Splash 247.com

Biden to replace Chinese-made cranes at all American ports

Sam Chambers

February 22, 2024

Port of Los Angeles

Election year in the US with hysteria growing by the day about a more strident China has seen the White House take action over a perceived threat at its ports.

President Joe Biden yesterday signed an executive order giving the coast guard greater powers to police cyber security at ports, as well as setting in place a plan to replace the nation's Chinese-built port cranes with Japanese ones over concerns they could be fitted with spy devices.

"These cranes, because they are essentially moving the large-scale containers in and out of port, if they were encrypted in a criminal attack, or rented or operated by an adversary, that could have real impact on our economy's movement of goods and our military's movement of goods through ports," said Anne Neuberger, deputy national security adviser for cyber and emerging technology.

Around 80% of the cranes used in American ports are made in China and use Chinese software. Biden has earmarked $20bn over the next five years to get these replaced by a US subsidiary of Mitsui.

American maritime assets were reportedly being targeted last year by Volt Typhoon, a Chinese state-sponsored snooping operation, according to tech giant Microsoft.

Microsoft said it had uncovered "stealthy and targeted malicious activity" focused on post-compromise credential access and network system discovery aimed at critical infrastructure organisations in the US. The attack is carried out by Volt Typhoon, a state-sponsored actor based in China that typically focuses on espionage and information gathering.

According to Microsoft, Volt Typhoon has been active since mid-2021 and has targeted critical infrastructure organisations in Guam and elsewhere in the US. In this campaign, the affected organisations span the communications, manufacturing, utility, transportation, construction, maritime, government, information technology, and education sectors.

"Observed behavior suggests that the threat actor intends to perform espionage and maintain access without being detected for as long as possible," Microsoft stated in an update on its site, going on to explain how the perpetrators rely almost exclusively on living-off-the-land techniques and hands-on-keyboard activity. They issue commands via the command line to collect data, including credentials from local and network systems, put the data into an archive file to stage it for exfiltration, and then

use the stolen valid credentials to maintain persistence. In addition, Volt Typhoon tries to blend into normal network activity by routing traffic through compromised small office and home office (SOHO) network equipment, including routers, firewalls, and VPN hardware. They have also been observed using custom versions of open-source tools to establish a command and control channel over proxy to further stay under the radar.

Shipping is well aware of the threat posed by state-backed malware.

A major cyber security report published by Thetius, CyberOwl and HFW detailed many recent cyber incidents including how the Stena Impero tanker's GPS was spoofed to force it to cross into Iranian waters unintentionally in 2019 with the ship and its crew then held for months.

The equipment required for basic GPS attacks costs less than $100, the report warned while adding that with the resources of a nation-state, "a sophisticated spoof on an entire region or sea is not just a possibility, it is a reality".
Getting to take over a ship's controls is also remarkably easy with data from CyberOwl showing 54% of the ships it monitors have between 40 and 180 connected devices onboard. This includes expected devices such as business workstations, PCs, printers, and company phones. Most alarming is that on many vessels monitored by the company, systems that were thought to be isolated, such as cargo computers and engine monitoring systems, were found to be connected to the onboard business IT network somehow.
Over 60% of computers monitored by CyberOwl have various unofficial or crew-installed software, and 30% of computers make frequent use of the local administrator account giving the user full rights to the machine.

Other key takeaways from the 43-page report include news that CyberOwl discovered nation-state malware on systems onboard seven separate vessels belonging to a large liner fleet. The malware belonged to the PlugX family, which is designed to provide the attacker remote access to the affected system, followed by full admin control of the machine without permission or authorisation. This includes the ability to manipulate files, execute commands, and spread locally. The particular malware variant was first discovered in 2020 and linked to political espionage on foreign nations.