



Investigating the Security and Accessibility of Voyage Data Recorder Data using a USB attack

Authors:

Avanthika Vineetha Harish, Kimberly Tam, Kevin Jones

Presenter : [Avanthika Vineetha Harish](#)

University of Plymouth, United Kingdom

avanthika.vineethaharish@plymouth.ac.uk



Cyber-SHIP Lab
SECURING MARITIME



**UNIVERSITY OF
PLYMOUTH**





Avanthika Vineetha Harish

- Industrial Researcher at Cyber SHIP lab and a PhD candidate at the University of Plymouth, UK.
- Focused on vulnerability assessment and security testing for maritime systems.
- Masters in Cyber Security from Lancaster University, UK, with full scholarship from the British Council.
- Bachelor's degree in Computer Science and Engineering from Mahatma Gandhi University, India.



Introduction

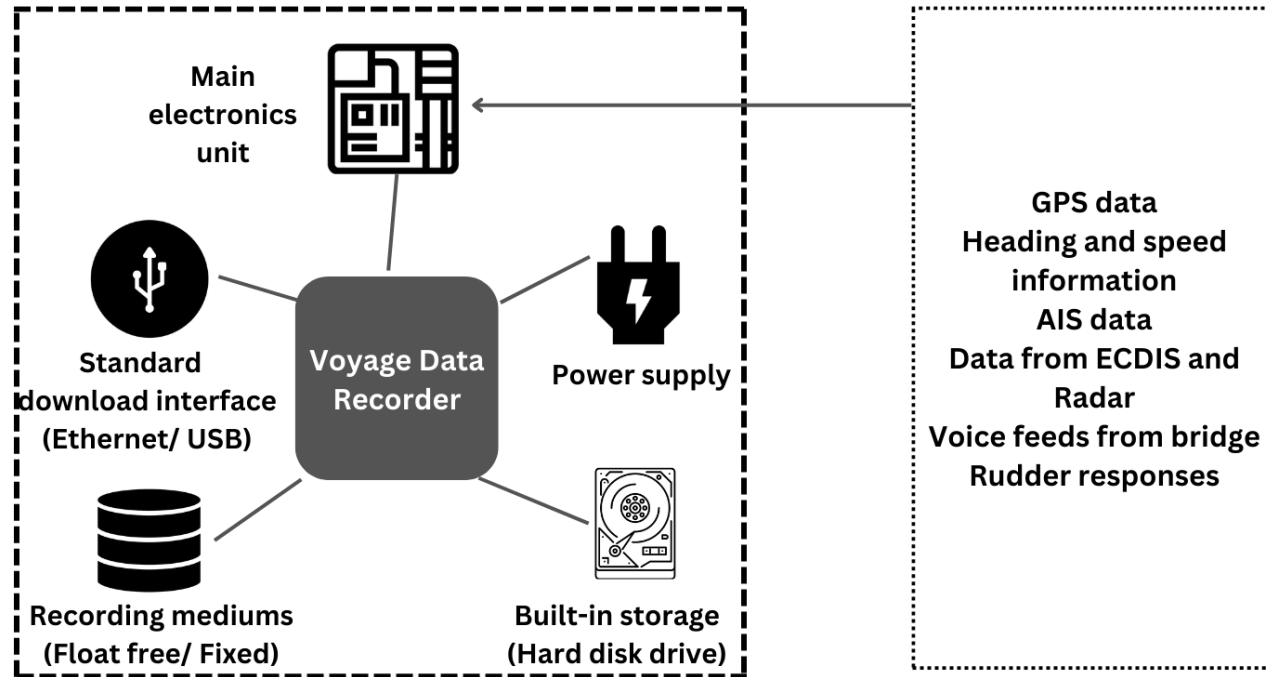
Voyage Data Recorder (VDR) - 'black box' for ships

- Critical role in accident investigations.
- Data need to be secure and tamper proof.
- Past cases where evidence data disappeared.



Background

- VDR components and features.
- International Maritime Organization regulations.
- Investigating authorities used VDRs extensively – popular cases like:
 - Sinking of El Faro [1]
 - Grounding of Costa Concordia [2]



Testing



Testing

- **Data tampering** : Manipulating accident investigation data can lead to loosen ends.
- **Testing on real hardware to see real effects.**
- **Automation of tests.**

Threat

- **Insider threat** : Critical evidence stored in VDRs are at sea for months and prone to insider access.
- According to a recent data breach report, there were 275 incidents related to data breach by privilege misuse from 2020 to 2021, and all these incidents were caused by insiders [4].

Attack Vector

- **USB** : Top cyber security attack vector, most VDRs use this port for updating, does not need much skill set.
- The number of USB threats rose to **52%** in 2022 from 37% in 2021 [3].

Aim:

- To investigate the possibility of VDR data manipulation by someone with limited technical skills and knowledge and to automate the attacks using USB device.



Tools used



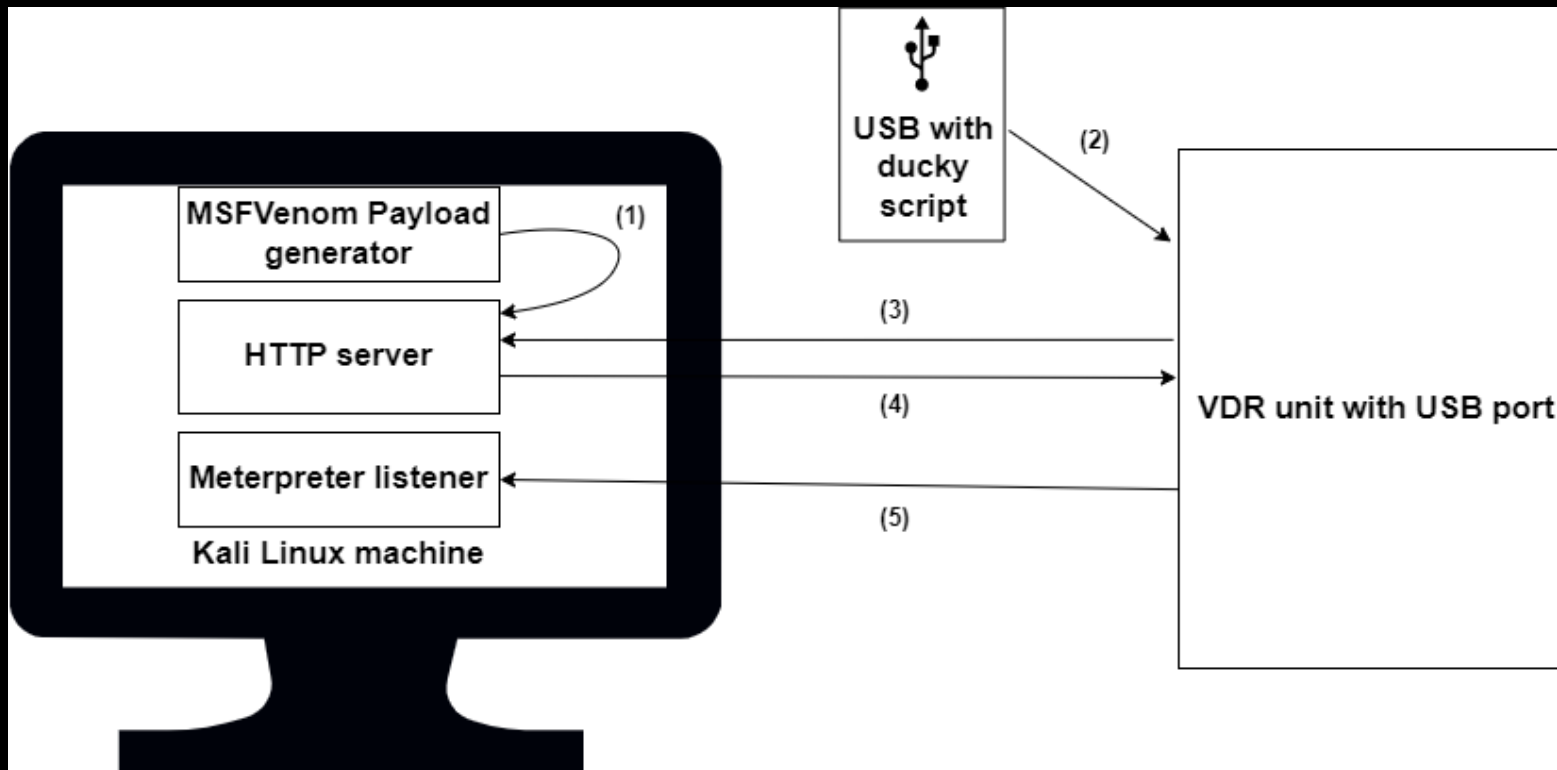
- **System Under Test** : Off-the-shelf VDR from a global shipping equipment manufacturer – taken off from a ship – with data from the year 2018.
- **USB rubber ducky** [5] : Injects keystrokes.
- **Metasploit framework** [6]: Powerful pen-testing tool
- **ShinoLocker** [7] : Ransomware simulator developed by a security researcher, Shota Shinogi, for education and training purposes.
- **Nmap** [8]: Network scanning and auditing tool

Highlights of the testing



1. Reverse shell

Interactive shell connection from target machine to attack machine



- (1) Payload generated (using Msfvenom [9]) and hosted in HTTP server
- (2) Ducky Script written with commands to download payload
- (3) Once USB blipped in, command to download payload
- (4) Payload downloaded from server to VDR PC and executed
- (5) Meterpreter listener receives connection from the VDR, and a session is opened.



Results :

- Reverse shell session obtained on the attack machine.
- VDR system running on Windows embedded standard 7 OS
- Privilege escalation.
- Retrieved 5 password hashes including that of administrator, captain and engineer accounts.
- Three blank passwords and the other two were simple ones.
- View, access and tamper files and folders.
- View, access and tamper logs and hiding the trace of manipulation.
- Affecting the **Confidentiality, Integrity** and **Availability** of data.

Suggestions:

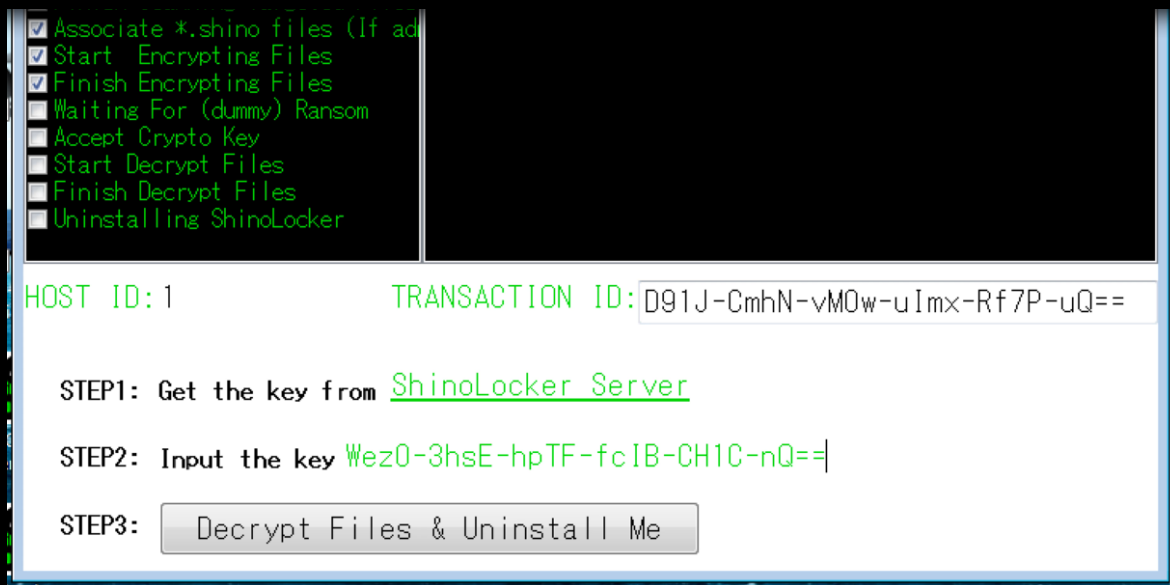
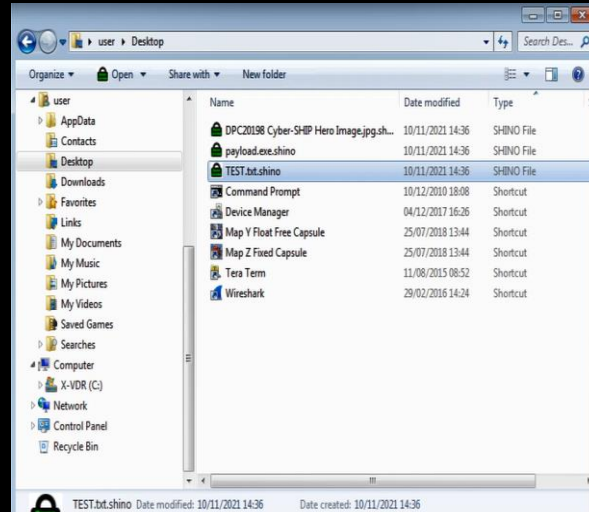
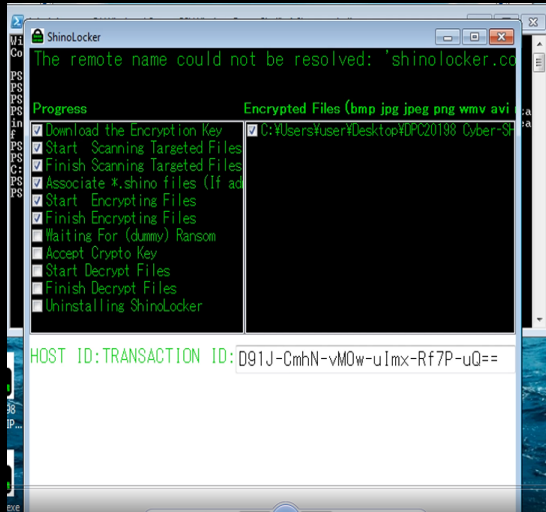
- Strong password policy as suggested by Cyber security guidelines onboard vessels document.
- Integrity checking mechanism.



2. Ransomware

- Most common cyberattack these days.
- Leading source of cybersecurity threat risk to US ports and terminals [10].
- In the last five years, four major global shipping companies (CMA CGM, APM-Maersk, MSC and COSTCO) have been negatively affected by ransomware and their operations have been halted for weeks [11].
- Recently, a Singapore-based offshore operator - Swift Pacific Offshore has reported a data breach that experts believe to be a ransomware attack [12].

Changing ransomware motives : Attack on Belarus Railway systems to release fifty 50 high-risk political prisoners in addition to banning Russian soldiers from using Belarusian trains as the ransom [13].



ShinoLocker ransomware : Tool used for training and teaching purposes; appeared to be the most practical option without causing damage to the VDR.

- Payload created for png, jpeg, ppt, txt file types.
- Ducky script was written to download the payload on to the VDR PC.
- When USB with ducky script was plugged in to the VDR system, the ransomware started encrypting the files of the previously mentioned file types.
- Affecting the **Availability** of data.



3. Hard drive erasure

- Can be accomplished by few lines of ducky scripting.
- Denial of service.
- Affecting the **Availability** of data.
- Could be catastrophic and can lead to investigation dead ends.

Enrica Lexie case: In 2012, two Indian fishermen on a fishing boat 'St. Anthony' were killed off the coast of Kerala, India in a shooting incident mistaking the fishermen as pirates and India detained two Italian mariners on board the ship 'Enrica Lexie', an oil tanker, owned by a Milan-based company. VDR was retrieved, however, captain **failed to preserve** VDR data after the incident and the second officer of 'Enrica Lexie' stated that he did not press the VDR for recording[14].



4. Eternal Blue vulnerability

- Windows 7 Embedded standard OS on VDR found to be vulnerable with Eternal Blue exploit.
- Remote code execution vulnerability in Microsoft SMBv1 Servers with vulnerability entry of **CVE-2017-0143** [12].
- CVSS (Common Vulnerability Scoring System) score of **8.1(HIGH)** and the famous WannaCry attack used this exploit to spread infection.
- The session was not opened, however, **VDR crashed** with a blue screen of death and the machine needed to be manually rebooted.
- Denial of service (Affecting the **Availability** of data and system).
- Keeping the systems up-to-date.



Discussions

Improving information security of VDR data

- Raising the standards
- Automation and sector specific tools for testing
- Best operational practices



Thank you

For any questions contact: avanthika.vineethaharish@plymouth.ac.uk

Avanthika Vineetha Harish, Industrial Researcher and PhD student,
CyberSHIP Lab, University of Plymouth, United Kingdom
For more details, visit: <https://www.plymouth.ac.uk/research/cyber-ship-lab>

References

- [1] National Transportation Safety Board, "Sinking of the US Cargo Vessel El Faro," 2015, [Online]. Available: <https://www.nts.gov/investigations/AccidentReports/Reports/SPC1801.pdf> (accessed 2022.10.21) [2] M. Piccinelli and P. Gubian, "Modern ships voyage data recorders: A forensics perspective on the Costa Concordia shipwreck," Proc. Digit. Forensic Res. Conf. DFRWS 2013 USA, pp. S41–S49, 2013, doi: 10.1016/j.diin.2013.06.005.
- [3] Honeywell, "Industrial Usb Threat Report 2021," 2021. Accessed:2022.10.21. [Online]. Available: <https://www.honeywellforge.ai/content/dam/forge/en/documents/cybersecurity/Industrial-Cybersecurity-USB-ThreatReport-2022.pdf>
- [4] G. Bassett, D. Hylender, P. Langlois, A. Pinto, and S. Widup, "DBIR Data Breach Investigations Report," 2022 [Online]. Available: <https://www.verizon.com/business/resources/reports/dbir/> (accessed 2022.10.21).
- [5] Hak5, "USB Rubber Ducky - Hak5," 2022. <https://shop.hak5.org/products/usb-rubber-ducky-deluxe> (accessed 2022.10.21).
- [6] Rapid7 Inc., "Metasploit | Penetration Testing Software, Pen Testing Security | Metasploit," Metasploit.Com, 2019. <https://www.metasploit.com/> (accessed 2022.10.21).
- [7] "ShinoLocker - The Ransomware Simulator-" <https://shinolocker.com/> (accessed 2022.10.21).
- [8] nmap.org, "Nmap: the Network Mapper - Free Security Scanner," <https://Nmap.Org/>, 2021. <https://nmap.org/> (accessed 2022.10.21).
- [9] Offensive Security, "Msfvenom - Metasploit Unleashed," 2016. <https://www.offensive-security.com/metasploitunleashed/Msfvenom/> (accessed 2022.10.21).
- [10] Jones Walker, "Ports and Terminals Cybersecurity Survey," 2022.Available:<https://sitescommunications.joneswalker.com/38/1936/landingpages/2022-cybersecurity-survey---lp.asp> (accessed 2022.10.21).
- [11] C. Cimpanu, "All four of the world's largest shipping companies have now been hit by cyber-attacks | ZDNet," ZDNet, 2020. <https://www.zdnet.com/article/all-four-of-theworlds-largest-shipping-companies-have-now-been-hit-by-cyber-attacks/> (accessed 2022.10.21).
- [12] Maritime Executive, "Ransomware Attack on Swire Pacific Offshore Breaches Personnel Data."2021. <https://www.maritime-executive.com/article/ransomwareattack-on-swire-pacific-offshore-breaches-personnel-data> (accessed 2022.10.21).
- [13] A.Greenberg,"Why the Belarus Railways Hack Marks a First for Ransomware | WIRED " 2022. <https://www.wired.com/story/belarus-railways-ransomwarehack-cyber-partisans/> (accessed 2022.10.21).
- [14] H. H. Judge Vladimir Golitsyn Judge Jin-Hyun Paik He Judge Patrick Robinson Professor Francesco Francioni Pemmaraju Sreenivasa Rao Registry, "Pca Case No. 2015-28 In The Matter Of An Arbitration-Before-An Arbitral Tribunal Constituted Under Annex Vii To The 1982 United Nations Convention On The Law Of The Sea The Italian Republic-V.- The Republic Of India-Concerning-The 'Enrica Lexie' Incident," 2020
- [15] NIST, "Nvd - Cve-2017-0144," National Vulnerability Database, 2017. <https://nvd.nist.gov/vuln/detail/CVE-2017-0144> (accessed 2022.10.21).