Cyber 9/12 DC – A Disaster to Entertain Poseidon and Ruin Christmas

Scenario Overview

The 2020 DC Cyber 9/12 Scenario, which will take place from October through December of 2022, focuses on maritime cybersecurity and how non-state actors can sow chaos and congest critical shipping lanes with severe global economic ramifications. The scenario proceeds through a series of escalating security events with challenging political constraints on response (Chinese partners on incident response, uncoordinated vulnerability mitigation, and interagency confusion over lines of responsibility). It concludes with the discovery of a state actor exploiting the chaos to ship a do-it-yourself dirty bomb kit through the impacted region to a distant buyer.

The principle antagonist is a non-state group based in the United States called The People's Militia (TPM), a call back to the same group active in our New York scenario this past November. The Militia is a hyper-antagonistic anti-capitalist group with strong anti-institutional tendencies and a doctrine of cyber capability acquisition and use informed by edge-case ideologies of domestic militancy in the US. The main cyber capability employed by the Militia is a piece of malware targeting manifest record keeping systems, starting on two ships managed by private firm Little Ocean Big Heart LLC. This malware compromises the integrity of inventory databases, wiping them in whole or in part and using leave-behind ransomware to frustrate efforts to restore from backup. The malware spreads from ships to ports with the manifest record keeping systems as the main infection vector. Over time, this malware begins to spread to other systems at the affected ports.

The scenario takes places in three acts – the first delivered to students 10 days before they arrive, the second provided to semi-finalist teams at the end of the first day, and the third is given to championship teams 15 minutes before the final round. The early injects focus on establishing the current economic importance of the Strait of Malacca chokepoint and re-introducing The People's Militia as an actor. We use a series of news articles to demonstrate that the lead up to the holiday season is a particularly busy time for shipping in the region as global shipping volume skyrockets. Using an interview recording with The People's Militia's leader and view into an encrypted web forum discussion, we establish how the People's Militia has expanded both the focus and scope of their operations, detail their basic ideology, and explain why they have become acutely interested in developing and utilizing offensive cyber capabilities.

Move 1 concludes with several important developments. First, a currently unknown actor – the DPRK – blackmails several commercial shipping firms with the supposed "capability to wildly disrupt and destroy your navigation capabilities." Concurrently, a well-known hacktivist leaks a suite of offensive maritime cyber tools and research focusing on maritime cybersecurity. Finally, the initial effects of the Militia's malware begin to manifest, raising questions within the USG about how to respond and who should lead this response.

As the effects continue to spread throughout the global port network as these ships travel across the region to the South China Sea (the malware spreads organically), international trade slows, causing global economic harm. Attempts to resolve the effects of the malware triggers leave-behind ransomware in several systems, severely complicating and obstructing incident response. These effects are compounded by a simple but disruptive attack on the integrity of data from the Automatic Identification System, executed by the DPRK using the leaked tools from the maritime cybersecurity firm, which further complicates navigation and forces manual watch standing in major shipping lanes particularly the Strait of Malacca, which have already grown immensely congested.

Finally, DPRK loads a dirty bomb kit on to a ship, taking advantage of the AIS failures to move the device components to a Hindu ultra-nationalist group looking to acquire and use a capability independent of the mainline defense establishment. The ship includes high value personnel from the DPRK weapons program whose disappearance triggers an escalating series of alerts and reporting from the IC. At this time, a private People's Militia communication is also discovered, which identifies the group as the main actor behind the primary global malware.

Students must therefore analyze how they can best A) respond to the ongoing cyber and economic crisis, B) interact with all actors involved to ensure the best solution for all actors (but specifically US and China), and C) block the proliferation event.

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 Fall 2022. 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**.

It is due **no later than 11:59 PM** on **Sunday, March 15, 2020**. Please submit your written policy brief to https://form.jotform.com/200554247431044

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 March 2020. Explore the implications of that information, not the plausibility.

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** – Bloomberg Business News
- **Tab 2** – Vulnerability Disclosure Email Chain
- **Tab 3** – The Intercept – Interview Transcript
- **Tab 4** – Cyberscoop News Article
- **Tab 5** – NSA Intelligence Report on DarkNode Forum Thread
- **Tab 6** – Reuters News Article
- **Tab 7 –** Little Ocean Big Heart LLC Internal Security Report
- **Tab 8** – CSIS Report
- **Tab 9** – Formal Notice From DHS CISA
- **Tab 10** – New York Times Report
- **Tab 11** – Slack Channel
- **Tab 12** – Twitter Chain
- **Tab 13** – Interagency Email Chain

Tab 1 – Bloomberg Business News Article

Bloomberg

Markets

A Typhoon of Sales Puts Global Shipping Routes in Stormy Weather

Jim Hildebrand

Major shipping routes across the globe are coming under unprecedented strain to meet demands for shipping, as the freight industry attempts to navigate the busiest holiday season on record.

10/21/2022

Photo from International Register of Shipping

The Busiest Peak Season on Record

A sharp rise in demand for luxury goods and clothes, electronics, automobiles, and all manner of durable goods is expected toward the end of the year, as business and consumers across the globe ramp up their purchasing in preparation for the holiday season. This busy period is known as "peak season," and usually runs from the end of August to the start of November; a second, smaller peak season occurs in January/February to coincide with the Chinese New Year.

During peak season an increase in demand for shipping space causes a rise in freight prices - rates can spike by 10-15% at the start of the season, and can continue to gradually increase as the season progresses before plateauing towards the middle of November. In turn, shipping companies

increase the number of active vessels to match supply to demand, congesting already crowded shipping lanes.

But if this increase is expected, why is the shipping industry struggling to cope with the number of ships on the water? After all, Christmas comes every year. According to Brian Serville, Head of Public Affairs at the Freight Transport Association (FTA), the United Kingdom's largest freight and shipping trade association, this year is different because of the continued concentration of manufacturing in Asia and the rising demand for Western consumer goods in China. Serville points to a dramatic increase in consumer demand for internationally shipped goods. "What we're seeing now is the explosion of a trend that has been steadily increasing over the past few decades. The buying public - whether that's global businesses or local people - has increasingly looked to international vendors to fulfil their procurement needs. When we look at the last 20 years there has been a gradual increase in demand, which means the shipping industry and infrastructure have had time to react and cope. But the spike in demand this year was completely unexpected - the industry simply cannot accommodate."

Unexpected is an understatement. Serville is right that in the last two decades global shipping numbers have continually - but gradually - increased. Year-on-year increases have rarely gone above 10%, and those that did followed periods of stagnant growth (1996-99) or unexpected downturns (2009-10). In the last 10 years it has never gone above 6%. However, early estimates are showing that the increase from 2020-21 is closer to an unprecedented 20-25% - and rising.

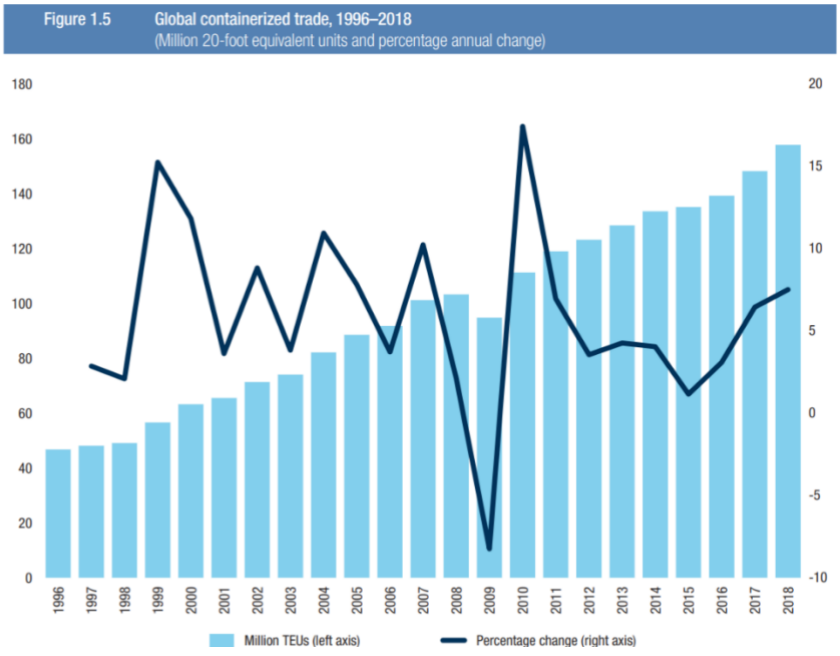


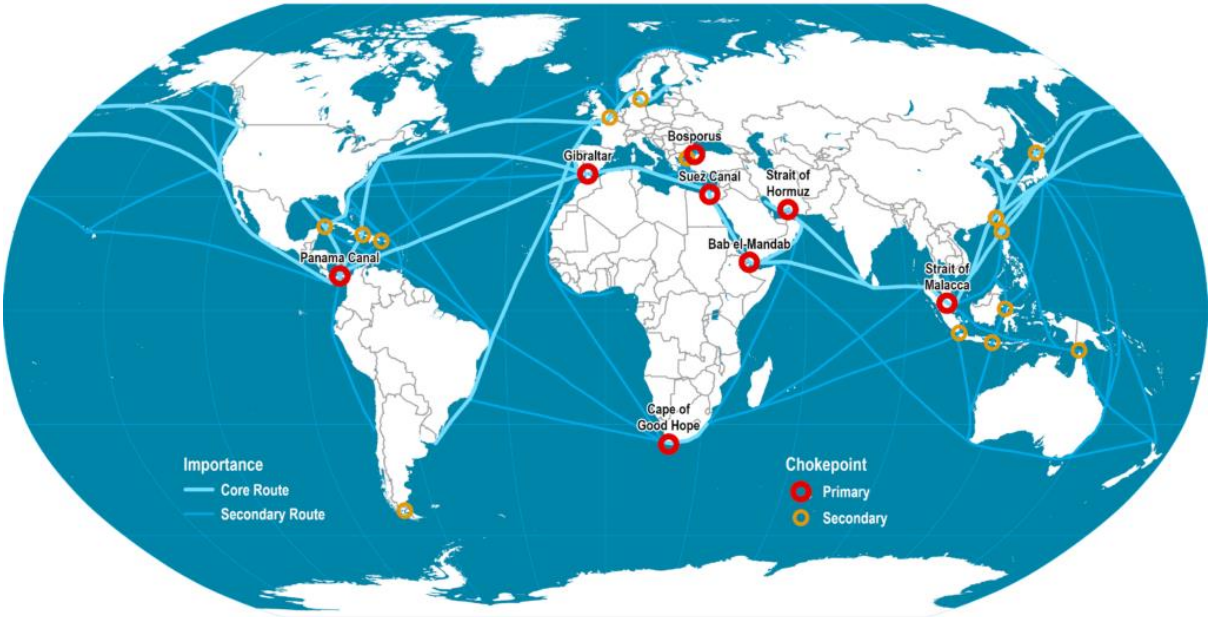
Chart by UNCTAD Review

The impact of this increase is not limited to rising shipping costs or long waits at the Suez Canal. A knock-on effect is that importers risk not being able to secure the goods they need, thereby threatening the global supply chain. From the perspective of the ports, and for those upstream in the supply chain, a lack of space on transport means warehouses that cannot shift their stock and trucks and transport unable to unload miles-long queues. Looking downstream, importers do not receive stock, businesses default on procurement orders, and consumers go without their products. All just in time for Christmas.

Serville is remarkably frank in this regard. "There is a real concern that the supply chain will fail this year. That's bad for the industry, bad for business, and bad for consumers."

Global Trade, Localized Chokepoints

Shipping is a global concern. But certain areas will be especially hit by increased demand and the subsequent increase in ships on the water. Global trade is linked by a few well-trodden routes; most notable is the circum-equatorial corridor, with connections made through the Panama Canal, the Suez Canal, and the Strait of Malacca. In times of conflict, trouble, or increased stress, these narrow channels (the Malacca Strait, for example, is only 2.7km wide) act as "chokepoints" along global sea routes.



Map by The Geography of Transport Systems

In a world dominated by East and Southeast Asian manufacturing, it is the Strait of Malacca that has taken on an increased prominence in the world of shipping chokepoints. The 900km long strait links Asia with the Middle East and Europe, and around 40% of world trade passes through the strait each year, including vast amounts of crude oil on its way to China and Japan from the Middle East.

The holiday season has come again and with it, increased demand for consumer goods and the vessels to carry them. Unlike the trade routes of yore, today's hyper-efficient shipping lanes have little spare capacity with minimally crewed ships and fuel sipping speeds. As this spiking demand has shown, the market will react given enough time, but there may only be so much room at sea.

Tab 2 – Vulnerability Disclosure Email Chain

From: Laone Andremu[mailto: “l.andremu@bolh.org”]
Sent: 5:22PM - 10/23/2022
To: Gregory Turner [mailto: “g_turner@bolh.org”]
Subject: Vuln. ID #A1763 in Code Review

Hi Greg,

I wanted to touch base with you about a vulnerability we’re still looking into in our SEAFARER cargo management software. One of my researchers discovered serious potential for data overwrite with our new rapid update feature that’s going to require some significant attention. I know our patch deployment system is still relatively immature, but we need to discuss how much demand our developing fix will place on customers – its looking like there will need to be a full reboot cycle and some spin up time where SEAFARER won’t be available. Let me know if you have some time later this week, if it’s easier we can chat in person.

Best,

Dr. Andremu
Senior Cybersecurity Analyst
Big Ocean Little Heart LLC

From: Gregory Turner [mailto: “g_turner@bolh.org”]
Sent: 10:01PM - 10/23/2022
To: Laone Andremu[mailto: “l.andremu@bolh.org”]
Subject: [RE] Vuln ID #A1763 in Annual Code Review

Hello Ms. Andremu,

Thanks for your note. We’ve always struggled a bit with rolling out patches. There are a lot of our users, especially in larger ports, that have used the in-house consulting team to tailor SEAFARER to their database infrastructure and operating environment. It’s a messy environment with a lot of stakeholders. I’m happy to get into the weeds later, but could you tell me a bit more about exactly what we’re dealing with? I’m still unclear.

Gregory Turner
Chief Systems Management Officer
Big Ocean Little Heart LLC

From: From: Laone Andremu [mailto: “l.andremu@bclh.org”]
Sent: 11:12PM - 10/23/2022
To: Gregory Turner [mailto: “g_turner@bolh.org”]
Subject:[RE] [RE] Vuln. ID #A1763 in Annual Code Review

Of course. I've attached our internal memo on #A1763. The sparknotes is that there may be a vector for an automated script to modify data. SEAFARER allows users to define temporary fields as part of the system for tailoring inventory management to operational specifics, sort of like adding a new column to an excel sheet. The problem is that there's not a robust data-integrity system in place for these ad hoc fields—they're a pretty early feature, and whoever designed them never really considered security because we assumed that only in-port and at sea operators, who already have admin access, would ever use them. The functions are basically tacked on the backend and written to save time for ports with big cargo flows and ships where there's not a lot of spare crew time to do data management on the cargo. It's like there's an open box at the end of every database object and when its full the extra data spills into the next column's data. The specs from the researcher's report are below. I can CC her too.

Issue ID: #A1763 **Location: cont_field_ext.c** **Severity: Moderate**
Summary: In cont_field_ext.c, struct cont_field_ext has no data management infrastructure during definition and construction. Functions cont_field_ext_WRITE, cont_field_ext_FILL, cont_field_ext_AUTO, cont_field_ext_SWAP, cont_field_ext_WRITE_MULTI, cont_field_ext _PUNCH, and cont_field_ext_COMP lack input consistency checks between ln and input_get_ln() and exception handling frameworks for other failed consistency checks. Cross-compatible backend database functions added through cont_field_ext.h also lack the same components, and, though out of report scope, it's worth noting that oChunk_HEAPMGR.c has allocation inefficiencies that will impede a patch.
Impact: At minimum, current configuration with admin access allows overflow attacks on database fields. Likely allows inputs that will delete or corrupt database records. Possibility for malicious code injection cannot be ruled out either due to unsiloed availability of manual admin test functions. We haven't determined the full scope of how #A1763 can be leveraged, but at a low level it is relatively easy to take advantage of with some system access and low sophistication.
Recommendations: Implement exception handling framework, robust data management objects in cont_field_ext.c. Reevaluate makefile dependencies and .h inclusions, particularly in relation to cont_field_ext.h and cache and backup siloing.

Let me know if we can send anything more useful your way.

Dr. Andremu
Senior Cybersecurity Analyst
Big Ocean Little Heart LLC

P.S. I hate to be that person, but I really do prefer Dr. to Ms.

From: Gregory Turner [mailto: "g_turner@bolh.org"]
Sent: 11:41PM - 10/23/2022
To: Laone Andremu[mailto: "l.andremu@bolh.org"]
Subject: [RE] [RE] [RE] Vuln. ID #A1763 in Annual Code Review

Dr. Swanson,

No need for the CC, and my apologies for the title issue. I think we'll have to all get on a conference call together. This looks like it could be a time sensitive issue, but maybe not if it's backend enough. Given that we supply software for inventory management programs in ports in over 30 countries, it's incredibly challenging to make sure the different versions and configurations of our product are compatible already, and a comprehensive update like this is going to be brutal. You are right to worry about service interruptions too. If we implement a fix, we're going to have to apply it to existing inventories, and that's a lot of data fields to redefine and repopulate. It might not be warranted but your instincts concerning patching otherwise are spot on.

Please run this through the Security Management team in legal. I know we've committed to share in process-patches with COSCO given our partnership in the region and at minimum their engineers need to be brought in on a coordinated vulnerability response.

If you can think of anyone else we need to bring into the loop – who can actually help with the response - I'm all ears.

Best,

Greg
Chief Systems Management Officer
Big Ocean Little Heart LLC

Tab 3 - **The Intercept – interview transcript**

NOTE: Please listen to the audio recording of this interview, provided by Will Loomis in the scenario dissemination email. For your convenience, a transcript of the recording has been provided below.

Prologue

Hi this is Reed McShay with The Intercept reporting:

Remember The People's Militia, or TPM for short? You may recall the shadowy cyber hacktivist group gained notoriety in late 2021 after conducting several high-profile breaches of government databases and, most notably, attempting to interfere in the New York City mayoral election. While city officials claimed TPM's activities had no material impact on the election, their actions tanked public faith in government and set off a series of large-scale demonstrations across the country.

TPM also made headlines for leveraging access to local and federal government databases to build and publish a since-removed application called 'Reverie', an analytics platform that aggregated personally identifiable information — unsecured facial recognition data, CCTV feeds, biometric security data, and other sensitive government datasets — to track people in real-time.

Downloaded over 100 million times before being removed from the Apple IOS and Google Play Stores, the app as of this recording has been linked by the FBI to over 100 homicides across the United States.

The group largely faded from mainstream media headlines following the death of its leader, Adam Denton, in a shootout with the Hong Kong Police Force on December 25, 2021.

Now, it appears the group is back with a renewed mission and a call to arms.

On October 26, I conducted a phone interview with one of the founding members of TPM, who agreed to the interview on the condition of anonymity. We discussed last year's events, how TPM has changed, and the group's outlook going forward.

Interview

The Intercept: First of all, thank you so much for taking the time to speak with us today. Ever since Adam Denton's interview with the New York Times last November, we haven't heard much from The People's Militia. Why have you decided to come forward now, and why The Intercept of all places?

TPM: Just because you haven't heard from us doesn't mean we've disappeared; we're just getting started. Kleptocrats across the globe are lying and stealing from their people, hoarding immense sums of wealth—including personal data—and failing to secure it. Governments are overreaching in cyberspace and the people must be protected. The mainstream media pays no attention… We came to The Intercept because of its track record of holding elites accountable.

The Intercept: On December 25, 2021, the Hong Kong Police Force moved in to arrest TPM leader Adam Denton, who was hiding out in Hong Kong, when he drew his firearm and was killed in a shootout. How has your mission changed since, if at all?

TPM: First of all, I never called him Adam. I only knew him by his online moniker, Ethereal Rose. He was martyred in Hong Kong, and we've sharpened our focus since his departure, expanding on his anti-capitalist vision.

The Intercept: How has your organization coped with his absence, and who is leading the organization now?

TPM: I take exception with your label "organization". We're more decentralized than ever, and that's only made us stronger. We have like-minded comrades around the world working for our cause, planning, writing, and recruiting. Because it's not just a problem in the United States—we need to look globally. We've taken up arms and are ready to fight.

The Intercept: In cyberspace?

TPM: Yes.

The Intercept: …and you believe this is all legal?

TPM: That's right. It's our inalienable right to defend ourselves in cyberspace. Criminals, corporations, foreign governments—our own government—all pose threats… It's a dangerous place. The Second Amendment protects the right to bear arms, and as far as we're concerned… there are no boundaries on that right. People must have the right to defend themselves... and attack when necessary.

The Intercept: So, how does that look? What in your mind justifies going beyond self-defense?

TPM: What I will say is that corporate greed and waste are out of control. They've always been out of control, but we're now in an era where corporations are collecting and monetizing every bit of our data. And what choices do consumers have?! Take...take Christmas for example… ugh makes me sick. It represents *everything* that's wrong with America. It's peak waste. And what choice do people have?

Tab 4- CyberScoop News Article

GOVERNMENT

Ransomware Attacks Are Testing Resolve of Cities Across America

Written By: Katrina Taylor

OCT 28, 2022 I CYBERSCOOP

The attack starts with an email. One click on a link and hackers gain access using a broad, aggressive, and increasingly easy method for spreading ransomware.

With a new high-profile incident every few weeks and industry failure to install patches for vulnerabilities, strains of ransomware are becoming a recurring global tactic.

The most recent ransomware attacks capable of shutting down government services goes by the name of HarshRealiti. In June 2019, casinos in Atlantic City and New Jersey's Department of Commerce were forced to shut down operations for weeks. The Department of Homeland Security's CISA responded with plans to release a report to help local businesses and federal institutions protect themselves against similar ransomware attacks. However, just last month, an unknown actor targeted New York city's DMV systems infrastructure, shutting down offices across the state for weeks.

Although we have seen an increased number of ransomware attacks recently, the threat is not a new one for government networks. More than 45 municipalities, including Federal offices, have been victims of cyberattacks this year with cities such as Baltimore, Greenville, and Atlanta, and smaller towns like Lake City, Florida all impacted.

In March 2018, Atlanta suffered a major cyberattack stemming from use of the SamSam ransomware. Months after, Greenville, North Carolina was the second major city in the country with a population of over 500,000 people to be targeted by ransomware. It's attacker, Hidden Tear, knocked the city offline. In Baltimore, where a virus

called RobbinHood encrypted several local systems in hopes of a $76,000 payday, a long and slow recovery was peppered with missteps and delays.

“Skill used to be the most important aspect in possessing cyber capabilities. Now, it’s not only highly skilled hackers who have the ability to completely wipe out government services. Individuals and groups can purchase and use these very same tools. With the barriers to entry lowered, ransomware is becoming a weapon of crippling institutional destruction,” says Mark S. Seever, Chief Information Officer at TheyWork.

The majority of ransomware cases have targeted small, cash-strapped local governments as they are unlikely to invest in updated cyber defenses or data backups. With limited financial bandwidth, Lake City is one of the few victims making the decision to pay the demanded ransom--$460,000--in Bitcoin, a cryptocurrency. With Federal institutions susceptible to disruption due to decentralized IT practices and inadequate infrastructure, federal offices across the United States are vulnerable to ransomware attacks. The future of ransomware is bright, government IT programs less so.

Tab 5 – Intelligence Report on DarkNode Forum Thread

Intelligence Packet: NSA Market Monitor ProgramID #5482251

Threat Level	**Moderate (2/5)**
Admiralty Code	**C3**
Event Date	**30/31 October 2022**
Source	**DarkNode Cyber Crime Forum**
Threat Actor (TA)	**Unknown, suspected People's Militia**
TA's Language	**English**
Targeted Geography	**United States**
Analysts	**Matt Richardson**

Key Points

1. **Abstract: During routine network monitoring, analysts came across an English language thread of interest on a monitored forum, DarkNode. The thread linked to past People's Militia operations but contained no high confidence information on legitimate group identities. Might provide insight into group organizational structure, planning methods, and network preferences.**

2. **Audience: U.S. LE and IC community entities; threat intelligence partners**

3. **Source and Validation: DarkNode has a mixed record of providing actionable or high quality information. It has been used as a marketplace for malware franchising and carder sales, including a brief run on Brian Kreb's top 10 list for sites with mag stripe information, 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 designed as hoaxes; most users are aware that it is monitored by intelligence agencies.**

4. **Mitigation Summary: We suggest increased monitoring of known People's Militia networks and malware marketplaces.**

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

Source Report: Text of DarkNode forum discussion
1. TA's post on 130/31 October 2022:

30/10/2022 2342EST

loomnlurk > appreciate you putting this together, can't be easy with all the attention that ny brought

> **CCHandler** > normally we wouldn't risk it right now, but you guys have a decent reputation
>
> **CCHandler** > don't mess it up
>
> > **Concourse** > Don't be dramatic. You're the IT guy, not the godfather.

30/10/2022 2350EST

Concourse > What do you have in mind loomnlurk?

loomnlurk > well we really liked what was said in the nytimes article, but there's a lot more to this, right

loomnlurk > there was all that talk about the mass consent involved in all the data gathered on citizens, and that's hard to deal with. some people are too lazy to know what they're giving up, some don't care, and some are actually ok with it.

> **Concourse** > Interesting.
>
> **Concourse** > Where does that idea take you?
>
> > **loomnlurk** > our local group came together after the Equifax breach, and we've always been more focused on direct action.

loomnlurk > you'll never be able to get people on board with as broad a message as we had in the nytimes article. Data is abstract and corporate governance is a snoozer. Sure, there's foreign governments and our governments and companies and the internet is scary, but we think that the real problem needs to be distilled and it will make the message more popular and our operations more focused.

31/10/2022 0001EST

CCHandler > come on, let's get to the point.

loomnlurk > ok ok here it is

31/10/2022 0023EST

loomnlurk > they don't just profit off our data, they hold us hostage with it. we're dependent on things we never consented to from the moment we're born, and they can't even be bothered to protect those dependencies. infantilization without representation.

Concourse > I like that a lot.

CCHandler > Damn right – cyberpunk meets Patrick Henry

31/10/2022 0040EST

loomnlurk > you ever want to buy a house? too bad, someone has been keeping your credit since you were eighteen. you never knew it, but you messed up and you'll never be able to take a loan out. or worse, it was a great score but they let someone steal the number and your life is wrecked and you won't know it till it's too late. no car, no house, and good luck sorting out the debt they racked up on your credit card.

Concourse > Sure but our action was to elevate the popular consciousness about liberty and the onslaught of corporate greed against our privacy – we made a moment.

loomnlurk > It's not just information. we're held captive by dozens of systems. want health insurance? Go work for one of those companies, do their dirty work, or die sick and still in debt, and if you ever leave, no more health insurance. want to eat fruit in december? pay up so someone can pump tons of diesel into the air to send it to you. Want to go to school, learn how to get a better shot at getting out of this? cough up a few hundred grand, or it's more debt and good luck finding entry level work to pay it off. The Second Amendment enshrines our right to take up arms to defend ourselves – why should the body politic limit itself to weapons of an immediate and physical nature?

Concourse > This is great and all but what's the endgame? We're not some ultra-nationalist group looking to play militiaman on the weekends. What does the amendment do for anything?

loomnlurk > look at it in the context of the constitution. it's not just about self-defense. it's about demanding representation, destroying the things that hold us hostage, and punishing the companies and governments. Direct action to assert our liberty against the tools of oppression whether pointed and momentary or systematic and unceasing. We have common cause with folks like the 99%ers – our oppression is as much in manufactured materialism and consent to a system of accumulated greed as with being told where to go or how to live.

loomnlurk > used to be that a handful of people could fight to change the system they were a part of if and when it became unduly oppressive

loomnlurk > its one thing to open people's minds its another thing to gather them into a fist to punch back

loomnlurk > we don't believe in half measures and the target shouldn't just be public consciousness or local governments it has to be the

system of moneyed influence that facilitates our oppression, shapes our values, and undermines our culture.

loomnlurk > in the olden days it was enough to carry a musket and mount a horse but our fight is different and our opponents more cunning – we need a different type of weapon not get beat in some old school shoot out

CCHandler > I'm still not getting how you take this from manifesto to action?

loomnlurk > we take action using the same capabilities used to wage war on us – retake cyberspace for the people that live and work and love in it – the cyber tools and tactics that work against governments when deployed by governments will work against them when deployed by the people.

loomnlurk > we've got some targets in mind, and we've been working at getting the tools to really do some damage to them through our own Digital Lafayette

31/10/2022 0058EST

Concourse > We should move this to somewhere a little more secure. Let's talk again soon if that timeframe works. Your message rings true and I hope you can deliver something concrete to act on it but it takes real tangible outcomes not some online screed to move things forward.

Concourse > Companies are a de facto government enabled by actual ones, as incompetent as they are tyrannical, and we have a right to fight for control in that system

Concourse > And functionally, that looks like destroying data and hurting the companies that create the kind of non-consensual framework you're talking about. I really like the idea of targeting those background corporations that escape the headlines a lot, and I have a feeling they'll be a little more vulnerable too.

loomnlurk > time frame works, and yea that's about it. i really like how you've put it.

Concourse > more to come.

Tab 6 – Reuters World News Article

REUTERS

World News November 2, 2022 8:16 AM

China Raises Security Warning Level in Malacca Strait, Surrounding Region, No Explanation Offered

Thomas Brandy, Michael Wentz

SINGAPORE/HONG KONG (Reuters) — Last night, Beijing raised the level of its security alert for Chinese flagged ships passing through the Strait of Malacca, a narrow maritime passage connecting the South China Sea to the Indian Ocean. The warning level grew from 2, moderate, to 3, severe, but officials from Beijing did not explain their reason for the change and refused to comment.

Transport and security ministries from neighboring countries, including Indonesia and Malaysia, also pressed China for an explanation but received nothing official. “We would like to know more about the situation, as we have critical ports and many ships in the affected area,” Sukarno Agung, a spokesperson from the Indonesian Maritime Security Agency, commented. “It is important that all partners work together for a secure maritime environment and we call on all affected stakeholders to be collaborative and proactive.” China has raised its security warning without explanation in the past, as recently as July 2019.

Some analysts point to Beijing’s increased reliance on the trade route through the Strait of Malacca to explain the advisory change. 80% of Chinese oil imports pass through the Strait. Overall, 70% of Chinese oil and natural gas is imported, and that dependency is expected to increase through the next two decades at least.

Others also noted the role of resurgent piracy in the area, particularly targeting oil and fuel tankers. New attack tactics, complacent crews, and increased shipping traffic have contributed to a steady increase in robberies since 2016. One ship was even robbed twice on the same day earlier this year.

“What we’d like to see is for the US to step up its role in coordinating protection in the region,” Professor Mia Dumchek of the Naval War College told Reuters. “It’s easy to only think of China when we look at Malacca, but in reality, critical US partners like Singapore, Japan, South Korea, and the Philippines also depend on the same shipping lanes.”

Tab 7 - Little Ocean Big Heart LLC - Incident Report Memo

To: Julianna White, Chief Risk Officer
From: Tian Baozhai, Principal Risk Manager
Laone Andremu, Senior Cybersecurity Analyst
Date: 11/4/2022
Subj: Cybersecurity incident & manifest recovery

Summary

3 vessels currently underway have corrupted or incomplete manifests stemming from an apparent cyber-attack on the SEAFARER cargo management software. The attack appears external in origin and has impacted 3 containerized cargo vessels sometime during transit to, loading at, or after departing from the Port of Long Beach.

Background

Little Ocean Big Heart LLC has a nearly thirty-year legacy of providing highly trained and experienced seagoing crew for deep draft vessels handling containerized cargo, break bulk, and crude oil. As the firm has grown, we have expanded from crewing operations and sustainment to full lifecycle logistics and manifest management services. As of this year we maintain cargo identification and transshipment tracing systems while handling manifest and specialized cargo management software for more than 70% of the gross tonnage underway in a given year for containerized and break-bulk cargo. In our most competitive market, the Trans-Pacific, we are responsible for manifest tracking and cargo management of more than 90% of gross tonnage in a given year.

Incident Report

2 vessels from [redacted] left the Port of Long Beach two days ago and while in transit to the Port of Shanghai identified serious problems with their manifests. Vessel 1's manifest didn't correspond with containers taken on in Long Beach and appeared to have been reverted to a partial manifest from several months ago after loading in the Port of San Diego. Vessel 2's manifest had been partially corrupted – the system displayed jumbled strings in lieu of tabular data for some of the recently loaded containers

Remote incident response on the two vessels indicates there was a compromised storage device inserted into the ship's systems, possibly the Manifest Data Unit – a small USB storage device used to transfer manifest records from the vessel to port facilities to track offload and new cargo, which contained a two-stage malicious payload. The first stage appears to abuse a well-known .lnk vulnerability in the Windows operating system to drop malware from a storage device to the ship's management console. While most modern versions of Microsoft's operating systems have been long patched for this flaw, the majority of our customer's management systems on-ship are based on a scaled down version of Windows XP. SEAFARER is built to work with these systems and so appears to still contain a pathway to exploit this vulnerability despite it having been patched in our production systems, all running Windows 10.

The second stage abuses a feature in SEAFARER which allows scaled changes to single data types in manifest records. Where operators at sea or in port want to make small changes, for example adding a temporary ID code to all cargo for use in automated cargo terminals with RFID recognition, SEAFARER enables users to rapidly make changes at scale to a set of manifest records by defining an operation and having it run without additional intervention. This feature was incorrectly reported as a vulnerability by a researcher, and we declined to seek a CVE or pursue additional mitigation beyond requiring

administrative permissions for these automated changes. To do anything else would have required substantial development time and the additional permissions required to run was deemed a sufficient mitigation by management.

The malware's second stage uses this scaled change feature to overwrite data fields with randomly generated strings or revert to recent entries. The attack then wipes SEAFARER's change log and deletes cached and partial file versions so only the corrupted manifest remains. The attack appears to have a pre-determined stop time so that, in the case of the first vessel, the manifest was not completely overwritten while in the second it was. We have not identified a means to reverse these changes. There is another vessel (vessel 3) from customer [redacted] that has also reported data corruption issues, but we've been unable to execute an incident response and have no forensic data beyond a sketchy incident report from the crew.

In the case of the first 2 vessels from [redacted], it appears operators had left the administrator account logged in by default to avoid repeated logging in and out while conducting operations at sea. This is in direct contravention to our Security Guidance of Feb 2022 describing the proper procedure to isolate permissioned processes and features by using the administrator account. Because of the large volume of containers onloaded at Long Beach, neither crew appears to have noticed if there were manifest record errors while in Port. It's not yet clear if any dock-side systems have been impacted.

Next Steps

Vessels 1 and 2 are headed for the Port of Shanghai and then to Rotterdam and Osaka respectively. We are concerned that without additional information about this malware that there is risk of wider compromise. Vessel 3 is scheduled for the Port of Qingdao and then to shuttle between the Port of Guangzhou and Gioia Tauro in preparation for the holiday season. We would like to capture more forensic data on all three vessels when they reach their next port of call but do not yet recommend raising specific alerts or modifying our guidance to customers absent reporting any other errors in manifest records. There is a moderate probability that these are isolated instances.

Tab 8 – CSIS Report

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

SHARE

CRITICAL QUESTIONS

Just How Much Does the World Depend on the Strait of Malacca?

November 4th, 2022

CSIS ChinaPower Team: Bonnie S. Glaser, Matthew P. Funaiole, Kelly Flaherty, Brian Hart, and Harry Du

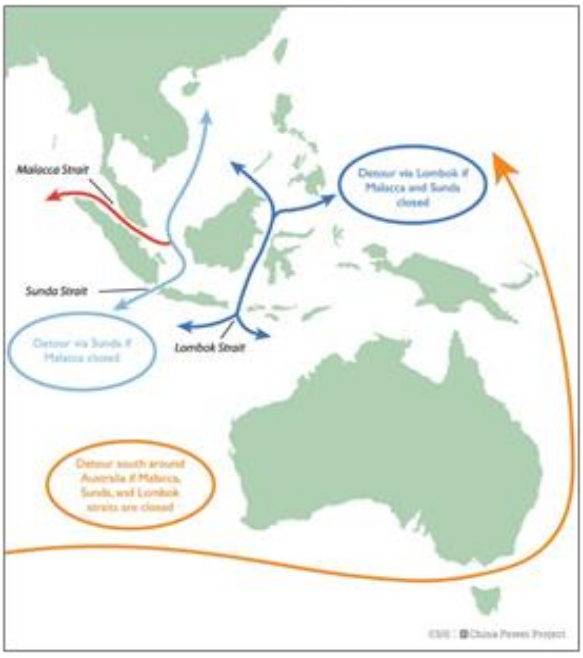
The Strait of Malacca has provided a critical shortcut through the Indonesian archipelago since ancient times, linking the Indian and Pacific Oceans. Without it, navigating lengthy and dangerous alternate routes would slow the pace of modern maritime trade or require manmade alternatives. Analyzing risk to regional economies and global industry requires understanding how natural chokepoints like the Strait of Malacca can interact with international trade and transit.

As much as 50% of global shipping passes through Asia by sea, and China's dominant trade economy redirects 33% of all world trade through the South China Sea. While the South China Sea often makes international headlines because of jurisdiction disputes— incidents of artificial island construction and militarized fishing boats, for example—the Strait of Malacca is a significant factor contributing to that sea's strategic importance. Its positioning allows boats to eliminate a lengthy detour around the Indonesian archipelago and cut straight from the Indian Ocean to the South China Sea and, eventually, the Pacific. It is estimated that a full quarter of all world trade passes through the 2.8 kilometers wide bottleneck at the Strait's narrowest point, Phillips Channel, and there is a maximum hull depth of 25 meters for ships traversing it.

A number of critical industries and large economies rely on this passageway for both importing and exporting products. Middle Eastern oil producers—Iran, Iraq, Saudi Arabia, Oman, Kuwait, and the UAE—export around 30% of the world's oil, and the vast majority of this, a fourth of all the world's oil, goes through the Strait of Malacca to reach eastern markets like China, Japan, South Korea, and even Australia. Almost every South East Asian country relies on the Strait for their exports. They include, among several other critical industries, chemical production, tin, hard drives, and other electronic components.

There are few attractive alternatives to the Strait of Malacca, so long as China's proposed Thai Canal through the Kra Isthmus remains a pipedream, which appears to be the case. To the south, the Strait of Sunda provides the nearest passage, though routes through it are more than 1,600 kilometers longer, and the strait, while wider, is more challenging to navigate due to a shallower maximum hull depth of 20 meters, sand banks, tidal currents, and even an active volcano. The other alternatives, while more forgiving for ship captains, create even longer journeys for cargo vessels—deep water passage through the Lombok Strait requires a voyage more than 4,000 kilometers longer than through the Malacca Strait, and the next best alternative is to journey around Australia, through treacherous waters and thousands of additional kilometers. Moreover, all of these alternate routes still pass through relatively narrow chokepoints created by islands and sandbars.
The Sunda narrows to 24 kilometers, and the deeper Lombok to 19 kilometers and again to 40 kilometers in the north. Tortuous routes around Australia still require navigating narrow passages throughout Indonesia and the Philippines, like the Ombai-Wetar Strait (35 kilometers), the Torres Straits (a series of passages between islands), and the Banda Arc (105 kilometers).

Akimoto, 2001, Alternate Routes, link



CSIS ChinaPower Alternate Routes, link

Perhaps the most concerning consequence of global trade's dependency on safe passage through the Strait of Malacca though is the potential for indirect effects of obstruction. The amount of trade that passes through the straits is massive, as noted before, but more critical is what that trade consists of: primarily, inputs. Massive quantities of oil, ore, component pieces, minerals, coal, palm oil and chemicals travel through the straits, often to countries like China, Japan, South Korea, and India, where they fuel further manufacturing processes. Any obstruction to trade in the region would have an outsized effect on the global economy, hurting manufacturing and energy production worldwide by impeding the flow of input commodities and fuel to critical industry bases.

A study by the CSIS's ChinaPower Initiative found that when flooding impacted Thailand's HDD manufacturing industry—one of the component industries reliant on the Strait of Malacca—the damage reduced global hard drive production by 30%. This incident provides a window into the issues posed by the world's reliance on the Strait of Malacca. The narrow strip of ocean doesn't just traffic enormous quantities of trade: it enables a vast array of economic sectors by providing a thoroughfare for critical amounts of raw materials, input goods, and intermediate products. While it's possible to measure the direct consequences of impediments to trade there (increased costs, longer shipping times, and higher cargo insurance premiums) it becomes exponentially harder to consider the costs that would ripple throughout the world economy—and exponentially more terrifying too.

Tab 9 – Formal Notice From DHS CISA

Alert (AA30-089A)

11/5/2022

Unknown Actor Threatens Ransomware Against Shipping

Summary
The Cybersecurity and Infrastructure Security Agency (CISA) encourages asset owner operators across all transportation and infrastructure sectors to review the threat actor assessment below and attached IoCs to ensure corresponding mitigations are applied.

An unknown cyber threat actor posted on the public platform,
SwipeUp, threatening the disruption of major shipping companies. While the legitimacy of the threat is unknown, the message demanded a payment of equivalent $10M in Bitcoin to refrain from all action. At this time, the unknown actor responsible for this extortion has not compromised operational technology systems or deployed any form of attack against commercial shipping companies.

Message:
“We possess the highest capabilities to completely destroy your operations. If you pay us 10 million USD in Bitcoin, we will leave your big boats alone. “

Assessment:

- The legitimacy and identity of the actor is unknown. Several messages have come from IP ranges associated with Russian, DPRK, and Thai intelligence services.
- Unknown actor has not been associated with any known compromises or past incidents at this time.
- There have been recurring efforts to improve the security posture of the maritime industry to cyber risks, but improvement is needed.

Tab 10 New York Times Report

The New York Times

Afternoon News Capsule: Maritime Malware Leaked by Shadowy Group

A hard choice rests on major shipping companies: whether to pay up or hunker down against the online threat

By Kath Phillips

Nov. 7, 2022

Washington, D.C ---Earlier week, an unknown actor publicly threatened major shipping companies, demanding $10 million worth of bitcoin or promising to wreak havoc on maritime operations and business around the globe. Experts have debated the legitimacy of the threat but confirmation, at least in part, of the potential attacker's capability came earlier today with the release online of a collection of hacking tools and research from an Israeli security firm. The company, Ipnos Collective Security, was a

penetration testing and security research firm focused on operational and information technology in the shipping industry.

The online leak allegedly comes from a compromise of Ipnos' internal project management system with gigbytes of instant messages, unpublished white papers and background memos, code samples, several fully functioning tools, and reams of research on potential vulnerabilities. One well-placed industry expert, speaking on the condition of anonymity, said the cache was one the most potentially harmful she'd ever seen in operational technology and could provide massively disruptive to the maritime industry.

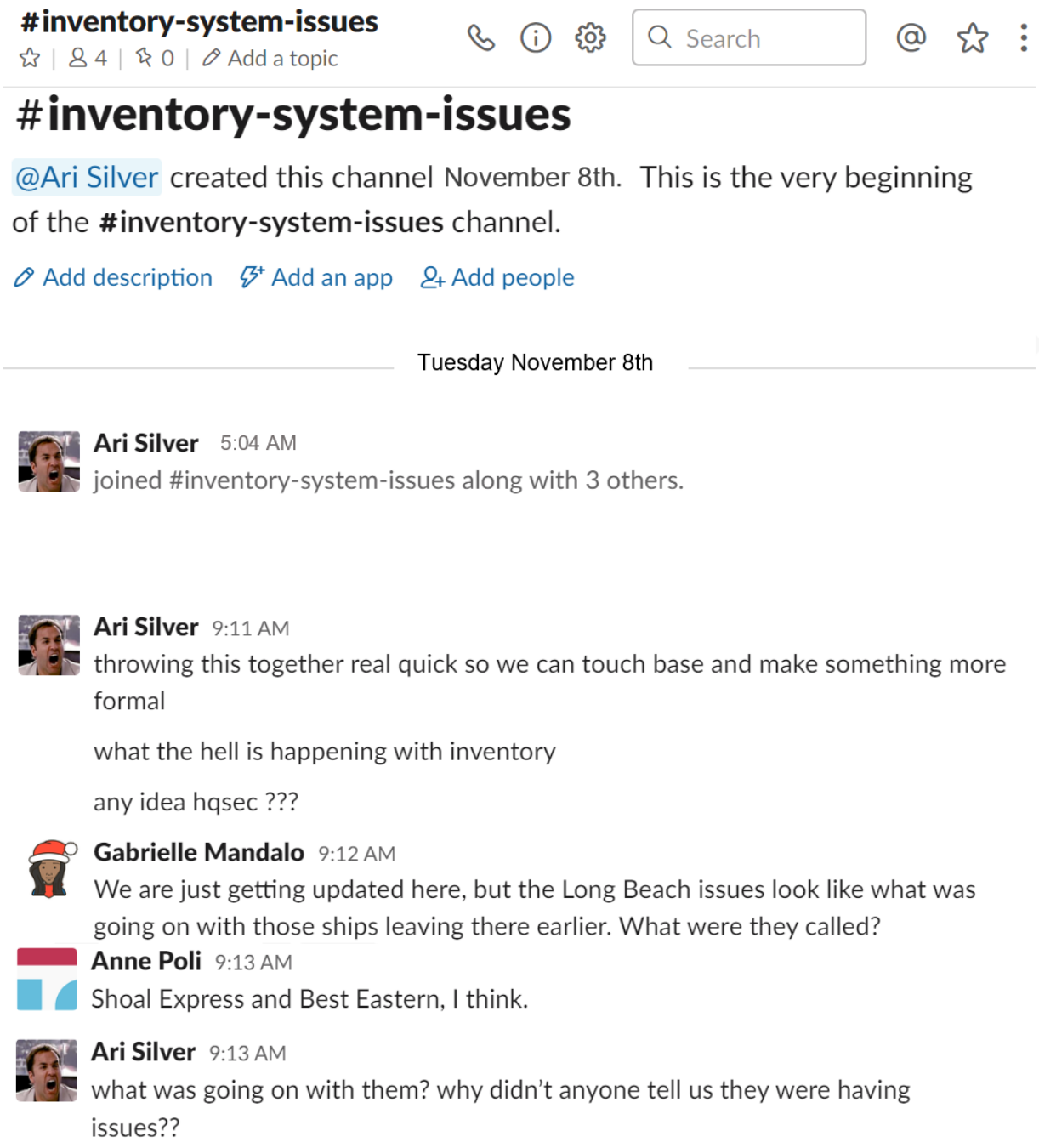
While the source of the malware leak is unknown, several commentators indicate their believe the same actor extorting major shipping companies could be responsible as a manifesto released on pastebin along with the leaked tools shares similar language and tone with emails received by firms threatened with extortion. With the potential to lock shipping companies out of their own networks and disrupt maritime navigation, communications, and control capabilities, these leaked third-party tools puts shipping companies in a difficult position: either pay off the attacker or call their bluff. One researcher claimed the tools were a ready-made kit of offensive action against maritime targets, "Cyber attacks on the high seas could be next, these tools are not the work of script kiddies and wannabes, they're dead professional kit with brilliant simplicity and clever choice of targets to boot".

Though the targeted companies did not provide comment on the potential economic and safety issues posed by the situation, the Department of Homeland Security's CISA issued an advisory. After warning maritime infrastructure and transportation sectors to increase their security efforts, CISA claimed a resolution may be imminent. "We are aware of the leak and are working with our international counterparts to identify the

sources of the threat needed to keep our people, ports, cargo, and ships safe and secure." said CISA's Deputy Assistant Director for Cybersecurity, William O'Leary.

The holiday season is rapidly moving into full swing and the prospect of major cyber-attacks on maritime infrastructure could unnerve markets even without a significant event. The next few weeks may prove critical as authorities race to uncover the source of this leak and mitigate the risk posed by newly available malware.

Tab 11 – Slack Channel (Will be made to look like slack once last edits are made)



Anne Poli 9:14 AM
something buggy in their inventory. The manifests kept deleting containers and or changing random fields of data. It was only a few containers though. Can long beach inventory confirm that's what going on?

Ari Silver 9:14 AM
yeah rich go and confirm for us if you have the time

Rich Morelli 9:15 AM
Sorry, Ari and I have been working serious hours to get this sorted out and we're having trouble. It sounds similar. We keep losing containers or grabbing the wrong ones whenever we hand off to drayage. That was definitely port side though, haven't heard about ship side till just now. The errors aren't huge, but they've been taking a while to sort out. Lot of bottom stack mix ups.

Gabrielle Mandalo 9:16 AM
yikes. Is it getting worse?

Rich Morelli 9:16 AM
Hard to tell. We're getting better at preempting issues and working out a container verification scheme while we try to correct the underlying issue, so the rate of issue occurrence is hard to judge.

1 reply Today at 9:16 AM

Ari Silver 9:17 AM
that's corporate speak for "the interns running between stacks are getting faster so we have no clue"

Anne Poli 9:17 AM
what happens when you try to recover logs from backup?

Ari Silver 9:18 AM
sometimes it works, sometimes they come back messed up the same or differently. Some ships don't even have their backups. it's taking more time to load in than to just manually double check though. except when someone opened the banana container, that took a while to clean up.

still waiting on why we never heard about those ships

Gabrielle Mandalo 9:19 AM

They actually emailed the manifest summaries before they even left Alaska and well before they hit Long Beach but we don't get the container by container breakdown or where they're stacked on ship till they pull the Manifest Data Unit in port. Things have been picking up though with the holidays, you know, more ships and more crew transfers. It was like maybe 30 containers, just wasn't a priority. Our bad.

What's the portside impact? How bad are wait times?

Rich Morelli 9:20 AM

Maybe 10% slower? It's not too bad, Ari and his team are just completely stuck

Ari Silver 9:20 AM

don't blame me, this inventory program has always been a pain. I swear every ship has a different version and not a single one is up to date. when I look at the logs themselves, they get deleted or shuffled which is making it even slower. i kinda wanna stop touching things and see what happens cuz this isn't working as is

Anne Poli 9:21 AM

we can look over it a bit here if you guys need rest. I have a good relationship with a couple of their engineers, I'll reach out. Where are those earlier ships now?

Rich Morelli 9:22 AM

long gone. They unloaded and sailed out before anyone knew there was a problem. Their containers sat in the stacks for a while, nothing urgent, so we didn't catch it until a few days ago.

Ari Silver 9:22 AM

so anywhere between here and manila, awesome. what's that, like a third of the planet to check?

Gabrielle Mandalo 9:23 AM
We'll get in touch and figure out what happened. You said Manila?

Rich Morelli 9:23 AM
Not sure exactly, maybe Tuas, one with a quick refuel in Manila. we can double check. All our other systems are fine. The delays are actually making dockage a lot easier.

Anne Poli 9:24 AM
So, correct me if I'm wrong, but this sounds more frustrating than anything. Maybe a corrupted inventory file gone bad? We'll get another channel going to share notes and I'll look over the Best Eastern and Shoal Express incident reports.

new messages

Gabrielle Mandalo 9:25 AM
I'm going to be safe and reach out to CISA just in case. Start talking to BOLH about the software and if they've seen issues like this before. Should check in with any ships who've offloaded since the problem began too. I'll talk to management about opening up some extra personnel and hours at POLB, and if you could formalize a system for the manual process, Rich, that'd be great as we move into these next high-volume weeks.

Tab 12 – Twitter Chain

Joe Williams ✓
@OTwarrior

Follow

Watching closely the #infosec developments at the Tuas Mega Port in Singapore. Hearing multiple complaints from pilots + crew that port management infrastructure is facing "technical difficulties" (where have I heard that before...) in regards to its cargo management software [1/2]

7:29 AM - 9 Nov 2022

224 Retweets **900** Likes

14 224 900

Joe Williams ✓ @OTwarrior · 7:30 AM
Replying to @OTwarrior
Possible disruption to database integrity also being reported... There's chatter that port management is thinking about reverting to paper backups to process ships + cargo manifests. More to follow. [2/2]
15 108 423

Sara Steves ✓ @InfoSecBoss · 8:23 AM
Replying to @OTwarrior
Sounds like malware to me. Do you think it's sophisticated #ransomware or script-kiddies-got-lucky?
8 23 42

Kelly Edelman ✓ @InThePyWeeds · 9:12 AM
Replying to @OTwarrior
Alarmingly similar news – my sources say that commercial ships near Strait of Malacca are having comparable technical difficulties.
2 37 14

Safa Patel ✓ @CyberWatcherOT · 9:45 AM
Replying to @OTwarrior
Sounds very similar to the 'techincal difficulties' port control were having @portoflongbeach. Could it be the same malware? Did it jump US -> Singapore?
3 14 7

Joe Williams ✓ @OTwarrios · 10:13 AM
Replying to @OTwarrior
Could be. If so makes me very concerned. Number of ships leaving + entering those ports surely close to 100 each day. If it did jump, no telling which ship it came from, where it will show up next, etc.. Tracing + containment should be no.1 priority.
31 54 62

Cornellious Fidget @CyberDiver · 1:14 PM
Replying to @OTwarrior
If this is intentional malware, it needs a name. I call dibs on NotNotPetya. No - Boaty McMalwareface!!
1 4 8

Tab 13: Interagency Email Chain

From: William Klein <wsklein@fbi.gov>
Sent: 9:12PM - 11/9/2022
To: Francis Yusif <francis.yusif@HQ.DHS.GOV>; Flora Galarza <flora.galarza@civ.mail.mil>; Mabel B. Edwards <mabel.b.edwards@uscg.mil>
Cc: William Gray <william.gray@civ.mail.mil>; Simon Park <simon.park@HQ.DHS.GOV>; Milton Handel <milton.c.handel@uscg.mil>
Subject: Operations at Long Beach Port

Francis, Flora, and Mabel,

Thanks for hopping on a call today on such short notice so we can coordinate on this issue. FBI has jurisdiction over the Port of Long Beach so we'll coordinate with Coast Guard, USN, and DHS once we've been able to match forensics of the ship computers to what we're seeing in port.

Best regards,
Will

William Klein
Cyber Division
Federal Bureau of Investigation

From: Francis Yusif <francis.yusif@HQ.DHS.GOV>
Sent: 11:34PM - 11/9/2022
To: William Klein <wsklein@fbi.gov>; Flora Galarza <flora.galarza@civ.mail.mil>; Mabel B. Edwards <mabel.b.edwards@uscg.mil>
Cc: William Gray <william.gray@civ.mail.mil>; Simon Park <simon.park@HQ.DHS.GOV>; Milton Handel <milton.c.handel@uscg.mil>
Subject: RE: Operations at Long Beach Port

Will,

Thanks for the recap. I know we're all on edge here with the timing of the incident. CISA has notified owner/operators of the risk and we're working to respond to a potentially related event with this Ipsos leak.

Flagging for the group that CISA has also received a vulnerability disclosure for Comprehensive Inventory Management System Software, developed by Big Ocean Little Heart LLC. We believe that this software is in use at the Long Beach Port and that the vulnerability may be exploited. BOLH is working on rolling out a patch, albeit slowly.

We have also received notice from several shipping companies that they have received ransom emails from an unknown source demanding payment in exchange for not disrupting their navigation capabilities.

CISA should be coordinating the incident response – we've got relationships with the affected software vendors and have already been in touch with the impacted shipping companies. We'd welcome FBI to work with us to address the criminal investigation but this is an ongoing cyber attack with potential for broader effects so we'll be asking DNSA for a Deputies meeting on this.

Sincerely,
Francis

Francis Yusif
Cybersecurity and Infrastructure Security Agency
US Department of Homeland Security

From: Flora Galarza <flora.galarza@civ.mail.mil>
Sent: 4:40AM - 11/10/2022
To: Francis Yusif <francis.yusif@HQ.DHS.GOV>; William Klein <wsklein@fbi.gov>; Mabel B. Edwards <mabel.b.edwards@uscg.mil>
Cc: William Gray <william.gray@civ.mail.mil>; Simon Park <simon.park@HQ.DHS.GOV>; Milton Handel <milton.c.handel@uscg.mil>
Subject: RE: Operations at Long Beach Port

All,

DoN and USD(A&S) are monitoring this situation closely with respect potential risk to POLB and major West Coast embarkation facilities. Will look for update risk analysis from DHS CISA. Please address this in a timely manner, we're monitoring the potential threat to our ability to project force from the West Coast and need to address this before CVN-70 and her group return to Kitsap. Francis, we would have appreciated earlier notice on the ransom and exploitation of this vulnerability as it has the potential to directly impact Navy assets.

SECDEF has directed we escalate this to NSC with DoD leading if there's not resolution or clear risk mitigation strategy moving forward in the next several days.

/r
Flora

Flora Galarza
US Department of Defense
OSD

From: Mabel B. Edwards <mabel.b.edwards@uscg.mil>
Sent: 8:43AM - 11/10/2022
To: Francis Yusif <francis.yusif@HQ.DHS.GOV>; William Klein <wsklein@fbi.gov>; Flora Galarza <flora.galarza@civ.mail.mil>
Cc: William Gray <william.gray@civ.mail.mil>; Simon Park <simon.park@HQ.DHS.GOV>; Milton Handel <milton.c.handel@uscg.mil>
Subject: RE: Operations at Long Beach Port

All,

Great to hear there's suddenly so much interest in the maritime. USCG has been responding to the two infected vessels out of Long Beach since they originally identified the problem. We'll continue to coordinate on this given the maritime nature of the crisis and our unique capabilities there.

We're also working with the harbor master at West and East coast commercial ports to try and ensure traffic doesn't snarl too badly.

Francis – please flag for us before this gets kicked to NSC again, we need to have a concrete plan of action in place before we feel ready to present the group's course of action.

More to Follow

Sincerely,

Mabel B. Edwards
US Coast Guard

From: William Klein <wsklein@fbi.gov>
Sent: 11:12AM - 11/10/2022
To: Francis Yusif <francis.yusif@HQ.DHS.GOV>; Flora Galarza <flora.galarza@civ.mail.mil>; Mabel B. Edwards <mabel.b.edwards@uscg.mil>
Cc: William Gray <william.gray@civ.mail.mil>; Simon Park <simon.park@HQ.DHS.GOV>; Milton Handel <milton.c.handel@uscg.mil>
Subject: Operations at Long Beach Port

All,

Due respect to USCG but is the organization really equipped for this? Do you even have a cyber incident response team capable of deploying out to a non-USG vessel or dealing with the forensics work shore-side?

-Will

William Klein
Cyber Division
Federal Bureau of Investigation

Atlantic Council

CYBER 9/12 STRATEGY CHALLENGE

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 Fall 2022. 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:

Oral Policy Brief (Day 2): For the second 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 2.5 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 March 2020. Explore the implications of that information, not the plausibility.

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 – CNN Article
Tab 2 – LOBH Internal Security Report

Tab 3– Wall Street Journal Article
Tab 4 – Søgard Security Report
Tab 5 – Bloomberg Article
Tab 6 – Pentos **Think Tank Panel Transcript**
Tab 7 – Integrated NSC Document
Tab 8 – Economist Article

Tab 1 – CNN Article

Hackers Use Ransomware Campaign to Target Major Shipping Ports

By Sara Tonin

Updated 8:26 AM ET, Sun November 11, 2022

(CNN Tech)- Global shipping ports are experiencing a well-coordinated ransomware attack. The attack, named "saBOATeur" by industry experts but increasingly referenced as "NotPetya 2.0" for its resemblance to the broadly disruptive 2016 cyberattack, appears to have originated at a port in the United States before proliferating across Asia and parts of Europe, affecting ships and ports from California to Shanghai.

Tuas Mega Port, one of the largest in the South China Sea and a key trading hub in the region, has seen operations slow to a crawl. Officials warn that other facilities will be impacted as well as they scramble to respond, but it is uncertain how systems are initially compromised and infected.

Tuas Mega Port is close to the Straits of Malacca, a key strategic bottleneck for global trade in the region, and the slowdown in the harbor's cargo processing times has begun to flood the already-crowded strait with vessels. Analysts project a worst-case scenario could cost the global economy upwards of $100 billion after just one week of critical port disruption.

Although it is unclear how harmful the malware will ultimately be and who is behind it, researchers continue to monitor the attack and are trying to determine the goals and identity of the attacker.

This story will be updated.

Tab 2 – LOBH Security Intelligence Report

LITTLE OCEAN BIG HEART LLC.

INTERNAL USE ONLY || **INTERNAL USE ONLY** || **INTERNAL USE ONLY**

TO: LOBH BOARD, CISO, SECURITY COMMITTEE
FROM: SIGIN Response Team
SUBJECT: Multi-Event SEAFARER Compromise

EXECUTIVE SUMMARY OF REPORT TO CISO–11/11/2022

Since initial reporting of issue ID #A1763 and contact with Long Beach Port Authority concerning inventory irregularities, operators at Tuas Mega Port have contacted LOBH support teams reporting similar issues. LOBH has not contacted local government or media regarding Tuas Mega Port issues. A LOBH support team operating out of Southpoint, Port Klang independently reported similar issues at reduced scale to LOBH management but has not alerted Port Klang Authority yet. In all three affected ports, initial infections in database components have led to compromised inventory management systems and impacted container manifest, bulk cargo, and other tracking systems. The net effect on operating entities is complete loss of records determining cargo location, content, and destination, among other data fields, requiring time consuming analog substitute tracking systems and manual confirmation in Tuas and Long Beach. Situation in Klang is expected to deteriorate similarly within 2 business days.

Remediation efforts by local incident response teams have been unsuccessful beyond establishing a placeholder protocol for affected ports. Reboots and backup restoration attempts have failed. Increased port volume due to seasonal demand and consequential operational load is straining personnel and operational capacity at all affected ports. Analysis expects wider spread of infection and concomitant decrease in port functionality associated with SEAFARER compromise. Loss-prevention measures must be undertaken promptly.

Current remediation team is interacting with USG elements—DoD, USCG, and CISA—for Long Beach Incident response. Tuas Mega Port Authority is drafting external coordination plan. Recommendation is to contract independent security firm to investigate issues and begin remediation efforts on their findings while diverting current personnel to mitigation efforts as direct incident response has been minimally impactful to this point. Best knowledge of current situation indicates ransomware infection of SEAFARER systems at unknown point affecting both ships and ports. Contained in detailed report below are incident reports, email exchanges, database logs, and timelines.

Tab 3 – Wall Street Journal Article

THE WALL STREET JOURNAL.

OPINION

Anchors Aweigh on an Unlikely Collaboration

Will the recent cyberattacks on shipping ports lead to future collaboration between the two rivals?

By Ronaldo Cohen and Cosina Ruiz

Updated 7:14 AM, 11/12/2022 ET

As an evolving cyberattack spreads through ports in both the Pacific and Indian Oceans, it is tempting to ask why the two largest stakeholders - the United States and China - are not working together to resolve the issue.

Both nations are already suffering heavy losses from the incident. A considerable amount of Chinese trade runs through the Strait of Malacca and the Tuas Mega Port, and sizable Chinese investments in the area over the past decade reflect this economic importance. For the United States, the Strait represents a key security interest, facilitating high value shipping links to Europe and the Middle East from valuable West Coast ports. On the home front, the delays and backlogs at the Port of Long Beach in California are mounting as the pre-Christmas season gets in full swing.

But as of yet, the two nations have been working in silos. This has to change. Erstwhile rivals, the two states have too much at stake to maintain a vestigial cold-war mentality in the face of global threats like this evolving cyber-attacks. A joint incident response may be the only way to pick apart what is happening.

State-level information sharing increases a nation's capacity to fight an attack by combining the knowledge and expertise of multiple countries. This is particularly useful here, where reports suggest the disruption to the ports is linked by the same malware.

Cooperation would do more than solve this one problem. According to the Council on Foreign Relations, international cooperation among states would help "to mitigate threats such as cybercrime, cyberattacks on critical infrastructure, electronic espionage, bulk data interception, and offensive operations intended to project power by the application of force in and through cyberspace."

The path forward, then, is clear; but why has it not been taken?

Since the 1949 overthrow of the US-backed Nationalist Chinese government by Chinese Communist Party leader Mao Zedong and the subsequent establishment of the People's Republic of China (PRC), US-China relations have been strained. A common enemy in Russia set the stage for improved US-Sino relations during and after the Cold War, with normalized diplomatic and trade relations coming in the decades that followed. When China became the world's second-largest economy, a US "pivot" to Asia was announced shortly after. The relationship, while uneasy, was civil.

But today relations have again soured. Chinese treatment of political dissidents, ongoing trade wars between the two economic superpowers, and accusations of PLA-backed intellectual property theft alongside American efforts to support the military development of several small surrounding states and alignment, if not outright sponsorship, of pro-democracy groups in Bejing have stood in the way of a long-lasting US-Sino partnership. However, if the two nations cannot learn to work together, the effects of this cyber operation and others to follow it could forever shift their place in the global world order.

Tab 4 - Søgard Security Incident Report

Søgard Cybersecurity Solutions

In the Business of a Safer World

Threat Level	**High (4/5)**
Client	Little Ocean Big Heart LLC
Event Date	2/3 November 2022
Report Date	15 November 2022
Affected Systems	SEAFARER Integrated Management Suite
Threat Actor (TA)	UNKNOWN
TA Language	American English
TA Timezone	EDT (UTC-4); PDT (UTC-7)
Analyst(s)	Veronica Kennelly

Client Background: Client is a large maritime logistics company providing crew, cargo, and inventory management solutions for ports, shipping, and warehousing entities in over 30 countries with a heavy market share. LOBH products interact with over 70% of containerized and break-bulk cargo in a given year at some point in their logistical cycle, and over 90% in the Pacific transshipment market. Their most successful product is SEAFARER Integrated Management Suite, a cargo, inventory, and manifest management software suite with port, ship, and intermediate terminal interfaces built on LOBH's Comprehensive Inventory Management System (CIMS) framework.

Overview: Client reported three ships experiencing similar inventory manifest issues (corrupted or reverted data), and client internal report confirmed malware leveraging two significant and unpatched vulnerabilities—a Windows .lnk storage-console transfer vector and a scaled data editing overflow vulnerability detailed in LOBH Issue Report ID: #A1763 (attached). At least two affected ships were allowed to sail out of Long Beach without intervention. Since, Long Beach Port Authority has observed severe and escalating port-side inventory disruption. Similar database disruption has been reported from the following ports: Tuas, Klang, and Guangzhou. Analysts have confirmed both ship-to-port and port-to-ship spread of the malware, sourced all disruption so far to the initial ship infections, and currently report with **HIGH** confidence that additional ports are affected but haven't yet seen disruption due to slow initial spread of the data alterations (Long Beach took approx. 5 days to notice alterations due to high container volume).

Technical Specifications:

Insertion: Forensic analysis confirms that initial infections gained system access at LOBH by obtaining passwords left in an unsecured S3 bucket by an engineer for managed security services provider [REDACTED]. Access allowed injection of malware into ship systems with logged-in admin accounts.

Spread: Malware contains several worm components undergoing analysis. USB transfer of manifests from ship to port and port to ship transmits malware to uninfected databases, assessed with **HIGH**

confidence in the field and reproduced in our environment. Email transfer of manifests in both directions transmits malware with **MODERATE** reliability, though only port-to-ship transfer has been reproduced. Both methods are widely implemented. Scope is not limited to SEAFARER databases. Malware contains simple yet robust modules for multi-system compromise and has affected LOBH system interfaces in drayage, freight, trucking, and at least one gantry crane linkage. Further analysis is ongoing, but several modules probe improperly siloed databases running on other common logistics software frameworks.

Payload: Current payload corrupts or reverts inventory records while destroying local caches and backups. Writes are bounded by inventory item references resulting in a slow initial phase of intra-port spread given large enough cargo volume. End result is eventual and total loss of reliable inventory records system-wide after period of rapid acceleration. Similar effects observed on ships, though malware sometimes is constrained by arbitrary runtime limits and limited item reference in transit, leaving only partial file corruption. Unclear if this is intentional anti-forensic feature or hasty development error. Given potential reversion reach, it is difficult to use partials to recover inventory data without manual confirmation of cargo verity.

Leave-Behind Payload: Efforts to reconstruct databases from backup have not succeeded. Malware uses leave-behind ransomware stored pervasively. Backup attempts result in re-corruption of loaded data and novel infection of backup systems using a Twofish cipher embedded in adapted PyLocky ransomware. This module has significantly slowed any attempts at data recovery and severely frustrated incident response.

Demonstration of Capabilities: Malware package is robust but not particularly complex, as methods are visible and obvious upon forensic examination. This attack required some in-depth knowledge of SEAFARER conventions and systems, which are not well concealed, and there is no demonstration of exquisite development capabilities on the part of the attackers.

Attribution: Analysts report with **LOW** confidence that due to variable names and time-zone specs, attacker is based in the United States and not a state actor, though spoofing such characteristics would be a trivial task. Notably, there are both British- and American-English spellings of several variable names.

Next Steps:

Søgard recommends port and shipping line operators develop and employ analog inventory management substitutes immediately, further isolate backup systems and separate infrastructure, implement contingency plans for transfer congestion, and begin investigating local databases for evidence of infection. Further guidance on international collaboration for infection quarantine is recommended but beyond the scope of this report.

Tab 5 – Bloomberg Article

Bloomberg

Markets

US Markets Face Shipping Disruption

By Bart Haroldson
5:23 PM – 11/16/2022

A tidal wave threatens to upend markets as a cyber-attack has disrupted the global shipping industry, with disastrous effects for businesses in the United States. The origin of the incident, which appeared first at the Port of Long Beach in California before spreading to Asia and a handful of European ports, is as yet unknown. What is clear is the damage it continues to wreak on affected ports and shipping routes. [Click here to read our October 21 article on the busiest shipping season on record.]

The cyberattack appears to interfere with the port management software used by the port authorities and the electronic shipping manifest used by the ship's captain. This couldn't come at a worse time for the global shipping industry, as an exceptionally busy holiday season has

increased the number of vessels attempting to dock by an unprecedented 20% from the previous year.

In response, port authorities have resorted to drastic measures. Both Long Beach and Tuas have resorted to manually sorting, identifying, and checking the cargo goods coming into port, considerably slowing down processing time. Both ports have also shut down for days at a time in order to stem the swell of new ships trying to offload and to give port management precious breathing room to manually sort incoming cargo. Ships, unable to dock or deposit their cargo anywhere else, must drop anchor outside the ports, for days and even weeks at a time. This is already creating considerable congestion in and around the ports and poses a serious safety concern, especially in high-traffic zones, such as the waters surrounding the Strait of Malacca and in the South China Sea.

What is the estimated cost of this delay? In short, billions of dollars. Shifting shipping away from the Strait of Malacca entails costly delays and disrupted timetables. The inability for ports to offload traffic at anywhere near normal rates means ships at anchor for days or weeks longer than anticipated. Best case is that the contents are durable goods like automobiles and toaster ovens. Worst case – spoiled food and volatile fossil fuels.

A worst-case planning scenario entails all three primary straits through Indonesia forced to severely reduce traffic, forcing many vessels to sail around the southern coast of Australia before pushing north into the Philippine Sea. This would be analogous to traders rerouting around Africa when the Suez Canal was closed from 1967 to 1974, and would carry considerable supply chain disruptions. Congestion and delays also lead to significant economic loss for businesses in the US and abroad.

For example, for each week the Strait of Malacca is closed or otherwise disrupted, shipping costs continue to rise, already high because of a period of peak demand. Companies must also pay for additional crew hours, extra fuel, and insurance rates, costs made even worse if ships are re-routed. If the worst happens, and ships are rerouted around Australia, the additional monthly cost to shipping lines alone would be in the tens of billions. Businesses in the US, increasingly relying on internationally shipped goods, are already feeling the sting.

A look at the market

The world financial markets are already taking on water. Shares in some of the biggest shipping industry companies, such as Costamare, Little Ocean Big Heart, and Norsk Shipping, have dropped as much as 22% in the last two weeks. That they show no signs of rallying reveals the lack of confidence shareholders have in a near term solution to the crisis. The shipping market is famously vulnerable to risk; even a slight shock can have an outsized impact on sector profitability.

Further afield, oil prices in China have increased dramatically. China imports almost 80% of its oil from vessels passing through the South China Sea via the Strait of Malacca. For an oil-hungry country like China, any delays, short- or long-term, present a worrisome economic and political scenario.

The long-term market effects of this disruption are yet to be borne out but are equally as concerning. American businesses will likely see an increase in insurance premiums across all sectors as they make claims to recover their losses. SMEs in the manufacturing, shipping, and commercial import/export industries may go under, as their small size means they are unable to withstand the losses. This wave is likely to hit the Midwest as much as it hits Midtown.

Tab 6 – Pentos Think Tank Panel Transcript Excerpt

Stan Mutembe**, Moderator**: For those of you continuing with our second panel, thank you for rejoining us. This discussion will focus on "The Continuing Maritime Trade Crisis: New Developments and the Current State of Play" on November 20th, 2022. My name is Stan Mutembe, Associate Director of Pentos' Program on Naval Strategy. I am joined by three of the foremost experts in their fields. To my left is Lorraine Chai, Director of Thetis International, an NGO dedicated to coordinating international maritime agreements and policy. Next, we are lucky to have Director Marina Flowers from our fellow think tank the Center for International Governance Solutions, whom we recently collaborated with on our *Maritime Cybersecurity: Sailing the Tide* report. Finally, I am delighted to introduce Simon Candi of Dino Security Dynamics, where he has carved out a reputation coordinating cyber incident responses in the United States, the EU, Japan, and South Korea - all regions of interest for us today.

Simon Candi, Dino Security Dynamics: Thank you for having us, Stan.

Mutembe: Of course. Let's start with you, Marina**.** Would you mind telling us what's happened so far, with particular attention to the recent developments concerning AIS?

Marina Flowers, Center for International Governance Solutions: Sure! As I'm sure we're all aware, in early November, a cyberattack started spreading through shipping inventory systems throughout the Pacific and beyond. What your audience might be less familiar with is that a second attack appears to have begun a few days ago targeting AIS. AIS stands for Automatic Identification System—it's a protocol that lets ships tell each other where they are, how big they are, and so on. It makes transit safer, reduces collisions, helps direct traffic, and forecast scheduling transit of canals and marine chokepoints.

Something has happened to make AIS data highly unreliable, just in the past few days. I'm sure Lorraine can talk about the specifics but what we've been researching is potential impact. The area hardest hit by saBOATeur, the South China Sea, is our main focus. The region is full of large ports, massive numbers of ships, and very tight waterways—think the Strait of Malacca for example. Congestion from the port slowdowns is only going to get worse now that ships and port controllers are essentially flying blind without reliable AIS data, and we are growing increasingly concerned about the potential for escalation. Keep in mind, this is a highly volatile region—piracy near Indonesia, endless disputes over island chains between Vietnam, China, Indonesia, Malaysia, and the Philippines. The compounding consequences could be remarkably potent.

Mutembe: Thank you—Lorraine**,** would you mind explaining to us what exactly is happening to AIS and how it could have been compromised? I know Thetis International has been pushing for improved security at sea for years now.

Lorraine Chai, Thetis International: It's actually a frightfully mundane story, Stan. In short, AIS is incredibly insecure. It's required for all passenger ships and commercial ships over 300 gross tons—in other words not that big, and ships often have it even if not required. It's almost everywhere. It's also

extremely vulnerable - information that it passes between ships lacks any kind of encryption and there are no digital checks to ensure information is accurate or from the source it claims. AIS data doesn't even contain timestamps of when it was generated or sent. We've done a fair bit of research on AIS, and one of our analysts can forge transmissions with a laptop, a coat hanger, and a car battery. *[laughter]* You can too if you know what you're doing. *[laughter slows]* That's barely an exaggeration, it's scary!

So, security isn't a question of whether or not you can, but how you're going to attack, and how comprehensively. An attacker could go after AIS broadcasts, or target the software and networks coordinating transmission receipt. What we're seeing right now is a variety of ship data interference. Ghost ships, which have come up before, are all over the South China Sea—transmissions that don't correspond to a real boat. Many other vessels are unable to broadcast their location accurately. A number of ships are broadcasting faulty information—incorrect flags, inaccurate dimensions and tonnages—and there are some ships seeing total system failure where they can neither broadcast nor receive. There could be other things happening though. It's really limitless what you can make the system do. So, Marina's assessment about increased congestion and collision is an understatement. Vessels *are* sailing blind to ships around them, and that's hardly the worst of it.

Mutembe: Switching to the security side of things, what can you tell us from your experience Simon? What's coming next?

Simon Candi, Dino Security Dynamics: We definitively don't know who is behind this or precisely how it's happening. We can say something about where the attack is likely coming from – a collection of offensive tools and penetration testing software leaked from Ipnos, an Israeli maritime cybersecurity company. The leaked data is public and includes a tool used to execute operations against maritime navigation and identification systems. I can't be particularly specific, but investigators are using that as a starting point, a kind of template for understanding how someone might go about undermining the AIS infrastructure.

That's the first step in any investigation—determine what has been compromised, to what extent, and how. The other branch of a response is mitigation, or what to do in the interim between compromise and remediation. Vessels can sail without it, and many have plans for AIS outages already in place. What I'd like to see is a formal operationalization of those protocols followed by their widespread distribution. I am worried that even veteran seamen have become accustomed to AIS, and might lack the capacity to execute these more traditional, old-school protocols – which may lead to escalation, as Marina mention ed. Most worrying is that even a great mitigation plan relies on ship crews, which have grown smaller with the advent of AIS and other automated functions. They could be exemplary personnel, but even the best of us can only handle so many 20-hour shifts. Ships are going to stay at sea with or without mitigation, and we mustn't let that persistence keep us from implementing solutions for them while we continue other investigations.

Tab 7 - Integrated NSC Document

FOR: National Security Council (NSC) Directors
RE:DPRK Intelligence Packet
DATE:NOVEMBER 24, 2022

PACKET SUMMARY: Multiple agencies submitted well-sourced intelligence items collected in tight timeframe concerning several developments in the DPRK. Given heightened tensions in region due to developing situation involving trade slowdown, items were compiled and fast-tracked for NSC review in context.

ITEM #1

DATE	NOV 18
THREAT LEVEL	LOW
ADMIRALTY CODE	B1
P.O.C. AGENCIES	CIA, NSA

CONTENTS: CIA analysts received tip from Chinese national tied to DPRK-China border smuggling syndicates describing **aberrant movements of individual** TELLER who is involved in DPRK special weapons development program in capacity as engineering and science advisor with some policy input. Recommendation was to increase monitoring of individual, who is currently tracked as a person-of-interest.

SOURCING: Source has historically proved **highly reliable**, particularly with regards to personnel movement around DPRK special weapons program

DETAILS: In response, CIA approved new collection against TELLER and raised priority intake for any lateral collection regarding DPRK special weapons movement. Review corroborated source observations, showing three confirmed attempts to evade REDMERCURY program surveillance over the past 72 hours. One was successful, resulting in a 4.5-hour window where location of TELLER was unknown. **Location was reconfirmed** before item was filed. **Priority monitoring continues** with NSA assistance.

ITEM #2

DATE	NOV 20
THREAT LEVEL	MODERATE
ADMIRALTY CODE	C3
P.O.C. AGENCY	CIA, DoS

CONTENTS: State Department cabled HIGHLY SENSITIVE relaying communication from PRC MFA indicating **increased instability in DPRK special weapons program funding**. Indicate regime has **supplemented ICBM development with limited export program** using highly radioactive fission byproducts including reactor and industrial materials. Increased emphasis on improved yield and fissile efficiency also indicated in core warhead program. Information lines up with partner observations and CIA analysis.

SOURCING: Source analysis traced communication to series of internal memos between MFA and MPS dealing with DPRK defector with access to senior leadership thinking who crossed border sometime in August. **Defectors have provided reliable intelligence**, and the MFA points of contact have not been directly involved in any of previous PRC misinformation and **has a good track record cooperating on intelligence items tied to DPRK**. At this time, credentials of defector cannot be corroborated, though he claims involvement in logistics side of DPRK special weapons program in managerial role.

DETAILS: Shifting priorities is a coherent response to changing pressures in the DPRK special weapons environment, and this report would line up with analyst predictions that regime would seek more sustainable sources of program funding. Kim appears to be modeling funding on late '90s RUS arms sales model.

ITEM #3

DATE	NOV 23
THREAT LEVEL	NONE
ADMIRALTY CODE	A1
P.O.C. AGENCY	USN, DoD

CONTENTS: USNINDOPACOM reports **losing acoustic contact with underwater unmanned reconnaissance vehicle** launched from **REDACTED** for reconnaissance and collections missions in the Sea of Japan, near Tanch'on. Technical reports indicate operator error resulted in a crippling collision with a near-shore outcropping. DPRK naval patrol recovered parts of the vehicle per visual sighting from **REDACTED** and initiated search to recover the remainder of the inoperable drone. This is not the first such incident (see attached report of UUV captured in 2005 under similar circumstances—cut optics cable led to loss of control), but captured UUV contains newer technology, particularly sensor package. **REDACTED** **was forced to leave station and is no longer in visual or acoustic contact with UUV or DPRK coastal operations zone.**

SOURCING: First-hand DoD report.

DETAILS: UUV mission had routine ship logging and mine mapping objectives. Navy reports with **HIGH confidence** that system security and encryption will protect critical technologies from being recovered by DPRK or other entities. **REDACTED** will return to station once period of acute patrol activity subsides.

Tab 8 – Economist Article

The Economist

Today Weekly edition Menu

Trade and Cybersecurity

No End in Sight

Market woes continue as international maritime crisis deepens

IT struggles with stopping malware, journalists with naming it

Nov 26th 2022

IN EARLY NOVEMBER, technical issues started to plague the second busiest container port in the United States. Confused operators along the roughly 25-mile waterfront stretch comprising the Port of Long Beach grew impatient as pandemonium built to a crescendo. Frustrations were manifest in miles-long backups of hundreds of flat-bedded tractor trailers awaiting offloaded containers recently arrived from Asia. At the heart of the bedlam was a failure of the system responsible

for tracking those containers and their contents. Suddenly, port operations knew neither the origins nor the contents of offloaded containers.

Like a viral outbreak, similar technical issues spread across the Pacific Ocean, afflicting major ports the likes of Klang, Guangzhou, and Manila. Behind the glitch causing headaches around the Pacific Rim was a piece of malware, sophomorically named “saBOATeur”. Latching on to ships via manifest files, the malware spread from port to port, infecting systems at each along the way and obliterating logs and databases. Shipping in the Pacific slowed to a crawl as ports resorted to manual checks, handwritten lists, and even post-it notes to keep track of cargo. As of today, several weeks into the crisis, critical ports in Australia, the Middle East, and around the Indian Ocean have been infected. Things have only gotten worse.

Double tap

AIS, short for automatic identification system, allows ships to broadcast their locations and vessel specifics to each other in (more or less) real time. It’s crucial for navigation, especially in the tight quarters of some of the world’s most crowded ports and chokepoints. On November 15, AIS suddenly began experiencing irregularities. Ship information was edited, deleted from, or added to the system sporadically, turning the open ocean into a minefield of nonexistent ghost ships, real ships turned invisible, and ships with incorrect location, size, and flag data. The combination of the two attacks, one inventory systems and a second on the AIS, has been disastrous. Ports are backed up as they scramble to manually perform tasks that have been automated by computers for the last two decades, congesting already crowded waterways. Ships are navigating by naked eye, draining the last reserves of crews already stretched thin as they drift in and out of what is essentially the world’s largest, angriest, and most expensive traffic jam. While no serious collisions have occurred yet, there have been dozens of reported minor hull-scraping incidents, and thousands of near misses, all of which slow down an already lethargic system.

Gridlocks and roadblocks

Most worrisome though is the lack of progress that has been made to remedy the situation. Security experts have struggled to restore ports to working order because the malware they are fighting scrambles data whenever they reload it from backups. Analysts have commented that, while the malware itself is not particularly complex, the systems it attacks are woefully under protected. The most successful remediation efforts, spearheaded by the Port of Osaka, are not even trying to fix the targeted databases, but rather working to make new, safer ones from scratch – but the task will take weeks to roll out on a large scale and longer still to adapt to all vessels waiting outside the port. Remedies for AIS are even further behind, as analysts have only just begun their investigations, and the immense international coordination required slows progress even more.

While the shipping industry awaits a fix, the crisis has taken a toll on the financial markets. Nearly every industry has felt the impact —refrigerated goods rot in port, factories and stores shuttered, and warehouses sit empty and unguarded. Once a surging torrent, global trade has declined to a feeble and unpredictable sputter, as no one can predict which and when goods will make it out of shipping hubs. China’s manufacturing juggernaut has been injured the worst as a gridlock developing in the Strait of Malacca has cut off the country’s critical supply of imported oil, and the shutdown has rippled across the world. The government is reportedly trying to fast track a massive pipeline project through the Tibetan Plateau to create a land route to

Middle Eastern oil refineries. The South China Sea, already overcrowded and overworked, most infected and thus congested trade zone. Southeast Asian countries are on the road to recession, as their economies are closely tied to the well-worn shipping corridors. The United States has not escaped harm either. While its newfound energy independence has spared it from the worst of international oil shortages, it too is experiencing manufacturing slowdowns, temporary localized food shortages, and widespread economic contractions as huge volumes of goods are blocked from shipment across the Pacific.

By the numbers...

Market indices: the Dow Jones has contracted by -6.3%; the S&P 500 by -5.4%; the Nikkei 225 by -10% (though it did rally once the Port of Osaka returned to 50% operational capacity); SSE Comp by a brutal -14.6%; FTSE 100 by -3.3%.

Manufacturing: By far the hardest hit industry (besides shipping), manufacturing is being forced to reorganize around local supply chains. Global production has slowed 14.5% so far and is projected to slow by 25% before a long-term solution is developed.

Trade: Unsurprisingly, trade has all but collapsed. From a high of just under $22 trillion USD in exports in late 2021, current estimates put the world on track for about a 24% reduction by the end of 2023 Q1. Real time numbers are difficult to come by, but estimates put losses at about $100 billion USD per week, and those losses are accelerating as effects spread and more goods require replacements.

...But not by the book

It's easy to get carried away worrying during a dramatic international crisis — and it has happened before, but researchers are probably underestimating the impact of today's trade tumult. A number of worst-case scenarios could quickly spiral out of control. Congestion could lead to an environmentally catastrophic collision between oil tankers, even in a harbor near a heavily populated city. A collision between military ships could escalate into conflict, and policymakers worry that China is eyeing a military takeover of the Strait of Malacca to ease its fuel shortages.

Prolonged economic distress paints an even more worrying picture. The worst affected countries—China, Malaysia, Indonesia, Singapore, Japan, and South Korea—could face civil unrest if shortages worsen, particularly as winter approaches in northern regions. Even in the United States, the worst affected nation outside of Asia, officials are worried about covering shortages as the holiday shopping season looms. The snowballing crisis is unprecedented, and economic impacts are already deep and far-reaching —the world is in uncharted territory as trade in the South China Sea asphyxiates, taking the entirety of a complex, interconnected system of international trade we have long taken for granted with it. ■

Atlantic Council

CYBER 9/12 STRATEGY CHALLENGE

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 Fall 2022. 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:

Oral Policy Brief (Final Round): For the final round 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.
- *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 2020. Explore the implications of that information, not the plausibility.

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 – Intercepted People's Militia Communications
Tab 2 – CISA Update
Tab 3 – Reuters Article
Tab 4 – NSA memo to the NSC

Tab 1 – Intercepted People's Militia Communications

Concourse > Thank you all for joining, Let's get on the same page about the progress of Operation Coalfire. There's a lot going on and a lot of noise in the media—I think leadership would like to know what we can take credit for, what to avoid mentioning, etc. before any PR moves. Myself included.
loomnlurk > good to touch base. !__front_runner__! has been running our technical operation and can answer questions. tech42gardner23 is our contact out of Hong Kong keeping us updated on the ground.
Concourse > Appreciate the introductions but let's get to it.
!__front_runner__! > it looks like our initial targeting wasn't as accurate as we'd hoped. we only knew the first port of call for the ships we loaded the malware onto, assumed they'd be up and down the West Coast.
Concourse > So the South China Sea is definitively us?
tech42gardner23 > 100%. I talked to a friend who works around Tuas, looks like our malware, front runner confirmed. We got lucky, hit big ports that ended up affecting our original US targets all the same.
loomnlurk > that should make adjusting our messaging easy enough. Still an assault on global corporate trade during yearly display of consumerism. just hit further down the supply chain. The whole mess is thanks to us.
Concourse > Good. We'd like to keep our communications a bit more professional than what Adam was putting out. If we talk less like we're the baddies in an 80's action movie, we might improve our recruitment a bit. But someone had a great idea about trying to pin it on a state to make our adversaries look responsible for their own issues. We're weighing pros and cons of a big publicity move now or later.
loomnlurk > We thought that interview with the Intercept was a bit much, felt awkward saying it.
Concourse > I think that's as much them as us. They've got a certain editorial…style.
Concourse > There are reports that ships are having navigation issue too—is that part of the payload?
!__front_runner__! > no, we don't think so. Someone else seems to have piggybacked our attack.
tech42gardner23 > it's sure helping us though—big impact, just hitting the news less, especially this side of the pacific. As far as reporters are concerned, a mess is a mess, and the government here is embarrassed to admit the second attack. there are significantly more ship collisions than making headlines too. It's really messing them up.
loomnlurk > I got worried about the slow initial spread and messed up targeting. Timeline was just off. No idea it would be this easy and effective.
Concourse >. loomnlurk, let's talk messaging soon. We're debating how vague to be and whether we can or should include the navigation issues if we take credit. Perfect target selection, and we're hitting them exactly where we wanted to, harder than we thought possible. This should ring the truth home amidst the offices and opulence where it needs to be heard. Be proud – you've struck a blow and we're impressed. Now you really have to show something ☺

Tab 2 – CISA Update

UPDATE: Alert (AA30-089A)

Attribution of Actor Threatening Shipping

Summary

The Cybersecurity and Infrastructure Security Agency (CISA) is able to make an update to Alert AA30-089A (threat to major shipping companies). National sources and methods can attribute the threat to Advanced Persistent Threat (APT) Bureau 121, affiliated with a state-sponsored DPRK entity. Analysts indicate that the threat is an attempt to increase internal revenue by leveraging shipping companies to pay a $10 million USD bitcoin ransom.

In addition, we can assert with moderate to high confidence the recent anti-AIS malware attacks on the shipping industry are the responsibility of the same unit. While bitcoin payments make it an unknown whether payment was made, Bureau 121 executed a comprehensive compromise of regional shipping through an attack on the AIS systems of major shipping corporations.

Assessment

- Attribution of threat is made with HIGH confidence
- Attribution of attack is made with MODERATE to HIGH confidence
- Unaffected vendors are urged to redouble efforts to secure navigation infrastructures
- Industry-wide overhaul of cybersecurity in maritime trade industries is recommended
- Attribution of inventory systems compromise cannot be made at this time but is understood as a separate attack

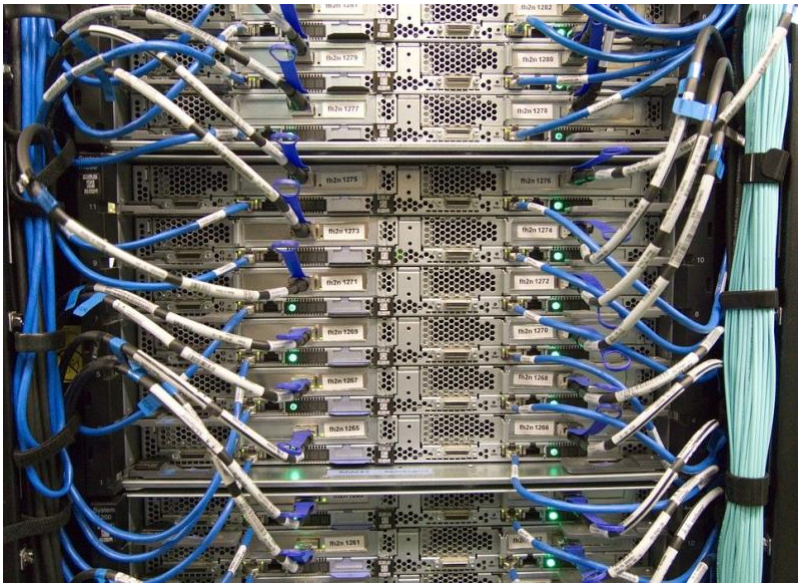
Tab 3 – Reuters Article

REUTERS

World News

Notorious hacktivist Phineas Fisher takes credit for Israeli cyberweapons leak

Wendy Turner, Michelle Campbelle



TEL AVIV (Reuters) – Hacker Phineas Fisher took credit early this morning on public platform SwipeUp for the leak of an Israeli cybersecurity firm's malware suite. The firm, Ipnos Collective Security, reported that the exploit tools were compromised earlier in November this year and were part of a larger leak including research papers, vulnerabilities datasets, and more. The specific project the suite was connected to focused on improving maritime cybersecurity.

The tools were put up for sale on a number of well-known grey market platforms, and not all of the websites have removed them. Among them are tools capable of disrupting navigation and communication for commercial vessels. Analysts believe that the current shipping chaos focused in the South China Sea, but reaching globally, is in part due to the use of the leaked cyberweapons. One tool specifically targets the marine AIS systems that recently ceased normal functions.

Fisher has a history of enabling corporate cyberattacks. The hacker (or hackers) behind the pseudonym have offered large bounties—up to $100,000 USD—to attack corporate networks and leak internal company and government documents. Firms who make cyberweapons for governments, including Ipnos Collective Security are also on the hitlist. While Fisher has a long history of making confidential information publicly available, he is seen more as of an enabler than saboteur and is not believed to be the source of the attacks that use malware he leaked.

Tab 4 – NSA Report to NSC

National Security Agency

North Korean Operative Update: DPRK Operative Eluded Surveillance, Boarded Unknown Vessel Confirmed To Contain "Dirty Bomb" Components And Nuclear Program Development Documents; December 2022 (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.

(TS/SCI/TK/DK) SUMMARY

(**TS/SCI/TK/DK**) On 30 November, 2022, under NSC recommendation, CIA and NSA increased operational surveillance of DPRK operative TELLER, connected to development of DPRK Nuclear Program. Individual had been observed undertaking evasive movements to undermine routine monitoring. Evasion attempts intensified under increased measures, frustrating recent operational load on reconnaissance assets caused by shipping chaos in South China Sea. During approximately 180 minute long window of surveillance blind spot caused by orbital arrangement of reassigned observation asset [redacted] operators lost track of TELLER. Review of long-range radiation readings from observational asset indicated [redacted] minimal anomaly indicative of diversion of significant quantity of cesium-137 and spent uranium pellets to Port of Namp'o. Combined with [redacted] communications sourced from and NSA reports with HIGH confidence that TELLER has boarded outbound DPRK transport or shipping vessel with components to construct functional dispersal weapon (dirty bomb) and to disseminate material acquisition instructions. Further observation of re-scrambling of several PRC naval assets in vessel's projected course area soon after indicates PRC awareness of situation. NSA and other elements have not been able to locate DPRK vessel due to regional maritime chaos.

Assumption with HIGH confidence is that DPRK is using regional maritime confusion to evade counter-proliferation surveillance and deliver a DIY weapons kit for export sale. Continued search by PRC vessels and USG ignorance of vessel location or identity suggests high risk of DPRK success. Intelligence

indicate buyer may be Hindu Nationalist Extremist group known colloquially as Saffron Flame. Report reliant on intercepted online and cellular communications has been assessed with MODERATE confidence, trending towards HIGH as DPRK ship course is approximated by PRC vessel tracking.

Saffron Flame is a political extremist organization with several wealthy backers and an ideologically hardline core of former Abhinav Bharat members. The group is of particular concern due to previous capacity toward violence against Pakistani military and civilian targets in sensitive regions including in Kashmir and a train running to Lahore. Saffron Flame operates without regard for human life and appears to prioritize mass casualty events as a means of disrupting administrative and government functions across Pakistan. Cesium-137 is a particularly troubling component for DPRK transfer due to ease of aerial dispersion, aerosolization, and water contamination, compounded by possibility of transmission of acquisition intelligence and handling procedures to Saffron Flame. Analysts have classified DPRK sale as a HIGH threat incident.

[…Full report truncated…]