Executive Summary – Cyber War at Sea

SEAS Cyber Suite of Technologies

Stryke Industries, Wattre Inc. and the Unique Mission Cell (UMC) Joint Vulnerability Assessment Branch (JVAB) participated inthe Stiletto Cyber Resiliency Demonstration (CRD) Cyber War-at-Sea (CWAS) event at Joint Expeditionary Base Little Creek, Norfolk, VA on 21 – 27 February 2021. This 5-day event featured over-the-air attack vectors and associated Cyber impacts an adversary could launch targeting maritime information technology (IT), operational technology (OT), and navigation systems via Automatic Identification System (AIS). The CWAS event included pier-side testing as well as phases underway using Fathom5's Grace Downrange (GDR) target vessel testbed installed on Stiletto.

During CWAS, JVAB launched attacks focusing on IT compromise, malicious controller area network (CAN) bus messages and AIS exploitation. The goal of JVAB was to compromise the target vessel's critical operational technology components while participating vendors demonstrated how they can detect, mitigate, and correct adversary activity targeting Grace Downrange. During the CWAS event, JVAB provided adversarial effects on the GDR IT systems to demonstrate Stryke Industries' SEAS cyber protection system. SEAS, as configured during CWAS, was a plug-and-play Cyber protection technology which sits in line between the host machine and the IT network. SEAS was configured in a set pair connecting Fathom5's Grace Downrange Vessel Server hosting the network's Active Domain (AD) and the Bridge Laptop. By design, SEAS creates an encrypted communication tunnel between connected machines protecting the data in transit, as well as guarding the protected hosts from Cyber-attacks via the ethernet port. Other I/O options for the SEAS design are also available.

JVAB used opensource Cyber-attack tactics, techniques, and procedures (TTPs) against Fathom5's Grace Downrange target systems to assess SEAS inclusion into the network, and its capacity to protect the Vessel Server and Bridge Laptop. While traditionally an AD server is a prime target for Cyber adversaries, the Bridge Laptop was the goal of JVAB as it was identifiedas the critical component linking the IT and OT environments. Any adversary with access to the Bridge Laptop could issue CAN messages to disrupt normal vessel operation. **The SEAS security solution performed as expected, denying JVAB host enumeration as well as denying JVAB's ability to launch remote code executions against the protected systems.**

WithoutSEAS in place, JVAB successfully enumerated the network identifying targets of interest and launched exploits against Grace Downrange network components ultimately gaining access to the Bridge Laptop where malicious CAN messages were launched against critical vessel components. The attacks during this event were conducted first pier side, then repeated from shore-to-ship in a littoral environment, and finally repeated from ship-to-ship while underway to simulatedifferent adversarial aggressions. **The SEAS security solution reported violations on all malicious activity** targeting the two protected network devices as well as hindered JVAB's ability to enumerate and exploit.