LUCENAGROUP
GLOBAL ASSURANCE STRATEGIES

SUPPLY CHAIN SECURITY BRIEF

17 July 2014

Vulnerability of port computers are a security risk that could lead to massive thefts and attacks

What if cargo gangs and criminal organizations had access to cargo details, destinations and client information from ports around the country, choosing loads based on value and cargo type? Sound far-fetched? Unfortunately, there have been several major cases where detailed shipment information was acquired through compromised computer networks. As criminals seek alternative ways to steal cargo, new methods and strategies will likely be employed that target port computer systems around the world. These intrusions not only pose a threat to companies, but also governments and economies. As more ports around the world rely on computers and software to manage and track shipments, they will be increasingly vulnerable to malicious network attacks and breaches.

Last October a sophisticated criminal network in Belgium hacked into the Port of Antwerp's computer systems, which allowed the groups to follow the movement and location of containers around the port. This facilitated the extraction of drugs that were concealed in certain containers. This week, it was revealed that a Chinese manufacturing company deliberately installed malware into their handheld inventory scanners. This malware extracted the manifest data from port shipments when the scanners connected to company networks. These revelations illustrate both the value of cargo and manifest information to criminal enterprises, foreign governments and corporations and the lengths these entities will go to break into computer networks.

For both the cases mentioned earlier, the breaches did not contribute to massive thefts of cargo (apart from the containers used to smuggle the drugs in Antwerp). This will not always be the case. Sophisticated cargo gangs and criminal organizations active around major ports could break into port networks to acquire the cargo, destination and storage locations of certain high-value shipments. This information could then be used to steal cargo at the port or once it departs. With respect to the China case (and other future cases like it), the compromised information could be used by government officials and foreign companies as an edge when negotiating contracts and deals. If used properly, customer data and product information could impact business operations at ports (or shipping companies that had the breach) and hurt local economies.

Breaches also pose a threat to the security of countries. If terrorists or drug traffickers gained access to systems and manipulated the data, they could pick up shipments hiding cargo or weapons before they were examined by customs. Furthermore, a terrorist group looking to strike the United States and disrupt the economy could easily do so from a sophisticated cyber-attack against port computer systems. If port computers failed to work properly, goods would not be able to be unloaded. The destinations and scheduled delivery times of shipments would be lost. This would have enormous implications for the U.S. economy, especially if simultaneous attacks disabled major ports on the West Coast of the U.S.

Many people and companies rely too heavily on computer systems for managing business and logistical operations and fail to see the threat until it is too late. Ports are no exception. Despite a recent Government Accountability Office (GAO) report warning of the vulnerabilities of U.S. ports to cyber-attacks, problems will not be solved overnight. The rapid evolution of computers means new vulnerabilities are discovered every day. Criminals are constantly looking for ways to stay ahead of law enforcement officials. As a result, the United States and other countries will see an increase in both the number of thefts from ports and criminal activity resulting from breached systems.

Sources

Tom Bateman, "Police warning after drug traffickers' cyber-attack", *BBC News*, 16 October 2013.

Kelly Jackson Higgins, "Chinese Hackers Target Logistics & Shipping Firms with Poisoned Inventory Scanners", *Information Week*, 10 July 2014.

Rachael King, "Hacking Groups Target Shipping Ports", *Wall Street Journal*, 9 July 2014.

About Lucena Group

Lucena Group is a Global Security Solutions Company that specializes in custom risk mitigation for global businesses. Below are some of the services we offer, contact Lucena Group for more information:

Global Support Services
Global protective solutions with specializations in Executive Protection, secure transportation, consulting and training, and kidnap and ransom negotiations.

Operational and Protective Intelligence
Lucena Intelligence (LUCINT) provides proactive, relevant, and fully customized intelligence, including Risk Trend Analysis, Foreign Travel Reports, and Tiered Custom Intelligence Packages.

Supply Chain Security
We ensure product/cargo integrity through compliance and assessments, customized security programs, and leveraging advanced monitoring and response technologies.

Investigations/Due Diligence
A niche level of intelligence support, data acquisition & investigative services to clients that include Persons of Interest, Domestic and International Due Diligence, and Skip-trace/Locate Investigations.

Jason Stolpa	**George Wheeler**	**Victor Garcia**
Global Logistics Intelligence Analyst	Senior Director	Senior Manager
+1 512.861.2284	+1 512.993.6707	+1 512.739.6798
jstolpa@lucenagroup.com	gwheeler@lucenagroup.com	vgarcia@lucenagroup.com