8 August, 2016

Operation Watersnake: Hacking the US by Ship

An attempted cyber intrusion at a Wisconsin port led officials to consider other significant vulnerabilities and weakly protected networks at critical infrastructure points around the United States, and to begin at least one known operation to identify security gaps. *Zachary Fryer-Biggs* uncovers the details.

Jane's

The 114 m Chem Hydra, a Marshall Islands-flagged oil tanker, eased into the Port of Green Bay Wisconsin on 23 September 2013. The rust orange-colored ship had travelled down the St. Lawrence River, motoring past Montreal, Canada, and around Michigan on its way to the US Venture Oil Terminal.

The next evening at 1830 h local time an interagency team from the US Coast Guard (USCG) and Customs and Border Protection swept the ship, crewed by 19 foreign nationals, and found what experts later concluded were two sets of equipment set up for hacking into nearby wireless networks.

The first sign was a Ukrainian-made black box, a marine long-range antenna, attached to a network device and a closed laptop sitting in a stateroom assigned to the ship's oiler, a term for an engineering position. The ship had no oiler on its crew list.

The second, a white box with no identifiable markings that was also an antenna, sat in a separate room connected to a laptop sitting open and powered on. On the screen was "WEPCRACKGUI", a freely available software tool designed to break into protected networks.

"It appears that an automated attack on a wifi network was under way, and although it had failed, it was set to restart," concluded a USCG report, obtained by IHS Jane's through a Freedom of Information Act (FOIA) request.

The boarding team did not determine whom the hacking equipment belonged to, but the origin of the one identifiable antenna matched with three Ukrainian crew members, who were also joined by two crew members from the Russian Federation. Eleven crew members, the majority, were from India. Experts said that although the nationalities of some of the crew members and hacking equipment could not be seen as definitive proof, it strongly suggested Russian involvement, whether as part of state-sponsored probing or organised crime, including smuggling.

The equipment found on Chem Hydra is only one example of the growing onslaught of cyber threats against critical infrastructure and the weakly protected networks that leave ports around the United States vulnerable. However, as reports about the incident circulated among government officials, some found it alarming enough to prompt further action.

Documents show that it spooked the government of Louisiana into conducting a test in early 2015, with help from the USCG, to gauge the vulnerability of the dense constellation of industrial facilities along the Lower Mississippi River. That test, Operation 'Watersnake', found that 5 of 17 industrial control system networks were highly vulnerable as result of weak or nonexistent encryption. Of eight digital surveillance networks, four were found to be highly vulnerable.

The Chem Hydra incident and the Louisiana test have not been previously reported, and the new details are noteworthy because officials rarely discuss such incidents publicly, out of concern for disclosing weaknesses, as well as the overall classified nature of nearly all things cyber in the United States.

Peter Singer, a senior fellow at the New America Foundation and author of Ghost Fleet: A Novel of the Next World War, said that facilities encountering the swarm of transport ships that dock in the United States daily are particularly vulnerable.

“Simply put, cybersecurity has not been a high priority,” Singer said. “It’s an environment that is ripe for exploitation, but has really big consequences.”

The operations manager for Ace Tankers, owner of Chem Hydra, said he did not have any knowledge of the Green Bay incident. “I don’t remember anything about that to be honest,” he said, adding that he did not believe anyone else at the company would know either.

Tanker companies, including Ace, typically use subcontractors to provide crew, and do not directly hire the personnel for a ship.

A spokesperson for US Venture Oil, owner of the dock where Chem Hydra was berthed, initially indicated that the company would look into the incident, but did not respond to IHS Jane’s requests for more information.

The USGC report does not indicate why personnel boarded the ship a day after it docked in Green Bay, but port records indicate that the Chem Hydra has not returned to the US Venture Oil dock since.

The Test

Details about the Green Bay incident come from a copy of a USGC report obtained by IHS Jane’s FOIA request after seven months of review by US government officials, as well as from a July 2015 briefing on Operation ‘Watersnake’ that referenced the incident and listed it as the impetus for the subsequent test. The documents viewed by IHS Jane’s were marked sensitive but unclassified. Sources confirmed several points about the operation, although the final report on ‘Watersnake’, including detailed findings, remains classified, according to sources.

The coast guard provided USCGC Pompano, a 27 m coastal patrol boat captained by Lieutenant Junior Grade Austin King. Louisiana, working through the Louisiana State Analytical and Fusion Exchange (LA-SAFE), had personnel mount hardware on the ship that could have been bought from any electronics supplier, as well as commercially available software to probe networks within sight of the river.

The hardware was the Danets USB Yagi TurboTennna, and the software came from Kismet. The setup closely mirrored that found on the Chem Hydra, with a long-range antenna paired with a network device and a computer running open-source wifi cracking software.

On 6 January 2015 the boat embarked, steaming about 290 km between Baton Rouge and New Orleans along the winding Mississippi, one of the United States’ most vital and trafficked waterways, while constantly pinging networks and testing their security levels.

The USCG provided the boat, but it was Louisiana officials that placed experts on board to probe available networks with the off-the-shelf equipment, according to sources.

Looking at only industrial control systems, energy transmission, and digital surveillance networks, the team found 6,740 active internet devices and discovered that half of the tested surveillance networks and nearly a third of the industrial control systems were highly vulnerable.

"It's not surprising, to be honest, but it is dramatic," one source familiar with the operation said.

The USCG directed all questions about Operation 'Watersnake' to LA-SAFE. A spokesman for LA-SAFE initially indicated he would look into the operation, but then did not respond to further questions.

Although the Mississippi River might more often call to mind steamboats and a bygone era, it still functions as a major corridor for the US economy. A 2015 study by several non-profit groups and the US Fish and Wildlife Service estimated that USD405 billion in annual revenue is reliant upon the river, which supports 1.3 million jobs. Half of the United States' barges are in Louisiana on any given day, and the river has "frequent exposure to foreign flagged vessels", according to the 'Watersnake' briefing.

However, beyond the economic impact, the Mississippi River also serves as a corridor for a range of industrial facilities working with dangerous materials. Those facilities rely upon industrial control systems, the same systems the 'Watersnake' test found highly vulnerable. Sabotage of those systems could result in a dangerous spill.

Retired Army Lieutenant General Russel Honoré said there are more than 100 chemical plants along the river between Baton Rouge and New Orleans. "Many of those plants produce some of the most toxic chemicals that are permitted to even exist," he said. Honoré, besides being from the area, also served as commander of Joint Task Force Katrina, and was responsible for military-aid to the region following the devastation of Hurricane Katrina in 2005.

Most of the concerns about the industrial facilities along the river after Katrina focused on flooding and the destruction of levies. However, after military planners began looking into vulnerabilities, the lack of security became a glaring issue.

"Most of these plants don't have any protection around them," Honoré said. "If you were walking on the street next to it, it's a simple chain link fence that surrounds a baseball field."

However, threats that could not be prevented by simple fences, such as a hacker on a barge heading up or down the river, did not receive any major attention until after the creation of US Cyber Command in 2010, according to sources. Even then, the assumption that the facilities' relatively rural isolation would provide protection meant that few steps were taken to harden either physical security or cybersecurity.

Beyond the chemical plants, there's another glaring vulnerability: a bridge across the river that carries fibre-optic cable responsible for a large portion of internet traffic in the southeastern United States. The bridge's structure has been damaged by weathering and its collapse, could cripple connectivity for a large corner of the United States.

The other threat would be a hacker using the vulnerability of the exposed pipeline to gain access to large amounts of data traversing the country. Realising the vulnerability the exposed section has created, some security has been posted around the bridge over the last decade, according to sources. Those sources discussed the bridge's vulnerability under the condition that the specific bridge not be identified by IHS Jane's.

The USCG report does not say why the operation was called 'Watersnake', but the name has interesting potential references. Joseph Conrad described the Congo River as "resembling an immense snake uncoiled, with its head in the sea, its body at rest curving afar over a vast country and its tail lost in the depths of the land".

More recently a video game released in 2011 used the term Operation Water Snake in reference to a fictional attack on the United States via the Mississippi river. In the game, Homefront, the North Korean military decides to irradiate the Mississippi River to drive a wedge through the middle of the United States and the fictional attack renders 160 km on either side of the river uninhabitable.