TLP:WHITE

MTS-ISAC

2020 Annual Report

Maritime Transportation System

Information Sharing & Analysis Center

Helping Build the Maritime Cybersecurity Community



TLP:WHITE

Letter from the MTS-ISAC

For multiple reasons, 2020 was a year many of us will not soon forget. As we sat on New Year's Eve in 2019 and looked toward 2020, we were filled with hope and ideas, some concrete and others more abstract, for accomplishments we wanted to achieve in the year ahead. Early in 2020 the world quickly realized we needed to improvise and innovate perhaps a little more than we thought at the end of 2019.

So, innovate and improvise we did! In the maritime sector, a small group of U.S. critical infrastructure stakeholders across the country from both the public and private sectors met in February 2020 to discuss a fundamental challenge to their cybersecurity efforts. **They understood the importance of working together, sharing cyber threat information with each other to empower their individual risk management strategies while improving the collective resilience of the maritime sector**.

While other forums existed, this group of key stakeholders clearly had a fundamental requirement for exchanging timely, actionable, and relevant cyber threat information was not being met. The outcome was the formation of the nonprofit Maritime Transportation System Information Sharing and Analysis Center (MTS-ISAC). The group formulated an agreed mission, which is to **promote and facilitate maritime cybersecurity information sharing, awareness, training, and collaboration efforts between the private and public sector**. The execution of this mission will effectively improve cyber risk management across the MTS community and serve as the information exchange center of excellence for the maritime community.

Given the severe impacts from COVID-19 on the maritime sector, we are **incredibly grateful for the commitment of our Board of Directors and all our stakeholders**. On both the public and private sector sides, their dedication and support in our first year of operation was nothing less than remarkable.

While there is more work in front of us than behind us, our first Annual Report highlights the incredible progress made to date, including key milestones and results achieved in our first year. We believe it is an amazing testament to the dedication and devotion to duty of everyone involved in supporting our mission.

From all of us at the MTS-ISAC, we appreciate your support! Thank you!!

Stay safe *and* secure,

Scott Dickerson	Christy Coffey	John Felker	Julian Delgado
Executive Director	VP, Operations	Senior Advisor	Analyst

Contact Information

Please contact us at:

Website: https://www.mtsisac.org/contact
LinkedIn: https://www.linkedin.com/company/mts-isac/

Contents

Sailing the Ship While Still Building It

Newly formed organizations often struggle to find their sea legs in the early going. Having a clear mission and mandate for the Maritime Transportation System Information Sharing and Analysis Center (MTS-ISAC) and a highly supportive Board of Directors allowed the organization to immediately set a course and get to work. After forming as a nonprofit in February 2020, the MTS-ISAC used a multi-pronged approach to quickly create an operational tempo while also working to connect MTS-ISAC stakeholders with other critical infrastructure sectors.

The MTS-ISAC community experienced strong sharing among stakeholders right from the start. In fact, **information was being exchanged before we even had some of the basic communication and platform structures in place!** Terrific information sharing allowed us to rapidly form products and dive right into the MTS-ISAC mission. Muscle memories were quickly formed as **daily intelligence shares, regular webinars, and cybersecurity advisories** started flowing from the MTS-ISAC to our small community. It seemed like before we blinked, the MTS-ISAC had become an international exchange.

On the partnership development side, the MTS-ISAC joined the U.S. Department of Homeland Security's Cyber Information Sharing and Collaboration Program. This connection ensured that the MTS-ISAC was could both receive and share cyber vulnerability and threat information in a protected manner with other critical infrastructure stakeholders. Shortly thereafter, the MTS-ISAC became a member of the National Council of ISACs to similarly share information with other private sector ISAC communities. With operations underway and partnerships forming, the MTS-ISAC found itself quickly underway.

"Being able to interact directly with my peers across the maritime community to discuss and shape our information sharing mechanisms is incredibly powerful."

Sean Walsh, Director of Information Security,
Matson Navigation Company, Inc.

While the MTS-ISAC's journey continues, this first annual report will explore cybersecurity activity that targeted the MTS across 2020 through the lens of information shared by maritime critical infrastructure stakeholders to the MTS-ISAC. Here is an operational snapshot of the MTS-ISAC's 2020 year:

Provided	Responded to	Received over	Generated almost
62	**40**	**1,000**	**200,000**
maritime cybersecurity advisories	**requests for information**	**MTS intelligence shares**	**indicators for customers & sensors**

2020 Attack Trends Against the Maritime Transportation System

The MTS saw a marked increase in cyber-attacks since the onset of the COVID-19 pandemic. In addition to the attack on the United Nations' International Maritime Organization, **multiple public and commercial shoreside facilities and vessel owners and operators around the world were hit by ransomware attacks**. While the impetus for this increase in attacks is unknown as of yet, there are multiple factors that may have created an environment for the number of attacks to increase throughout 2020, including:

- **Geopolitical tensions** have remained high between nation-state threat actors and the multiple countries where their victims are located;
- The **COVID-19 pandemic** has impacted economies and an untold number of workers worldwide. There is the potential that some underemployed or unemployed workers have been lured into transnational criminal activities to survive;
- Due to a variety of **legal and law enforcement challenges**, cyber-attacks remain a relatively low-risk endeavor for many threat actors;
- A sudden and significant **increase in the number of remote workers** in 2020 increased the potential attack surface as the number of connections, often from less secure home and/or public networks to corporate networks, increased; and
- The maritime industry continues to modernize, and third-party integrations continue to increase, providing a target rich environment in an industry where organizations often do **not adequately resource their IT and security teams** even during peak economic times, and in which they may have further cut cybersecurity efforts as a result of the pandemic.

So, which cyber risk items trended high for MTS stakeholders in 2020? Are there unique threats to maritime? While ransomware incidents plagued the MTS across 2020, what adversary activity trended and may have contributed? Where did threat actors poke and prod? Let's take a closer look.

Both Sea and Shoreside…Phishing with COVID-19, Maritime, and Other Common Themes

Phishing remained a preferred attack technique, with Emotet and ransomware campaigns relying heavily on social engineering as a tactic across 2020. Common **phishing themes included invoices, DocuSign, OneDrive with links or attachments, missed messages (voicemails and facsimiles), and spoofed O365 alerts were reported by vessels, including tugboats, and ports** alike. While these themes have been successfully used by attackers for years, not surprisingly, in 2020 COVID-19 subjects were frequently reported by both shoreside and vessel stakeholders.

"As a best practice, we rotate seasoned cybersecurity crew between vessels so that they can both train and influence."

Paul Kingsbury,
Maritime Cybersecurity Engineering & Operations,
Royal Caribbean Cruises, Ltd.
(2020 MTS-ISAC webinar)

In November, a European vessel operator reported a Sat-C phish message with commonalities to a MTS-ISAC Sat-C phish advisory from April. Both of the COVID-19-themed messages directed the ship's master to report sensitive information to a spoofed government email address. While the messages were sent six months apart, analysts are confident they were sent by the same adversary due to commonalities.

There were also regular reports by ports of vessel impersonation emails with COVID-19, invoice, payment, port inquiry, itinerary, manifest, maintenance, and similar subject lines across 2020. In addition, emails spoofed vessel owners and operators and the Coast Guard as senders. Other maritime sector subjects were also used, including references to FEMA's Port Security Grant Program and TSA's TWIC Program.

"By correlating cyber security information across MTS critical stakeholders, the ISAC provides all of us the early warning needed to protect our individual organizations from incidents; value that we could not obtain elsewhere."

David Cordell, Chief Information Officer, Port of New Orleans (Port NOLA)

Unfortunately, email security **tools are not a panacea**, and attackers were able to successfully evade these tools on multiple occasions. This highlights the importance of training users regardless of the security tools in place, as it is critical for users to be able to identify and report phishing attempts. Regrettably, **training too may not be enough**, and then rapid detection and response becomes critical. Thanks to stakeholder reporting, the MTS-ISAC community was able to see firsthand what a phishing attack timeline can look like. In one case, the time from a user's click, which led to the account being compromised, to the adversary's first login attempt with the user's credentials was less than three minutes. Fortunately, **layered security controls allowed the organization to halt the attack** before the organization was negatively impacted.

Emotet Campaigns Plague the MTS in the Second Half of 2020

From July through December, emails with Emotet malware, a trojan that is sometimes used as a precursor for ransomware, were used to actively target MTS stakeholders. These emails, which included an **embedded link or a password protected zip file**, were **sent from compromised, trusted third parties'** infrastructures. Because these emails were sent from compromised infrastructure, attackers were able to leverage legitimate email threads, including referring to current projects. Again, user diligence to identify suspicious emails along with a clear understanding of how to report them to the security team were critical to mitigating risk and raising community awareness.

In some cases, multiple MTS stakeholders reported receiving Emotet emails from the same compromised organization. However, most often, **Emotet emails were sent to localized distribution lists using legitimate email threads**. In response to these localized Emotet campaigns, the MTS-ISAC spent the fourth quarter of 2020 preparing to launch **information exchange communities** with MTS stakeholders. Several of these communities are **operationalizing in early 2021**, which will enable MTS critical infrastructure stakeholders to **improve their cyber risk management posture by exchanging information locally with trusted entities while connecting globally through the MTS-ISAC**.

"Priority alerts and the requests for information generated by MTS peers provided us early situational awareness of relevant threat activity."

John Crochet,
Director of Information Technology,
Port Fourchon

Adversaries Scanned with Intent

Adversary interest in Remote Desktop Protocol, Secure Shell, and other services trended high across 2020. MTS stakeholders saw near constant scanning of public-facing infrastructure for vulnerabilities, including **searching networks for vulnerable cameras, Voice-over IP phones, RFID, IT infrastructure, and Internet of Things (IoT) and Industrial IoT devices**. Whenever public facing infrastructure vulnerabilities were not patched, it was targeted. As soon as the SolarWinds breach announcement was made in mid-December, MTS stakeholders began reporting IP addresses targeting port 17777, used by **SolarWinds Orion**.

Last hop IP address geolocations associated with MTS scanning trended differently across the year. However, logs showed malicious traffic consistently coming from universities, academic institutions, and research organizations regularly targeting MTS stakeholders. Also, search engine spiders attempted to crawl MTS infrastructure to discover vulnerabilities and unpatched systems.

"MTS-ISAC provided blocklists that have contributed to a steady, and significant, reduction of failed login attempts."

Chris Carter, Information Security Analyst,
Port of Vancouver USA

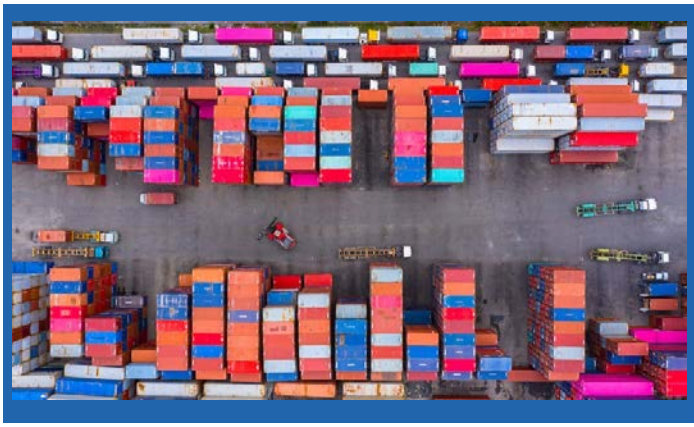
Targeting of the Remote Workforce

The COVID-19 pandemic forced MTS stakeholders to quickly respond with solutions to support critical business operations while protecting essential workers. Similar to other industries, multiple organizations in the maritime sector had to almost overnight transform to support elements of their workforce working remotely. And similar to other industries, this quickly drew interest from adversaries.

As many organizations quickly implemented tools to support remote workers, adversaries began focusing their attacks on those tools. From May to June, O365 credential stuffing attacks increased by 66%. July, August, and September logged another 29% increase from the June high. However, the fourth quarter's failed login attempts dropped to align with early 2020 numbers and stayed low. This may have been due to a lack of success in the credential stuffing campaigns, perhaps due to organizations increasingly implementing two-factor authentication (2FA) during

the year to counter these login attempts and the increased use of virtual private networks (VPNs) to support remote workers.

Late in the third quarter, stakeholders reported a noticeable increase in VPN hacking attempts. Of interest, logs provided to the MTS-ISAC showed that in some cases, the VPN activity correlated with previously reported Sodinokibi ransomware indicators. Furthermore, analysis of multiple logs shared with the MTS-ISAC identified additional common IP addresses being used to target VPN services.



"Automated sharing and consumption of high quality and relevant indicators into security monitoring and detection products are game changers for maritime transportation system stakeholders."

Ralph Yost,
Cybersecurity Director, Tideworks

Focusing on Information Exchange

Collaboration and information exchange through the MTS-ISAC took both traditional and unexpected paths in 2020. While MTS stakeholders were encouraged to share a variety of information, including phishing emails, security logs, reports, alerts, and advisories, they also **shared best practices and information regarding sightings of activity and indicators**, which provided the community greater visibility into the scope of an attack. Requests for information, issued to better understand when new or unusual activity was targeting the MTS and other industries, was viewed as a valuable source of information.

"As the Port Authority of New York and New Jersey, we have a long-standing commitment to safety and security which is now bolstered by our collaboration with the MTS-ISAC to create an information exchange for all of our stakeholders."

Michael Edgerton, Port Security Manager, Port Authority of New York and New Jersey

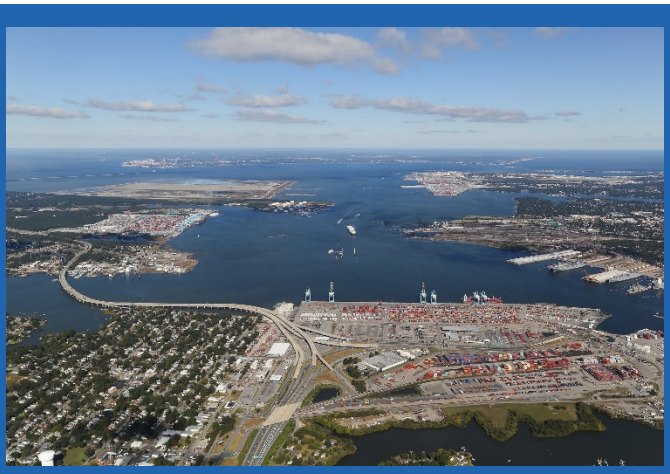
Information exchange, supported by **a community-of-communities approach**, was conceived of at the inception of the MTS-ISAC. Adversary campaigns, especially those that successfully focused on breaching trusted third-parties and then pivoting attacks within a trusted ecosystem, became the springboard for the creation of regional or interest-specific communities within the MTS-ISAC umbrella. Regional **communities not only provided a valuable source of actionable intelligence, but they helped speed the adoption of best practices and improved coordinated responsiveness** through exercises. By the end of 2020, multiple communities were taking form.

Helping Build the Community

In 2020, the MTS-ISAC provided a number of no cost training opportunities for MTS stakeholders. Webinars, supported by subject matter experts and held on popular topics like "Protecting GPS", "Insider Threats", "Maritime Cyber Insurance", "The Human Side of Cyber", "Managing Risk While Addressing Coast Guard NVIC 01-20 and MTSA Requirements", "IMO 2021 and Information Sharing for Small Fleets", and others, attracted participation from private and public sector stakeholders alike. During webinars, attendees had the opportunity to interact both with the presenters and each other, which provided more opportunities for lively interaction during a year that limited many in-person opportunities to interact. Building on the series of webinars, the MTS-ISAC sponsored and actively participated in the 2nd annual Maritime Cybersecurity Summit, which provided an opportunity to collaborate with both vendors and experts.

"Over the past few years, our port has become proficient at protecting GPS signals. We were happy to share our subject matter expertise – all those lessons we learned, with the MTS-ISAC's community of trusted stakeholders."

Randy Plotkin,
Information Security Manager,
Virginia Port Authority



The MTS-ISAC also supported the information sharing efforts of multiple other organizations, including InfraGard and Area Maritime Security Committee calls. Thought leadership was provided by contributing articles of interest to industry trades and speaking on a wide variety of contemporary maritime topics and cybersecurity trends. The MTS-ISAC also helped improve situational awareness for the broader community by expanding its TLP: GREEN distribution list to include multiple Sector Area Maritime Security Committees to provide them with MTS-ISAC advisories.

Helping to advance stakeholder collaboration efforts, the **MTS-ISAC led a cybersecurity tabletop exercise** for the Port of Mobile and several of its public and private sector stakeholders. The exercise scenario brought together real-world examples of physical and cyber security incidents that have occurred in the maritime sector. This allowed stakeholders to discuss the complex response challenges associated with physical-cyber hybrid events. In addition, the MTS-ISAC supported the U.S. Coast Guard District 8's tabletop exercise as well as Sector New Orleans' exercise.

"Exercises are an essential tool in our box. They provide an opportunity for us to work with port partners and sharpen our responses to unexpected and unfavorable conditions."

Brett Valentz,
IT & Network Infrastructure Manager,
Alabama State Port Authority

The MTS-ISAC added two valuable service provider partners. Perch Security partnered as a co-managed threat detection and response platform backed by an in-house Security Operations Center (SOC). HudsonCyber partnered to offer the community an enterprise technology solution that monitors fleet and shore-based environments for cybersecurity vulnerabilities and emergent cyber threats. These additions strengthened the arsenal of cybersecurity services for MTS stakeholders who aim to prevent deliberate and non-targeted cyber-attacks from infecting and damaging technologies and operating systems.

Looking to help better prepare the workforce of the future, the MTS-ISAC engaged with Tiffin University's Center for Cyber Defense and Forensics. Students were provided hands-on research opportunities to conduct analysis, identify trends, and better understand adversary activities that they will be challenged with defending against after graduation.

MTS-ISAC Cybersecurity Advisories

The MTS-ISAC created and shared **62 cybersecurity advisories** across 2020. Each advisory consisted of a high-level overview of what happened, a section with threat indicators that a cybersecurity team could use to take action, followed by recommendations for consideration. Content for advisories was created directly **from cyber threat information shared to the MTS-ISAC by critical infrastructure stakeholders**. While some advisories documented trends observed over a short period of time, most were issued quickly to alert the MTS of active and potentially harmful activity.

"We are a committed partner of the MTS-ISAC; committed to community-based information exchange to reduce cyber risk at our port and help protect other MTS critical infrastructure stakeholders."

Davin Garcia,
Information Technology Manager,
Port of Stockton

Evolving Requirements

Both vessel and shoreside cybersecurity efforts will be under increasing scrutiny starting in 2021. The International Maritime Organization (IMO) had a deadline of January 1, 2021 for *Maritime Cyber Risk Management* to be addressed in Safety Management Systems. To help Port State Control Officers and marine Inspectors be better prepared for IMO 2021, the U.S. Coast Guard released their Vessel Cyber Risk Management Work Instruction on October 27, 2020. This document provides guidance on how commercial vessels will be assessed to ensure they are cyber safe and secure.

Meanwhile, *Navigation and Vessel Inspection Circular (NVIC) 01-20* provided industry with information that the U.S. Coast Guard will be inspecting Maritime Transportation Security Act of 2002 regulated facilities for cyber risk management efforts for the first time starting with annual inspections occurring on or after October 1, 2021. Both of these organizational efforts have signaled to maritime stakeholders that cybersecurity is a priority that must be addressed to ensure safe and secure MTS operations, regardless of whether those operations are occurring shoreside, on an offshore platform, or onboard vessels.

In addition to IMO 2021 and NVIC 01-20, other cybersecurity guidelines, policies, and strategies that maritime stakeholders may want to better understand include:

- The European Union Agency for Cybersecurity (ENISA) released their *Cyber Risk Management for Ports* report on December 17, 2020. The report introduced a four-phase approach for cyber risk management that follows common risk management principles that aligns with the International Ship and Port Facility Security (ISPS) Code.
- BIMCO released *The Guidelines on Cyber Security Onboard Ships (Version 4)* on December 23, 2020. The MTS-ISAC helped provide updates to these guidelines, which outline practices for awareness, protecting shipboard equipment and data, communications security, and cyber incident response plans.
- The International Association of Classification Societies continues its work in support of the IMO and is also developing guidance in support of cybersecurity resilience efforts.
- In December 2020, the *National Maritime Cybersecurity Plan* was approved by the White House, which outlined 10 priority actions focused around: risks and standards; information and intelligence sharing; and creation of a maritime cybersecurity workforce.
- Updates were made through the National Defense Authorization Act to Title 46 of the U.S. Code authorizing the U.S. Coast Guard to prevent or respond to cyber incidents.

"Through our MTS-ISAC participation, we gained visibility to current, real-word examples of cyber threats targeting MTS stakeholders."

Naoki Saito, General Manager of Maritime Education and Training Certification, ClassNK

Looking Ahead

The MTS-ISAC leverages a community-of-communities approach, which enables stakeholders to work more effectively locally while being tied into the global maritime community. These communities have formed around a specific area of interest the stakeholders have and are based around, for example:

- Port areas;
- Types of vessel operations (e.g. container, cruise, bulk); or
- Industry groups.

These communities formed organically over the history of the maritime sector because they have common operational interests. In 2021, several **communities are taking form under the MTS-ISAC** umbrella. This is an incredibly **cost-effective nonprofit option** for communities **to share cyber threat information** more broadly in comparison to other sector offerings.

When organizations and communities share cybersecurity information anonymously with each other, while also having visibility into what may be occurring across the maritime sector, the individual community becomes more resilient, which also benefits the rest of the MTS. **Because information is shared anonymously, individual stakeholders can maintain their competitive advantages while still addressing the common threats to the sector.** As the MTS is ultimately a system of system with operational upstream and downstream interdependencies, this collaborative approach of the MTS is a key to success for maritime stakeholders moving forward as the integration of networked IT, OT, and IIoT systems in the maritime space continues to rapidly expand. As our collective understanding improves following both physical and cyber incidents, we see that **competitive advantages are best realized within a more resilient maritime sector** rather than when the system feels the shock of a negative chain-reaction. Information about threats that can negatively impact the resilience and business of the maritime sector are no longer a "competitive advantage" when the resulting consequences impact all stakeholders, not just competitors.

"We, at JAXPORT, are dedicated to solving 21st century problems with 21st century solutions. A dedicated community of vetted, interested stakeholders is a critical 21st century solution to the ever-evolving possibilities and problems of an ever-increasingly, always-connected society."

Frederick Wessling, Director Information Technology, Jacksonville Port Authority (JAXPORT)

When the MTS-ISAC formed in 2020, the Board of Directors understood there were multiple priorities to make the MTS-ISAC operational. Most of those were tackled early on and highly effective, as shown in the previous sections of this report. Now, due to rapid expansion of the MTS-ISAC, we are researching additional options for a threat intelligence platform that may better support the community of stakeholders. This transition and integration have been planned for the first half of the year.

Lastly, the MTS-ISAC is working to ensure a broader set of maritime stakeholders are aware of the benefits of engaging with their peers on cybersecurity efforts. The unique structure of the MTS-ISAC benefits stakeholders in ways that local, national, and regional efforts cannot. **We'll continue working to connect stakeholders in new and innovative ways to share actionable cyber information and reinforce best practice implementation.**

We look forward for what the future holds as we help build the maritime cybersecurity community!

Helping Build the Maritime Cybersecurity Community