WEBCAST | February 23, 2023
Sponsored by
Applied Risk
a DNV company
A Blueprint for Building Sustainable OT Cybersecurity Programs
REGISTER NOW
SECURITYWEEK
CYBERSECURITY NEWS, INSIGHTS & ANALYSIS

MALWARE & THREATS

Ransomware Attack on DNV Ship Management Software Impacts 1,000 Vessels

Norway-based DNV said a ransomware attack on its ship management software impacted 1,000 vessels.

By Eduard Kovacs
January 18, 2023

Norway-based industrial risk management and assurance solutions provider DNV said a recent ransomware attack on its ship management software impacted 1,000 vessels.

TRENDING

The Effect of Cybersecurity Layoffs on Cybersecurity Recruitment

Zendesk Hacked After Employees Fall for Phishing Attack

Russia-Linked APT29 Uses New Malware in Embassy Attacks

Microsoft Urges Customers to Patch Exchange Servers

Cyberattacks Target Websites of German

impacted 1,000 vessels.

DNV revealed on January 9 that its ShipManager software was targeted in a cyberattack on January 7, which forced the company to shut down associated servers.

In an update shared on January 17, the company clarified that it was targeted in a ransomware attack that impacted 70 of its customers and roughly 1,000 vessels.

“There are no indications that any other software or data by DNV is affected. The server outage does not impact any other DNV services,” DNV said in a press release.

It’s unclear which ransomware group is behind the attack and whether any data has been stolen. SecurityWeek has checked the websites of several major groups, but found no mention of DNV. However, threat actors typically name victims and threaten to leak stolen data only after initial negotiations have failed.

[Read: The Vulnerable Maritime Supply Chain – a Threat to the Global

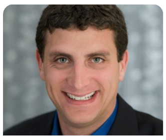
Cyberattacks Target Websites of German Airports, Admin

Critical Vulnerability Impacts Over 120 Lexmark Printers

Meta Awards $27,000 Bounty for 2FA Bypass Vulnerability

US Infiltrates Big Ransomware Gang: ‘We Hacked the Hackers’

EXPERT INSIGHTS



Dealing With the Carcinization of Security

Economy]

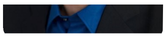
DNV provides a wide range of services for the maritime, power, oil and gas, automotive and aerospace, food and beverage, and the healthcare industries. The company's ShipManager software for the maritime industry is designed for ship management operations and ship design.

DNV says on its website that 300 shipping companies worldwide use its maritime software for more than 6,000 vessels.

SecurityWeek talked to several experts last year about cybersecurity in the maritime industry, including attack vectors, the potential effects of maritime supply chain damage, threat scenarios, attacker motivations, and what the industry should do to address existing problems.

Related: Maritime Cybersecurity: Securing Assets at Sea

Related: US Releases Cybersecurity Plan for Maritime Sector



Security

Varied viewpoints as related security concepts take on similar traits create substantial confusion among security teams trying to evaluate and purchase security technologies.

Marc Solomon

Stop, Collaborate and Listen: Disrupting Cybercrime Networks Requires Private-Public Cooperation and Information Sharing

No one combatting cybercrime knows everything, but everyone in the battle has some intelligence to contribute to the larger knowledge base.

Derek Manky

How the Atomized Network Changed Enterprise Protection

Our networks have become atomized which, for starters, means they're highly dispersed. Not just in terms of the infrastructure – legacy, on-premises, hybrid, multi-cloud, and edge.

Matt Wilson

Mapping Threat Intelligence to the NIST Compliance Framework Part 2

How threat intelligence is critical when justifying budget for GRC personnel, and for threat intelligence, incident response, security operations and CISO buyers.

Landon Winkelvoss

Password Dependency: How to Break the Cycle

Related: UN Maritime Agency Hit by 'Sophisticated Cyberattack'

WRITTEN BY

Eduard Kovacs

Eduard Kovacs (@EduardKovacs) is a contributing editor at SecurityWeek. He worked as a high school IT teacher for two years before starting a career in journalism as Softpedia's security news reporter. Eduard holds a bachelor's degree in industrial informatics and a master's degree in computer

LATEST NEWS

- Zendesk Hacked After Employees Fall for Phishing Attack
- Malicious Prompt Engineering With ChatGPT
- Cyberattacks Target Websites of German Airports, Admin
- GoTo Says Hackers Stole Encrypted Backups, MFA Settings
- NSA Publishes Security Guidance for Organizations Transitioning to IPv6

techniques applied in electrical engineering.

More from Eduard Kovacs

- High-Severity Privilege Escalation Vulnerability Patched in VMware Workstation
- GoAnywhere MFT Users Warned of Zero-Day Exploit
- UK Car Retailer Arnold Clark Hit by Ransomware
- EV Charging Management System Vulnerabilities Allow Disruption, Energy Theft
- Unpatched Econolite Traffic Controller Vulnerabilities Allow Remote Hacking
- Google Fi Data Breach Reportedly Led to SIM Swapping
- Microsoft’s Verified Publisher Status Abused in Email Theft Campaign
- British Retailer JD Sports Discloses Data Breach Affecting 10 Million Customers

Latest News

- Cyber Insights 2023: Venture Capital
- Atlassian Warns of Critical Jira Service Management Vulnerability
- High-Severity Privilege Escalation Vulnerability Patched in VMware Workstation
- Exploitation of Oracle E-Business Suite Vulnerability Starts After PoC Publication
- China Says It’s Looking Into Report of Spy Balloon Over US
- GoAnywhere MFT Users Warned of Zero-Day Exploit
- Google Shells Out $600,000 for OSS-Fuzz Project Integrations

- F5 BIG-IP Vulnerability Can Lead to DoS, Code Execution

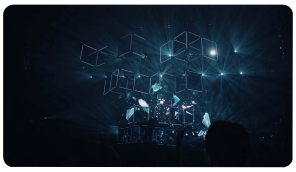
Related Content

Industry Reactions to Hive Ransomware Takedown: Feedback Friday

Eduard Kovacs

US Infiltrates Big Ransomware Gang: 'We Hacked the Hackers'

Associated Press



Microsoft Office to Block XLL Add-ins From Internet

Ionut Arghire

THIS HIDDEN SITE HAS BEEN SEIZED

The Federal Bureau of Investigation seized this site as part of a coordinated law enforcement action taken against Hive Ransomware.

This action has been taken in coordination with the United States Attorney's Office for the Middle District of Florida and the Computer Crime and Intellectual Property Section of the Department of Justice with substantial assistance from Europol

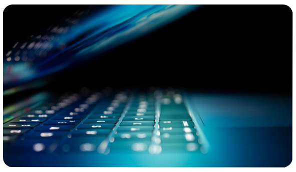
US Reiterates $10 Million Reward Offer After Disruption of Hive Ransomware

Eduard Kovacs

THIS HIDDEN SITE HAS BEEN SEIZED
Hive
The Federal Bureau of Investigation seized this site as part of a coordinated law enforcement action taken against Hive Ransomware
POLIZEI BADEN-WÜRTTEMBERG
EUROPOL

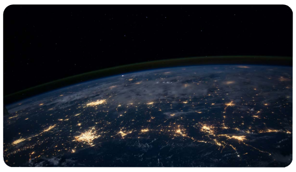
Hive Ransomware Operation Shut Down by Law Enforcement

Eduard Kovacs



US Government Agencies Warn of Malicious Use of Remote Management Software

Ionut Arghire



Chinese Hackers Adopting Open Source 'SparkRAT' Tool

Ionut Arghire

Comodo Forums Hacked via Recently Disclosed vBulletin Vulnerability

Eduard Kovacs

Popular Topics

Cybersecurity News
Industrial Cybersecurity

Security Community

Virtual Cybersecurity Events
Webcast Library
CISO Forum
ICS Cybersecurity Conference
Cybersecurity Newsletters

Stay Intouch

Cyber Weapon Discussion Group
RSS Feed
Security Intelligence Group

About SecurityWeek

Advertising
Event Sponsorships
Writing Opportunities
Feedback/Contact Us

News Tips

Got a confidential news tip? We want to hear from you.

Submit Tip

Advertising

Reach a large audience of enterprise cybersecurity professionals

Contact Us

Daily Briefing Newsletter

Subscribe to the SecurityWeek Daily

Privacy Policy