Sophisticated scams highlight growing cyber risk to shipping

A hacking operation by suspected Chinese military operatives on a US Department of Defense-contracted ship and an $18m bunker-tender scam are just the latest IT-based attacks to have hit the maritime sector

Eric Martin **Stamford**

A series of newly revealed attacks on the shipping industry have highlighted the growing risk to the sector in cyberspace.

In one, a commercial ship on contract to the US military was the target of an intrusion by suspected Chinese military hackers.

Another incident saw a major fuel supplier fall victim to an $18m scam as the bunkers sector faces growing cybercrime threats.

A report released in recent weeks by the US Senate's Armed Services Committee found some 50 successful intrusions or "other cyber events" on US Transportation Command (Transcom) contractors in the 12 months ending on 30 May 2013.

Transcom was only aware of two of the 20 successful intrusions that qualify as so-called advanced persistent threats, which were all attributed to China and targeted at airlines or shipping companies.

The report found that in 2012, the Chinese military compromised "multiple systems" on a commercial ship on contract to Transcom. The vessel was not identified in the report, which contained numerous redactions of sensitive information and was secret until recently.

▸**KEY FINDINGS:** A report by the US Senate's Armed Services Committee found some 50 successful intrusions on US Transport Command (Transcom) contracts in the 12 months up to May 2013.
Photo: BLOOMBERG

> "Former MarAd counsel Denise Krepp: It's clear now that hackers can also destroy or manipulate ship data. The manipulation of data could allow terrorists to more easily enter the US. It could also allow the Chinese to significantly impact our country's vital supply chains.

'SPEARPHISHING CAMPAIGNS'

Marine shipping providers were also the target of so-called spearphishing campaigns by China's People's Liberation Army. Such attacks use spoof e-mails targeted at a single company to secure access to confidential data.

During the period covered by the report, two shipping companies were among 16 Transcom contractors identified by the Federal Bureau of Investigation (FBI) to have been targeted by a cyber-intrusion.

Foreign governments regularly probe computer networks of the US Defense Department, and logistics providers, including ship operators, are a prime target. That is because in the event of major conflict, military resupply networks are expected to be a front-line target of cyber warfare, according to the Senate report.

Transcom relies on vessel operators through the Voluntary Intermodal Sealift Agreement (VISA) and the Maritime Security Program (MSP), whose participants range from small US operators to global titans including APL and AP Moller-Maersk. In 2012 alone, commercial ships moved 95% of Department of Defense dry cargoes, the study found.

Denise Krepp, a former chief counsel for the US Maritime Administration (MarAd), calls the Armed Services Committee report troubling. She says that when the US Maritime Transportation Security Act was enacted in 2002, the worry was physical attacks on vessels or ports.

"It's clear now that hackers can also destroy or manipulate ship data. The manipulation of data could allow terrorists to more easily enter the US. It could also allow the Chinese to significantly impact our country's vital supply chains," Krepp said. She argues that the US Coast Guard (USCG) should use its authority to require additional cyber security measures for Transcom-contracted vessels.

A Department of Defense spokeswoman did not immediately respond to a request for comment on the report.

Chinese military hackers are not the only cyber security threat facing the shipping industry. Cargo insurer AGCS Marine Insurance Co has filed a federal lawsuit in New York over a scam that cost US bunkers giant World Fuel Services (WFS) an estimated $18m.

The lawsuit, which is challenging WFS's insurance claim over the incident, says "someone" impersonated the US Defense Logistics Agency to set up a fake tender for a large cargo of fuel. After WFS received the offer to participate in the tender and eventually supplied the cargo, it submitted an invoice. The government agency had no record of the fuel tender.

But it was too late, WFS had already purchased 17,000 metric tonnes of marine gas oil from Monjasa and delivered it via ship-to-ship transfers in two parcels to a tanker known as the *Ocean Pearl* while it was off the Ivory Coast, according to legal documents that were filed in July but that have only recently drawn the attention of cybersecurity experts. Receiving no payment for the deal, WFS sought recovery from AGCS for cargo loss.

A WFS spokeswoman did not immediately respond to a request for comment on the lawsuit.

Maritime lawyer Stephen Simms, principal at Baltimore law firm Simms Showers, says cyber scammers are targeting the bunkering sector with increasing frequency.

IMPERSONATION THREAT

In an industry in which transactions are frequently done by e-mail, one way these criminals are cheating bunkers buyers is by impersonating sellers and sending messages providing payment information — but the bank details lead the buyer to put the funds into an account belonging to the scammer, rather than a legitimate seller.

It is a scam that Simms says requires an industry insider, or even a current or former employee of the defrauded company.

"It happens because there are people who understand the way payments work and data is used in the maritime industry, and they manipulate it to commit cybercrime," he said, speaking to TradeWinds from Antwerp, where he delivered a presentation on the topic at a bunkering symposium.

STAYING SAFE IN CYBERSPACE

Here are some steps Simms Showers lawyer Stephen Simms recommends to prevent becoming a victim of cybercrime:

▸ **PICK UP THE PHONE** — although transactions are increasingly done by e-mail, voice confirmation will help ensure you are dealing with the person you are meant to be dealing with.

▸ **ENSURE DETAILS MATCH** — look for variations in instructions for wiring funds.

▸ **USE ENCRYPTED E-MAILS** — it may slow down a conversation, but it will enhance security.

▸ **CARRY OUT CYBERSECURITY AUDITS** — auditors should examine processes for receiving orders and sending payments.

▸ **BE WARY OF INSIDER THREAT** — make sure that former employees no longer have access to systems and current employees do not bring in malevolent software via external-storage devices.

▸**ADVICE:** Lawyer Stephen Simms advocates picking up the phone to verify a person's identity. **Photo:** BLOOMBERG