WAPACK LABS CYBER INTELLIGENCE SERVICE

MPS-ISAO Intelligence Strategic Partner

Tactical Intelligence Report

Serial: TR-131-2017
Report Date: 20171020
Actor Type: II
Countries: All
Industries: Maritime

VSAT and "x0rz"

In a recent cyber security report written by William Doyle and published in the Maritime Reporter magazine, Doyle interviews an internet security researcher identified as, "x0rz". x0rz provides insight into how many shipboard VSAT systems can be penetrated through the public internet, causing data results to broadcast live in real time on Twitter.[1] Thus, ships can be tracked and identified through services like Shodan. Shodan is a search engine which allows users to find electronic devices and computer systems connected to the internet, i.e., power plants, traffic signals and even ships. x0rz discovered that some ship's systems are not securely configured which permits a remote attacker to gain access using default credentials.

x0rz describes in The Next Web News, that he conducted research of a ship's VSAT system.[2] The system x0rz gained access into, allowed a review of the call history from their VSAT phone. This permitted x0rz the ability to change the system settings, and even upload new firmware. x0rz logged the username "admin", then used the password "1234", thereby gaining access to the ship's communication system. VSAT terminals are also popular aboard private jets and military aircraft as well.


BGR photo

Wapack Labs recommends maritime shipping companies make their satellite communications terminals such as VSAT, as well as Inmarsat, and Iridium more challenging to hackers by changing the default logins and passwords. **Never permit a ship's equipment access to the Internet by keeping the settings to internal only.** It is imperative shipping companies stay on top of firmware and software updates. Maritime interests should consider retaining the skills of a penetration tester, or lab which is familiar with satellite communications equipment, to include the routine switches, routers, and software found aboard ships.

[1]https://twitter.com/x0rz/status/887243369012973568
[2]http://www.bgr.in/news/not-just-personal-computers-ships-and-aircrafts-are-hackable-too/

WAPACK LABS CYBER INTELLIGENCE SERVICE

MPS-ISAO Intelligence Strategic Partner

Wapack Labs maritime subject matter expert reveals that based upon his military and commercial maritime experience the default login and passwords on many Inmarsat and Iridium phones were routinely remained on default settings.

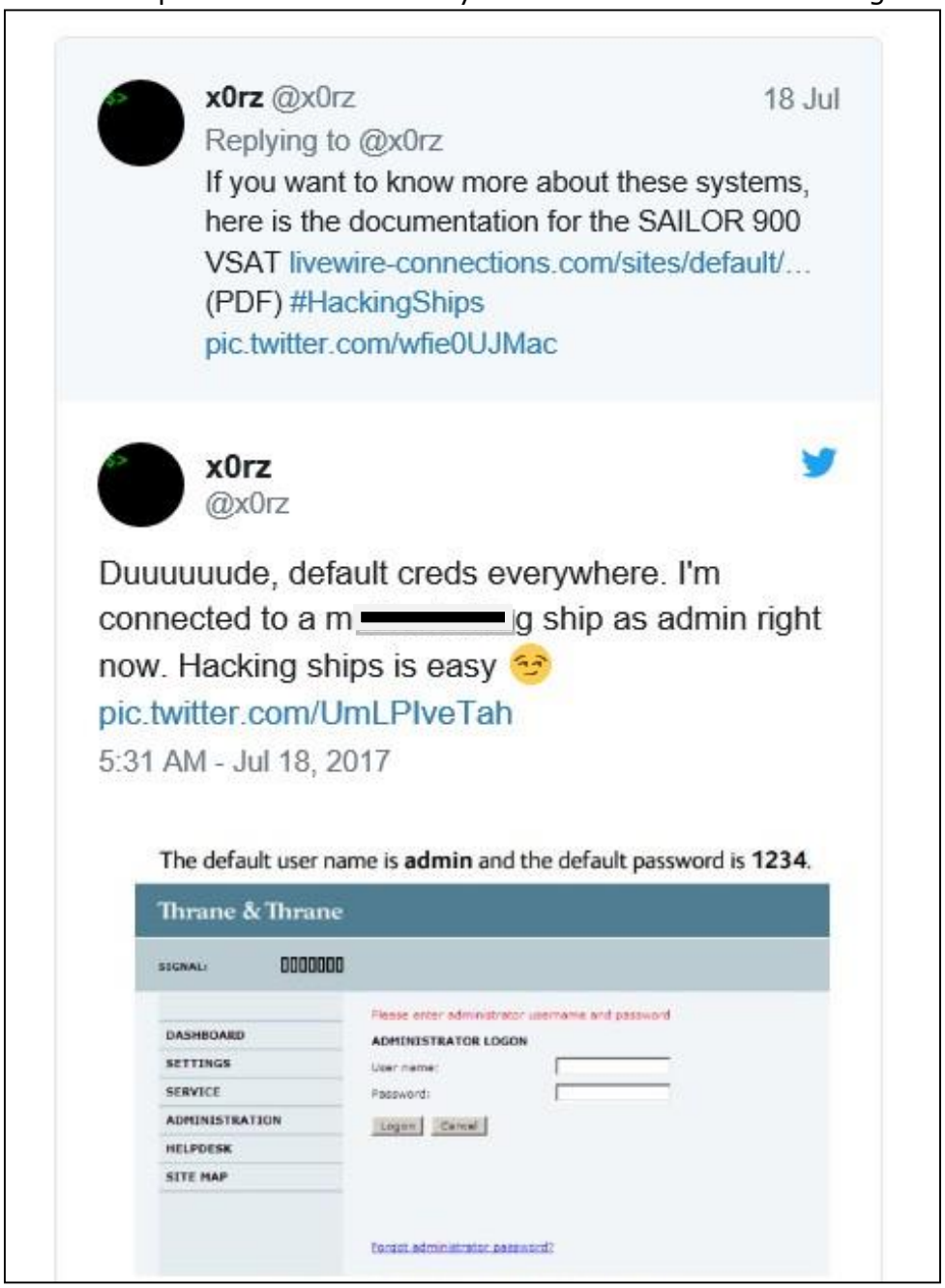

Figure 1. Twitter feed from x0rx, explaining default settings

WAPACK LABS CYBER INTELLIGENCE SERVICE

MPS-ISAO Intelligence Strategic Partner

About MPS-ISAO

Headquartered at the Global Situational Awareness Center (GSAC) at NASA/Kennedy Space Center, the MPS-ISAO is private sector-led working in collaboration with government to advance Port and Maritime cyber resilience. The core mission to enable and sustain a safe, secure and resilient Maritime and Port Critical Infrastructure through security situational intelligence, bi-directional information sharing, coordinated response, and best practice adoption supported by role-based education. The MPS-ISAO is a founding member of the International Association of Certified ISAOs (IACI). More information at: www.mpsisao.org.

About Wapack Labs

Wapack Labs, located in New Boston, NH. We are a Cyber Threat Analysis and Intelligence organization supporting the Red Sky Alliance, MPS-ISAO, the FS-ISAC, and individual corporations by offering expert level targeted intelligence analysis answering some of the hardest questions in Cyber. Wapack Labs' engineers, researchers, and analysts design and deliver transformational cyber-security analysis tools that fuse open source and proprietary information, using deep analysis techniques and visualization. Information derived from these tools and techniques serve as the foundation of Wapack Labs' information reporting to the cyber-security teams of its customers and industry partners located around the world. For questions or comments regarding this report, please contact the lab directly by at 603-606-1246, or feedback@wapacklabs.com.