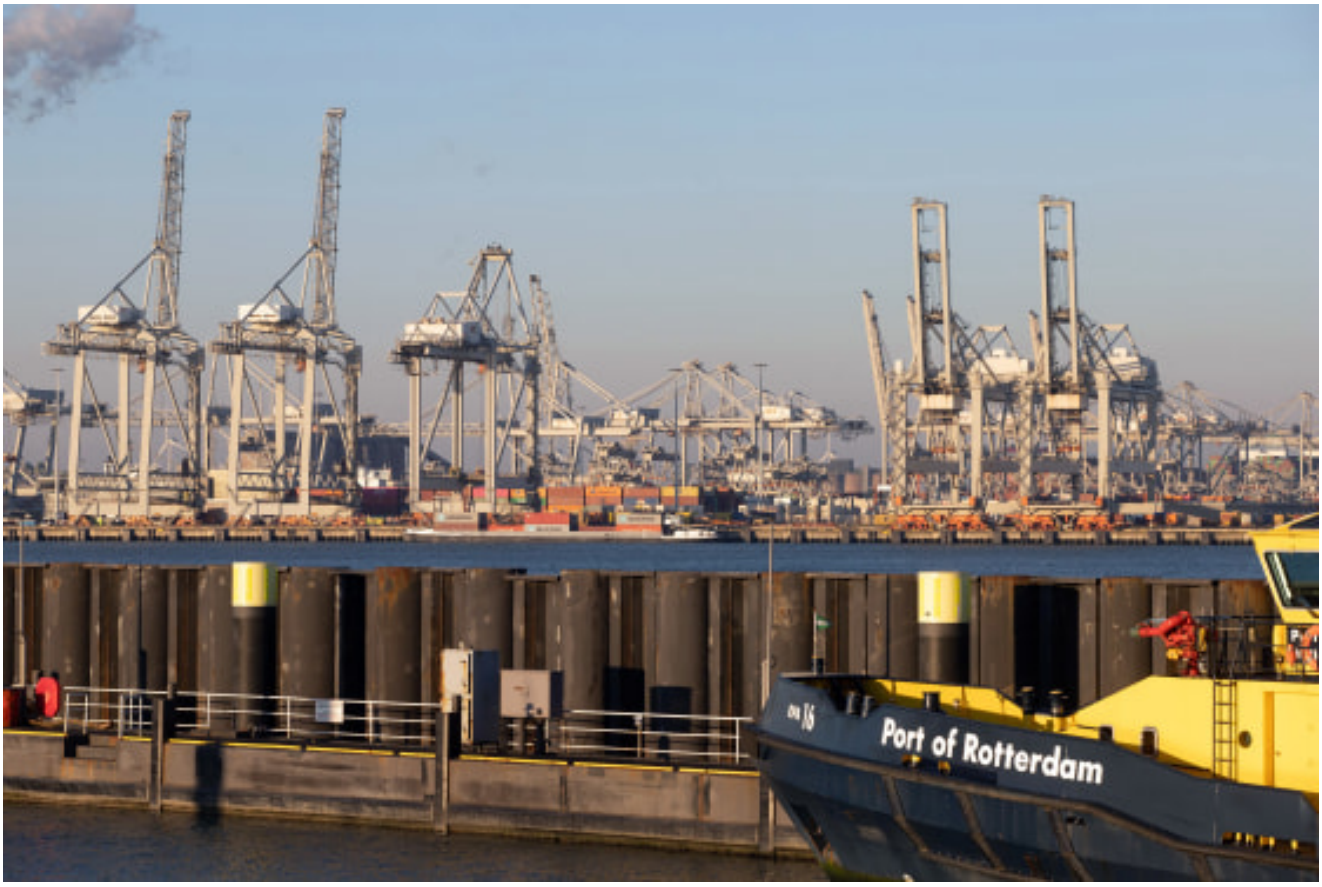
China-linked group uses malware to try to spy on commercial shipping, new report says

nbcnews.com/news/world/china-linked-group-malware-spy-commercial-shipping-cargo-report-eset-rcna152129

May 14, 2024



BIRMINGHAM, UK — The cyber espionage group known as Mustang Panda introduced malware over the past five months to gain remote access to “computer systems belonging to cargo shipping companies based in Norway, Greece, and the Netherlands, including some that appeared to be aboard the cargo ships themselves,” according to the Slovakia-based cyber security firm ESET.

The report came as top U.K. and U.S. officials on Tuesday warned of a growing cybersecurity threat from China, particularly to critical infrastructure.

According to the report, Mustang Panda, which has been accused of carrying out espionage against governments and other organizations across Asia and more recently in Europe, has used similar malware tools in previous spying campaigns. The “remote access trojan” type of malware allows an attacker to gain full access to a device and issue commands, after breaking in through an email, a malicious website, vulnerable software or an unprotected machine.

It was the first time evidence had emerged that a China-linked cyber espionage group was focusing on commercial shipping, researchers said.

“We haven’t seen this in the past,” said Robert Lipovsky, principal threat intelligence researcher at ESET. “It shows a clear interest in this sector. This was not a single occurrence. These were several distinct attacks at different, unrelated organizations,” he said.

It was unclear if the cyber spying effort included the use of USB devices physically planted at the companies or on ships, he said.

A spokesman for China’s embassy in Washington strongly denied the accusations.

“We oppose any groundless smears and accusations against China. In fact, China is a major victim of cyber attacks,” said spokesman Liu Pengyu.

“We keep a firm stance against all forms of cyber attacks and resort to lawful methods in tackling them. China does not encourage, support or condone attacks launched by hackers.”

At a cybersecurity conference Tuesday in the United Kingdom, British and U.S. officials described a mounting danger from Chinese cyber espionage and hacking.

“China is the single biggest area of focus right now,” a British cybersecurity official told reporters on the sidelines of the conference in Birmingham organized by the U.K. government.

In a speech at the conference, the head of GCHQ, the U.K.’s cyber intelligence agency, said that although Russia and Iran posed immediate threats, China remains “the ‘epoch-defining’ challenge” and presented a risk for the security of the internet and the international order.

“China has built an advanced set of cyber capabilities and is taking advantage of a growing commercial ecosystem of hacking outfits and data brokers at its disposal,” Anne Keast-Butler said. “China poses a genuine and increasing cyber risk to the U.K.”

In a speech at the same conference, Harry Coker, White House national cyber director, said China’s cyber spying meant that Beijing had the ability to disrupt and damage America’s civilian infrastructure.

“In a crisis or conflict scenario, China could use their pre-positioned cyber capabilities to wreak havoc in civilian infrastructure and deter U.S. military action,” Coker said.

The Biden administration has accused China of carrying out a massive espionage effort known as “Volt Typhoon” that penetrated an array of critical infrastructure.

China has rejected accusations from the U.S., Britain and other governments that it is carrying out cyber espionage, cyberattacks or intellectual property theft. On Tuesday, Chinese Foreign Ministry spokesperson Wang Wenbin said the U.K. has repeatedly hyped allegations about Chinese cyber activities.

British and U.S. officials at the conference said China's cyber tactics increasingly have shifted from trying to steal intellectual property or foreign intelligence to gaining stealthy access to critical utilities or other infrastructure organizations, using it as a potential leverage in a crisis.

China has "moved on" from intellectual property theft, Natalie Pittore of the National Security Agency said at a conference panel discussion.

"It's increasingly what appears to be a pre-positioning (inside infrastructure) to have an effect," said Pittore, the NSA's cybersecurity liaison to the U.K.

"They're not in there actively stealing information the way you would with foreign intelligence access, or even IP theft," she said. "Instead, what we observed from these Chinese APTs (advanced pervasive threats) is that they will get in, they will get a level of control and even more so the level of ability to control a network, and they go very quiet."

Jean-Nicholas Fievet
Jean-Nicholas Fievet is a senior desk editor for NBC News based in London.