

COMBATING

CYBER-

BY SEAN M. HOLT, M.B.A.



MARITIME

ATTACKS

"We're in a world today where it's not enough to be secure. You have to prove you're secure."

- Chris Krebs, Former Director of the Cybersecurity and Infrastructure Security Agency

On September 11, cyberattacks on Caesars Entertainment and MGM Resorts attracted worldwide attention. The companies' global operations, share prices – and possibly credit ratings – were severely impacted.

The method of attack against MGM: ransomware-as-a-service (RaaS) made by ALPHV, or BlackCat, and social engineering by impersonating an employee they found on LinkedIn in a call known as “vishing” (“voice” plus “phishing”) to MGM’s IT help desk. Vishing gained attackers login credentials or a one-time password to bypass multifactor authentication and enter the system.

After three days of being paralyzed, Caesars purportedly shelled out \$15 million to the hacking group Scattered Spider, also known as Roasted Oktapus or UNC3944.

The method of attack against MGM: ransomware-as-a-service (RaaS) made by ALPHV, or BlackCat, and social engineering by impersonating an employee they found on LinkedIn in a call known as “vishing” (“voice” plus “phishing”) to MGM’s IT help desk. Vishing gained attackers login credentials or a one-time password to bypass multifactor authentication and enter the system.

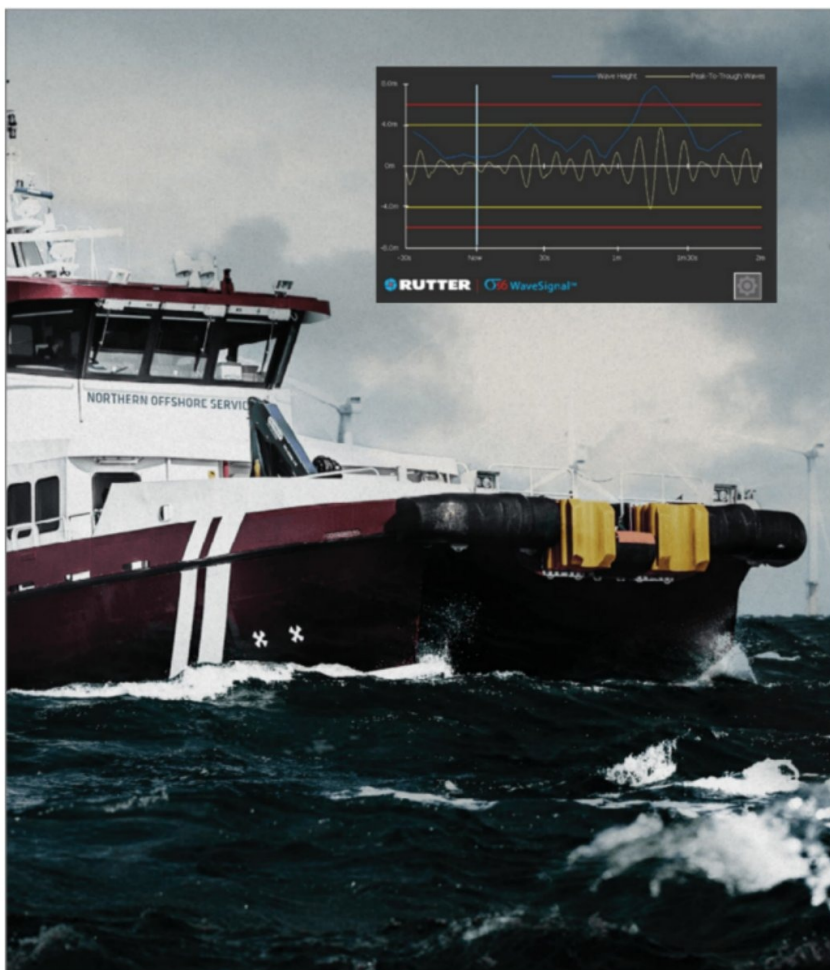
To help defend against the dark arts, we caught up with industry and government leaders to gain cybersecurity insights.

CYBERCRIMINALS ARE WINNING

“The cybercriminals are winning,” says Brian Foremny, Chairman of Fort Lauderdale-based SECNAP Network Security. “In 2015, the total worldwide global ransomware damages were \$325 million. By 2017, it grew to \$5 billion. By 2021, it was in the \$20 billion range.”

With the current global annual spend on cybersecurity at approximately \$150 billion, the *Wall Street Journal* projects it will reach \$265 billion by 2031. “The problem isn’t from a technical standpoint,” Foremny explains, “it’s that effective solutions haven’t been affordable by anyone other than the Fortune 1000/Global 2000 companies. Large enterprises, with notable exceptions, rarely get hacked. Small- to mid-market enterprises (SME) become easy targets by not deploying a complete security solution.”

SECNAP, having been in business since 2001, has recently entered the maritime space with its CloudJacketXi product and is on a mission to help underserved SMEs



Rutter has partnered with Ørsted to improve the safe transfer of personnel to offshore wind turbines using Rutter’s radar wave prediction technology, sigma S6 WaveSignal™.

Ørsted will be deploying WaveSignal™ to crew transfer vessels within their contracted fleet!

For more information, visit:

www.rutter.ca/wavesignal-ctv

for less than a pumpkin-spiced latte a day. Foremny says criminal organizations such as ALPHV lease or license RaaS to smaller, less sophisticated gangs that become affiliates and share the bounty.

To address the growing threat, U.S. Presidential Executive Order (EO) 14028 was issued in May 2021 to address specific technologies and practices for government agencies, critical infrastructure and private companies. Foremny says when the EO was published, most ransomware deployed by gangs targeted endpoints like laptops and mobile devices. Now, sophisticated malware creators and developers have created a new generation of malware that is not detectable by endpoint detection and response (EDR).

“The crown jewels of companies don’t reside on laptops,” he adds. “They’re kept on servers or cloud networks.” Such evolving attack vectors force cybersecurity providers, like SECNAP, to constantly remain ahead of threats.

GUARDING AGAINST THREATS

In an exclusive interview, U.S. Coast Guard Rear Admiral

BRAKING SOLUTIONS

FOR THE MARINE INDUSTRY

Suction Dredger | Main Propulsion | Bow Thruster
 Diesel Pump | Fan Drive | Marine Pump
 Marine Propulsion | Pump Drive | Compressor Drive

**HILLIARD
BRAKE
SYSTEMS**

HILLIARDBRAKESYSTEMS.COM

OPTICAL BEARING DEVICE

With our Optical Bearing Device, the Navigation Officer can determine the ship’s position, independently of the GPS and detect spoofing or jamming to the GPS system



Hanging Version
Pull-Down from Deck-Head

Type Approved;

Meets the requirements of SOLAS V/19.5.3 for Gyro-Compass Bearing Repeater



Approved Body No.:
0575



Approved Body No.:
0097



www.scansys.no

Email: sales@scansys.no

Oslo, Norway: +47 6681 2740
 Fort Lauderdale, USA: +1 954 583 5700
 London, UK: +44 20 8550 6458

Rather than focus on a few specific threats, he says the marine industry can protect our nation's critical infrastructure by implementing systems and processes that prevent and respond to various cyber threats.

Wayne Arguin, Assistant Commandant for Prevention Policy, points out how increased reliance on digital systems has triggered a rise in cyberattacks: "Digital systems help make the marine transportation system the most economical, efficient, environmentally friendly way to transport products worldwide. These same digital systems also create complicated interdependencies, vulnerabilities and risks, and their prevalence in the industry is only growing."

He explains the Coast Guard's role in all of this: "By working closely with the National Security Council, intelligence community, partner agencies and foreign partners, the Coast Guard can best understand threats from state-sponsored and downstream cyber actors. We help the maritime community reduce vulnerabilities and mitigate consequences. Whether state-sponsored or not, the same practices that defend against all potential cyber adversaries – access control, multifactor authentication, network segmentation and incident response planning – help defend against threats."



PERSONNEL PARTICIPATING IN THE CYBER COMPONENT COMMANDERS' CONFERENCE LISTEN TO LT. CMDR. TODD BATTEN ON THE BRIDGE OF COAST GUARD CUTTER LEGARE.

He says the most pressing cyber threats can lead to a long-term disruption of the marine transportation system: "Ransomware remains a major risk for the maritime community. Even if ransomware does not directly impact an operational technology system, a loss of ability to

tication, network segmentation and incident response planning – help defend against threats."

• NEW COMPACT SEWAGE TREATMENT
• PROVEN TECHNOLOGY
• COAST GUARD CERTIFIED
• CONVENIENT OVERBOARD DISCHARGE
• RELIABLE OPERATION

HEADHUNTER

WWW.HEADHUNTERINC.COM

PHONE: +1-954-581-6996 3380 SW 11TH AVENUE FORT LAUDERDALE, FLORIDA 33315 HEADMASTER@HEADHUNTERINC.COM

Made in USA

manage business operations could have cascading impacts on the supply chain.”

Rather than focus on a few specific threats, he says the marine industry can protect our nation’s critical infrastructure by implementing systems and processes that prevent and respond to various cyber threats.

“Following best practices, reporting incidents to the Coast Guard’s National Response Center, and sharing information with their local Area Maritime Security Committees are key actions that protect our Marine Transportation System,” he advises. “The Coast Guard has significantly increased our capability, and our Cyber Protection Teams can support the maritime community before or after an incident with vulnerability assessments, on-network threat hunting and post-incident response.”

He notes that “The Cyber Protection Team’s cyber skills are unprecedented for the Coast Guard. The Coast Guard also established maritime-focused cyber specialists in every Captain of the Port Zone. They are civilian employees serving as the focal point for port-level cyber coordination across industry and government. During compliance inspections, many companies have indicated they would like more details on conducting vulnerability assessments and accounting for them in their plans. Based on this feedback, the Coast Guard released its *Maritime Cyber Assessment and Annex Guide* to aid the industry in its efforts to harden their networks.”

In addition, he points out that “The United States is a member state of the IMO and works closely to address cyber risks in the shipping industry. For example, the IMO released guidelines for addressing maritime cyber risk management in a vessel’s Safety Management

“Cyber threats are not going away. For maritime stakeholders, cybersecurity must be a part of company culture. A great way to help build that culture is implementing CISA’s Cross Sector Cybersecurity Performance Goals.”

System (SMS). More recently, the IMO is undertaking an effort to revise its Guidelines on Maritime Cyber Risk Management and identify the next steps to enhance maritime cybersecurity. One example is the Cybersecurity and Infrastructure Security Agency’s (CISA) Cross Sector Cybersecurity Performance Goals. These are not

CLOUDJACKET

**COMPREHENSIVE
CYBERSECURITY
PLATFORM**

Providing enterprise-grade protection against malware, ransomware, data breaches, unauthorized access, and other sophisticated attack vectors, at a cost accessible to the maritime sector.

XDR+EDR+SIEM+MDR+NDR+24/7 SOC

Amidst rapid digital transformation, the significance of cybersecurity has escalated for the maritime and offshore industries. This shift has introduced novel threats and brought forth a plethora of regulatory requirements, underscoring the imperative for robust security measures in these sectors.

SECNAP
NETWORK SECURITY

www.SECNAP.com | sales@SECNAP.com | 844.638.7328

Reinforcing the recent MGM cyberattacks, Bhalotra adds, “We see more and more attacks against senior executives, particularly ones that approve financial transactions. They’re very visible on social media and give keynote speeches at conferences” – thus opening the door for similar social engineering cyberattacks.

regulatory mandates but a comprehensive set of cyber protections that clearly define and address the common and impactful cyber risks. Effective implementation of these protections greatly decreases the vulnerabilities seen during Cyber Protection Team assessments.

“Cyber threats are not going away. For maritime stakeholders, cybersecurity must be a part of company culture. A great way to help build that culture is implementing CISA’s Cross Sector Cybersecurity Performance Goals.”

CYBERATTACKS & REPORTING REQUIREMENTS


Back in April, ABS Wavesight, a software-as-a-service (SaaS) company, and ActZero, a managed detection and response (MDR) provider, allied to deliver cybersecurity solutions to the global fleet. Paul Sells, CEO of ABS Wavesight, says, “The proliferation of connectivity and



U.S. ARMY GEN. PAUL NAKASONE (MIDDLE) AND COAST GUARD CAPT. KEVIN CARROLL (RIGHT) PARTICIPATING IN THE CYBER COMPONENT COMMANDERS’ CONFERENCE.


expansion of the digital landscape in shipping increases our reliance on tools to help run business aboard ships.”

Sameer Bhalotra, Co-founder & CEO of ActZero, who was former Senior Director for Cybersecurity on the National Security Council and currently is a member of the U.S. Secret Service Cyber Investigations Advisory Board, states that “Organized crime groups around the world




CIMOLAI Technology spa
Special Equipment


info@cimolai.tech
www.cimolaithechnology.com




Mobile Boat Hoists




Ship Lifting Platforms “Cimolift”



Portal Cranes



Transfer Systems



AN ALTERNATIVE BALLAST WATER TREATMENT SYSTEM

- NO FILTERS
 - TREAT AT SEA
 - CONTROL COMPLIANCE

InTank® = InVoyage™ + InControl™



NEW InTank®FITT® = 0.5m² footprint!



- **FILTERLESS.**
Treat and neutralize at sea = operational and compliance benefits.
- **UNIQUE.**
InTank allows the rapid semi-sub flood and drain operation without treatment.
- **INSTALLED.**
Handy to Cape, MR to VLCC, semi-sub rigs & vessels.



www.intankballast.com intank@sciencofast.com

have gotten really good at launching cyberattacks that render computers unusable. You can't log into your email. You can't communicate with your employees. You can't talk to your customers. You can't talk to your ships and your fleet. You can't do banking, make payments, or make payroll. All your computer networks are just frozen. These big, organized, current groups are very sophisticated businesses. They're not like a teenager in their basement hacking. They have finance departments, recruiting, payroll twice a month and support for their people to launder the money."

Reinforcing the recent MGM cyberattacks, Bhalotra adds, "We see more and more attacks against senior executives, particularly ones that approve financial transactions. They're very visible on social media and give keynote speeches at conferences" – thus opening the door for similar social engineering cyberattacks.

Bhalotra provides maritime cyberattack examples: "In 2021, a big Japanese shipping company had two breaches in the same year. The largest took ten days to contain and recover. When they couldn't manage their fleet, it was a huge loss. In



MOORING & TOWING SOLUTIONS



Towing Pins

OCIMF Roller Fairleads

Guide Sheaves

Shark Jaws

Balanced Head Fairleads

Smith Berger Marine, Inc.

7915 10th Ave. S., Seattle, WA 98108 USA
 Tel. 206.764.4650 - Toll Free 888.726.1688 - Fax 206.764.4653
 E-mail: sales@smithberger.com - Web: www.smithberger.com

In September, ActZero was named “Partner of the Year for the Americas” by famed cybersecurity technology company CrowdStrike. “We use A.I. and highly trained specialists in our three global operations centers to identify and block attacks in milliseconds,” Bhalotra notes.

June of the same year, a South Korean shipping company was hacked. A few months later, a big containership company lost all its customer data. In November 2021, both a Singapore and Greek company lost confidential

information including proprietary data on their customers. Whether it’s state-sponsored groups trying to steal government secrets and stop critical infrastructure in preparation for war or organized crime trying to make money off the dark web, it’s really bad. The U.S. Secret Service is paying big money for information trying to find these hackers because they’re killing businesses.”

In September, ActZero was named “Partner of the Year for the Americas” by famed cybersecurity technology company CrowdStrike. “We use A.I. and highly trained specialists in our three global operations centers to identify and block attacks in milliseconds,” Bhalotra notes. He stresses the significance of investing in cyber defense as “small businesses are very susceptible to the loss of annual profits from just a one-shot cyberattack.”

Bhalotra concludes by advising: “When choosing a security information and event management (SIM) solution – which will hook up to every node, switch, firewall, endpoint, host, device and system to log and analyze billions of pieces of information – trust with the solution or partner is paramount. Furthermore, many governments, including the U.S., require disclosure of breaches [as noted by MGM’s recent U.S. Securities & Exchange Commission K-8 filing]. Companies must disclose what happened, who’s affected, and how to fix it. We now even see insurance companies requiring coverage.”

BATTEN DOWN THE CYBER HATCHES

Given maritime’s increased reliance on digital systems, evolving cyber risks are here to stay. The days of shrugging off cybersecurity threats due to illiteracy or intimidation are over. Don’t give up the ship!

MarEx

SEAN HOLT writes from Singapore.

MED MARINE

VOLTRA[®]
BATTERY ELECTRIC TUG

ROBERT ALLAN

VOLTRA[®] 2100

VOLTRA[®] 2300

VOLTRA[®] 2500

VOLTRA[®] 2800

VOLTRA[®] 3000

medmarine.com.tr