hours ago

Is protesting enough?! We must take real action if we want to be heard and respected. The government is too busy stealing our money to listen.

Also keep in mind Boko Haram could use this opportunity to attack our villages, please prepare to defend yourselves and your families.



**firenthud2010 13 hours ago**

Yes, we cannot allow ourselves to be attacked! We must respond.



**pizzahoarder2 12 hours ago**

Yes!! I'm glad to see someone uncovering the truth. Ghana has hidden behind the scenes and international superpowers for too long! Hopefully allies will realize the Ghanaian cyber threat and stand by us to combat it. I've covered this extensive on my blog [bit.ly/863hdg](http://bit.ly/863hdg)

Nigeria doesn't need the allies to fight its battles! Nigerian leaders and citizens can take action on their own. #ExposeGhana



**tranquilitybase1 12 hours ago**

So true! It is evil what Ghana is doing to Nigerian citizens. Many cities are facing food shortages because of missing shipments. Will they have us starve?

It is already difficult to get food in some villages, we mostly grow our own, but halting imports and diverting food aid is only making it worse.

I know some families have been without food for days.



**relegatedustbin 12 hours ago**

^^my family is also without food, inshallah this will be over soon.

Ghanaian cybercriminals have become so successful because big powers are distracted by each other. They are some of the most active and dangerous cybercriminals operating today.



**blacktreacle86 11 hours ago**

There is too much focus on the Russians, Iranians, and North Koreans! These Ghanaian hackers are wreaking havoc unnoticed!



## Tab 6 – Reuters News Article



TECHNOLOGY & CYBER SECURITY

APRIL 26, 2021 / 4:32 PM / UPDATED 3 HOURS AGO

# Cyberattacks on ports spread beyond Nigeria

By Jason Mutulu

2 MIN READ



PORT HARCOURT, Nigeria ( Reuters ) – Devastating ransomware attacks have ravaged ports worldwide since March 25. Port officials have scrambled to obtain shipments, track missing cargo, and secure their systems. Ports on all continents, besides Antarctica, have been impacted by the ransomware attacks. The Port of Corpus Christi Texas, a port boasting six refineries that normally exports an average of 1.3 million barrels per day (BPD), has been forced to decrease output to approximately 600,000 BPD since disclosure of the ransomware attack.

Now, cybersecurity experts fear the criminals behind this attack are expanding their efforts.

Companies impacted by the ransomware have reported suspicious emails requesting invoice information or filled with incorrect invoices. Many of these suspicious requests are being shared online, between companies to confirm their authenticity.

Business leaders are strongly cautioning their employees and customers from engaging with any suspicious emails in case they contain malware. Amid all the confusion of missing cargo and containers, port managers and wholesalers are struggling to distinguish the truth.

“We can’t keep up,” one port officials speaking under the condition of anonymity admitted. “We’re searching for missing containers, trying to prevent any more mistakes, and scrutinizing emails is exhausting.”

Cybersecurity analysts say this was a carefully orchestrated campaign. Potentially the most meticulous and far-reaching attack we’ve seen,” a cybersecurity expert said.

Experts have confirmed that the additional emails targeting impacted businesses and their customers are part of a larger phishing scheme to introduce more malware into compromised businesses. The financial and logistical strain of continued ransomware attacks threaten to hamstring businesses and the international trade system.

Cyber 9/12 Strategy Challenge | Intelligence Report

*Note: All materials included are fictional, unless otherwise marked, and were created for the purpose of this competition. Any resemblance to real persons, organizations, or events is coincidental. All scenario content is the intellectual property of the Atlantic Council unless otherwise specified in writing. This content is licensed for use by our Cyber 9/12 competition partners and students competing in our Cyber 9/12 competitions without fee or compensation, and to all other parties with the written consent of the Atlantic Council. This scenario is developed for academic purposes and is not meant to represent the views of the competition organizers, authors, or any affiliated organizations.*

It's a wakeup call to the world, that cyber indeed has physical consequences.

Reporting by Jason Mutulu in Lagos; additional reporting by Erin Xi, Ada Ajibola

*Our Standards: The Thomas Reuters Trust Principles*

## Tab 7 – MTS-ISAC Press Release



# The MTS-ISAC Calls for Urgent International Action on Ransomware Affected Ports & Vessels

Apr 27 2021

WILMINGTON, DELAWARE, US, April 27, 2021 / -- The Maritime Transportation System Information Sharing and Analysis Center (MTS-ISAC) is calling for an international coordinated response to the strain of ransomware known as BASKERVILLE that has infected 43 ports across the world, a campaign that is still underway.

On March 23, it was reported that criminal actors had inserted malware using the cargo management software provided to customers by the tech company TidalWaves. TidalWaves CEO, Ravindra Radhakrishnan rebutted the criminal theory stating, “We are witnessing an attack by an adversary with top-tier offensive capabilities.”

Working with our partners, both domestic and internationally, the MTS-ISAC has assessed the ransomware epidemic to be one of the most significant ever to impact the maritime industry and calls for action. This attack represents a broad and successful assault on international trade and transportation, which has exploited not only a key aspect of the software supply chain but the supply chain of the entire global economy.

Almost thirty days after the initial attack, a backlog of 74 ships remain outside the port of Houston, their cargo unable to be unloaded. The impact of these attacks and delays is already estimated to have cost more than \$950 billion worldwide.

Yet our concern does not stop there. Within the United States, several vessels across ports in Houston, Wilmington, Delaware; Long Beach and New York have reported suspicious activity and breaches of security aboard their vessels.

These adversaries have targeted the very lifeblood of the global economy and the assault is underway. The MTS-ISAC and our partners across the maritime industry strongly urge tech companies, the US government, and international partners around to work together to identify, target and apprehend these adversaries.

This is not just an attack on specific targets, but on the trust and reliability of the world’s critical infrastructure in order to fill the short-minded ambitions of cyber criminals.

## Tab 8 – Email Exchange between EC3 and FBI

**Date:** 1 May 2021

**To:** [james.y.johnson@fbi.gov](mailto:james.y.johnson@fbi.gov)

**From:** [igheate@ec3.europol.org](mailto:igheate@ec3.europol.org)

**Subject:** Arrest of 1881 Colectiv Operatives

Good Afternoon Colleagues,

On 30 April 2021, our team successfully detained suspects we believe to be connected to recent global ransomware attacks. With the intelligence shared and information from the Colectiv 1881 member Interpol arrested in March, we identified and tracked down a handful of operatives linked to 1881 Colectiv, as well as to the attacks.

We are currently interviewing these operatives to learn more about the attack, TTPs used and the group's plans and motives.

We welcome any additional information you may have about 1881 Colectiv, its members, or other leads to follow as we work together to stop these attacks.

Sincerely,

Officer Gheata

Contract Agent, Europol's European Cybercrime Center

**Date:** 1 May 2021

**To:** [igheate@ec3.europol.org](mailto:igheate@ec3.europol.org)

**From:** [james.y.johnson@fbi.gov](mailto:james.y.johnson@fbi.gov)

**RE:** Arrest of 1881 Colectiv Operatives

Dear Officer Gheata,

Congratulations on the arrests. From our understanding, 1881 Colectiv is an active criminal group, known to hack for hire. They've offered their services to bidders in and outside of Europe in the past and appear to be most interested in profitability and the high drama of visible attacks on widely used services and infrastructure.

Our intelligence suggests 1881 Colectiv may collaborate with other cyber groups when convenient or lucrative. As of late, we have noticed an uptick in communications between 1881 operatives and an actor with potential ties to Iran. Has your team discovered any links between 1881 Colectiv and other cyber groups or state actors related to this attack? Might the operatives in your custody have any information on the missing cargo shipments?

Thanks for the update and your diligent work. Let's please keep in touch as our leadership consider next steps and the possibility of an indictment.

Respectfully,

James Johnson

Special Agent, Division Chief FBI Cybercrime Cente

Cyber 9/12 Strategy Challenge | Intelligence Report

---

*Note: All materials included are fictional, unless otherwise marked, and were created for the purpose of this competition. Any resemblance to real persons, organizations, or events is coincidental. All scenario content is the intellectual property of the Atlantic Council unless otherwise specified in writing. This content is licensed for use by our Cyber 9/12 competition partners and students competing in our Cyber 9/12 competitions without fee or compensation, and to all other parties with the written consent of the Atlantic Council. This scenario is developed for academic purposes and is not meant to represent the views of the competition organizers, authors, or any affiliated organizations.*

## Tab 9 – ODNI Report to the NSC



# Ransomware Impacts on Shipping Logistics; May 2021 (TS//SI//OC/REL TO USA, FVEY/FISA)

(U//FOUO) INTELLIGENCE PURPOSES ONLY: (U//FOUO) The information in this report is provided for intelligence purposes only but may be used to develop potential investigative leads. No information contained in this report, nor any information derived therefrom, may be used in any proceeding (whether criminal or civil), to include any trial, hearing, or other proceeding before any court, department, agency, regulatory body, or other authority of the United States without the advance approval of the Attorney General and/or the agency or department that originated the information contained in this report. These restrictions apply to any information extracted from this document and used in derivative publications or briefings.

### SUMMARY

[REDACTED] (TS//SI//OC/REL TO USA, FVEY/FISA) On May 6 2021, under NSC recommendation, CIA and National Geospatial Intelligence Agency have increased operational surveillance shipping operations and containers in ports impacted by recent ransomware attacks. Many shipments appear to have been misplaced as result of ransomware attacks, reaffirming claims from US defense contractors that containers with critical equipment are missing. In particular, one company cannot locate a several containers with critical equipment for surface-to-air missiles and another is missing a shipment of medical equipment intended for the US Thumrait Air Base in Oman.

The ransomware toolkit instrumental for the attacks has been leaked following a series of arrests of 1881 Colectiv operatives in Romania.

It is assessed with high confidence that criminal groups around the world have mobilized and are utilizing the 1881 Colectiv kit. Its usage is already prevalent across Western Africa where criminal groups are leveraging the ransomware to target local offices of US companies and vendors already impacted by earlier attacks and struggling to patch legacy systems.

The continued congestion at the Port of Harcourt tied with significantly greater loss or misplacement of cargo than under normal operations, the widening scope of the ransomware attacks, broader disruption of maritime transportation systems, and possible disruption to energy flows through the region pose a significant national security risk to the United States. There has already been disruption to USAID Food for Peace shipments intended for populations in Nigeria displaced by Boko Haram, impeding the US Government's ability to support the Nigerian government and strengthen bilateral cooperation. China's continued success in exerting economic influence in the region should be of concern, especially as Beijing shifts its focus by offering technical support during a cyber crisis.

# Cyber 9/12 Strategy Challenge

## Intelligence Report III

### INSTRUCTIONS

**Please read these instructions carefully. They have changed from previous years.**

Your team will take on the role of experienced policy advisers, part of a hypothetical cybersecurity task force, preparing to brief the National Security Council (NSC). This packet contains fictional information on the background and current situation involving a major cyber incident affecting US systems. The attacks notionally take place in Spring 2021 in a world where the **SolarWinds compromise never occurred**. The scenario presents a fictional account of political developments and public reporting surrounding the cyber incident.

The NSC needs information on the full range of response options available regarding this incident. Your team has been tasked with developing an appropriate course of action for recommending to the NSC.

You are to consider as facts the following pages for formulating your response.

**You will use the fictional scenario material presented to perform two tasks:**

**Oral Policy Brief (Day 2):** For the first day of the competition, prepare a ten-minute oral presentation outlining your impact and risk assessment, as well as your suggested course of action. You will present to a panel of judges playing the role of the NSC.

**Keep these tips in mind as you are reading and considering your policy response alternatives:**

- *Analyze the issues.* The goal of the competition is for competitors to grapple with complex issues and weigh the strengths and weaknesses of potentially conflicting interests. Priority should be given to analysis of the issues and not to listing all possible issues or solutions.
- *Engage the scenario.* Believe that the universe we have created is plausible and that the events that happen in it are realistic. Nevertheless, remember to think critically about the intelligence you have been provided and its provenance.
- *Think multi-dimensionally.* When analyzing the scenario, remember to consider implications for other organizations and domains (e.g. private sector, military, law enforcement, different levels of government, diplomatic) and incorporate these insights along with cybersecurity.
- *Consider who you are, and who you're briefing.* You are experienced cyber policy professionals briefing the National Security Council. As such, you should be ready to answer questions on agency responsibility, provide justifications for your recommendations, and have potential alternatives ready.
- *Be creative.* Cyber policy is an evolving discourse, and there is no single correct course of action to the scenario information provided. There are many ideas to experiment with in responding to the crisis.

Cyber 9/12 Strategy Challenge | Intelligence Report

---

*Note: All materials included are fictional, unless otherwise marked, and were created for the purpose of this competition. Any resemblance to real persons, organizations, or events is coincidental. All scenario content is the intellectual property of the Atlantic Council unless otherwise specified in writing. This content is licensed for use by our Cyber 9/12 competition partners and students competing in our Cyber 9/12 competitions without fee or compensation, and to all other parties with the written consent of the Atlantic Council. This scenario is developed for academic purposes and is not meant to represent the views of the competition organizers, authors, or any affiliated organizations.*

- *Don't fight the scenario.* Unless stated otherwise, assume all inter-state relations, policies, and treaties have remained the same as they were in March 2021. Explore the implications of that information, not the plausibility. **The only exception to this is that in this scenario, students should work with the assumption that the SolarWinds hack never occurred.**

Given the unclear nature of the threat, the NSC requests that your team prepare a concise assessment of the ongoing situation and reporting. Your assessment should include:

- How or where the relevant systems could be vulnerable to exploit, and what steps can be made to mitigate these vulnerabilities;
- An assessment of potential risks and impacts to consider if the vulnerabilities are successfully exploited; and
- Responses the NSC can or should consider addressing these vulnerabilities, taking into account the severity and likelihood of the threat.

To provide this assessment and policy recommendations, you will apply your understanding of the technologies involved, cybersecurity, law, foreign policy, international relations, and security theory to synthesize useful policy measures from limited information. Your recommendation must analyze the possible strengths, weaknesses, opportunities, and threats of your proposed response.

In formulating your response, you will be expected to have considered, at a minimum:

- All stakeholders when determining an action or recommendation, including the role of the government and private sector;
- The long and short-term impacts of your recommendation;
- Which agency will be responsible for the action you have recommended;
- Appropriate recommendations for local vs. federal government;
- Whether you can, or should, attribute the threat; and
- The covert or overt nature of your response.

Additionally, this message is accompanied by several documents that may assist your team in preparing the assessment and policy brief for the NSC:

- **Tab 1** – CyberScoop Article
- **Tab 2** – SEC to the FBI
- **Tab 3** – Email from Port of Beirut
- **Tab 4** – CIA Memo

# CYBERSCOOP

## TECHNOLOGY

### DormantHound malware adds insult to injury taking ships offline

Written by William Klein  
MAY 18, 2021 | CYBERSCOOP

More than sixty percent of the world’s merchant fleet have been taken offline in a devastating cyberattack, continuing the relentless campaign that has already debilitated global shipping ports for weeks.

The new malware, dubbed DormantHound, by the Rabinara Group is believed to have been circulated by the frequent exchange of USB sticks containing pirated movies and television shows by mariners who find themselves increasingly isolated aboard their vessels without Internet access due to COVID-19 restrictions.

According to sources in the maritime transportation sector, nearly 30,000 vessels have been reported to have been affected with a significant proportion of them being located at sea and calling for rescue. With global trade and shipping outputs significantly lowered, shipping logistic and insurance company stocks have plummeted in response to the crisis, adding potential economic downturn to the ongoing trade crisis.

*This is a developing story and will be updated.*





## Tab 2 – SEC Memo to the FBI



TO: CHRISTOPHER GALLAGHER, DIRECTOR  
FEDERAL BUREAU OF INVESTIGATION,  
WASHINGTON DC;

CC: ESTE KARO, ASSISTANT DIRECTOR,  
CYBER DIVISION CRIMINAL, CYBER, RESPONSE, AND SERVICES BRANCH  
FEDERAL BUREAU OF INVESTIGATION,  
WASHINGTON DC

DATE: May 19, 2021

RE: Short Sale of Industrial Stocks tried to Recent Ransomware Attacks

Following the series of ransomware attacks targeting the maritime shipping industry, the SEC launched an investigation in the trading activity regarding the affected companies. The investigation uncovered an unusual pattern of trading activity prior to the disclosure of malware discovered at, or ransomware attack targeting, each of these companies. A series of customers without significant history of leveraged behavior began to book naked short positions against each of these firms.

Investigators discovered that a large number of the trading accounts were created approximately two weeks before the date of the first ransomware attack, all using fictitious materials to backstop their application for the ability to execute short trades. Over 200 separate accounts immediately took short positions in a subset of the affected companies in amounts between 5,000-200,000 USD. Over the course of the week as these firms began to disclose ransomware attacks and resulting impacts on port operations, the industry as a whole began to experience marked downward pressure from existing and long-standing investors. As this downward pressure accelerated and certain firms began reporting contract breaches with customers, these new accounts began to close out their short positions – filling their short sales with now markedly less expensive issues in each of these companies and realizing significant gains.

Analysis of trading activity in the week before each subsequent ransomware attack showed this same pattern of activity, with a widening set of now more than 350 accounts and varying patterns in entering and exiting their short positions.

As the accounts in question were identified, our investigators began to collect all associated account and transaction records and we of course reached out to FBI and USSS to support. Working with Secret Service, the investigative team identified a significant portion of the accounts created by a set of 13 IP addresses, all traced back to a bulletproof host known to be popular with Eastern European cybercriminal groups. Realized gains from all of the accounts have hopped from their original bank of deposit to less reputable financial institutions and several through bitcoin tumblers and exchanges, in at least 5 instances, to wallets known to have been previously used by 1881 Colectiv.

We are flagging this activity for further investigation and are sharing over our existing investigative records through the FBI liaison already working with this team.

### Tab 3 – Email from Port of Beirut

**To:** [reroutes@industrialfreight.org](mailto:reroutes@industrialfreight.org), [globalmanagement@industrialfreight.org](mailto:globalmanagement@industrialfreight.org),  
[missingcargo@industrialfreight.org](mailto:missingcargo@industrialfreight.org), [help@industrialfreight.org](mailto:help@industrialfreight.org)

**From:** [trackmyshipment@beirutport.gov](mailto:trackmyshipment@beirutport.gov)

**Date:** 20 May 2021

**Subject:** URGENT: MISSING SHIPMENT

Good Morning,

It has come to our attention that due to recent ransomware attacks, critical military equipment was mistakenly shipped to **Port of Beirut in Beirut, Lebanon**. Port officials discovered the error early this morning at 4:32am local time.

The cargo is marked to contain sensitive materials and includes a warning “FOR US MILITARY USE.” The equipment originated from the Port of Baltimore, Ref# 43C8H2.

Please advise where to reroute and any further guidance.

Sincerely,

**Omar Abdallat**

Director Cargo and Container Tracking  
Port of Beirut

**TOP SECRET/SCI//NOFORN**



**TO:** HEADQUARTERS  
**FROM:** ██████████  
**DATE:** 20 MAY 2021  
**SUBJECT:** HEZBOLLAH PURSUING SAM SYSTEM

(TS//NF) On 6 May 2021, ██████████ met with ██████████ who revealed Hezbollah operatives are looking to take advantage of the chaos caused by the ransomware attacks on ports around the world to obtain erroneously shipped and misplaced weapons. ██████████ learned operatives are planning multiple operations in the coming weeks to gain territory, recruits, and collect critical components for a surface-to-air missile (SAM) system mistakenly sent to the Port of Beirut.

(TS//NF) Based on information from ██████████ colleagues and commanders, Hezbollah is aware of the critical SAM system equipment mistakenly delivered to the Port of Beirut. According to ██████████ Hezbollah has been developing bombing and missile capabilities since 2019. ██████████ explained Hezbollah leadership considers this equipment critical to defensive operations as they continue to invest in missile development in Beirut and the Bekaa Valley.

(TS//NF) Hezbollah plans to collect the SAM system equipment at the Port of Beirut. Operatives are currently being mobilized.

(TS//NF) ██████████ has high confidence in the veracity of ██████████'s information. ██████████ assesses this mission is high priority to Hezbollah leadership. This opportunistic operation is not unique. We have intelligence that Iranian government operatives have also collected misplaced shipments. These have primarily been pharmaceuticals drugs and COVID-19 vaccines discovered at Chabahar Port, originally intended for the US Thumrait Air Base in Oman.

**TOP SECRET/SCI//NOFORN**