STATE OF FREIGHT

Hackers can bring ships and planes to a grinding halt. And it could become much more common

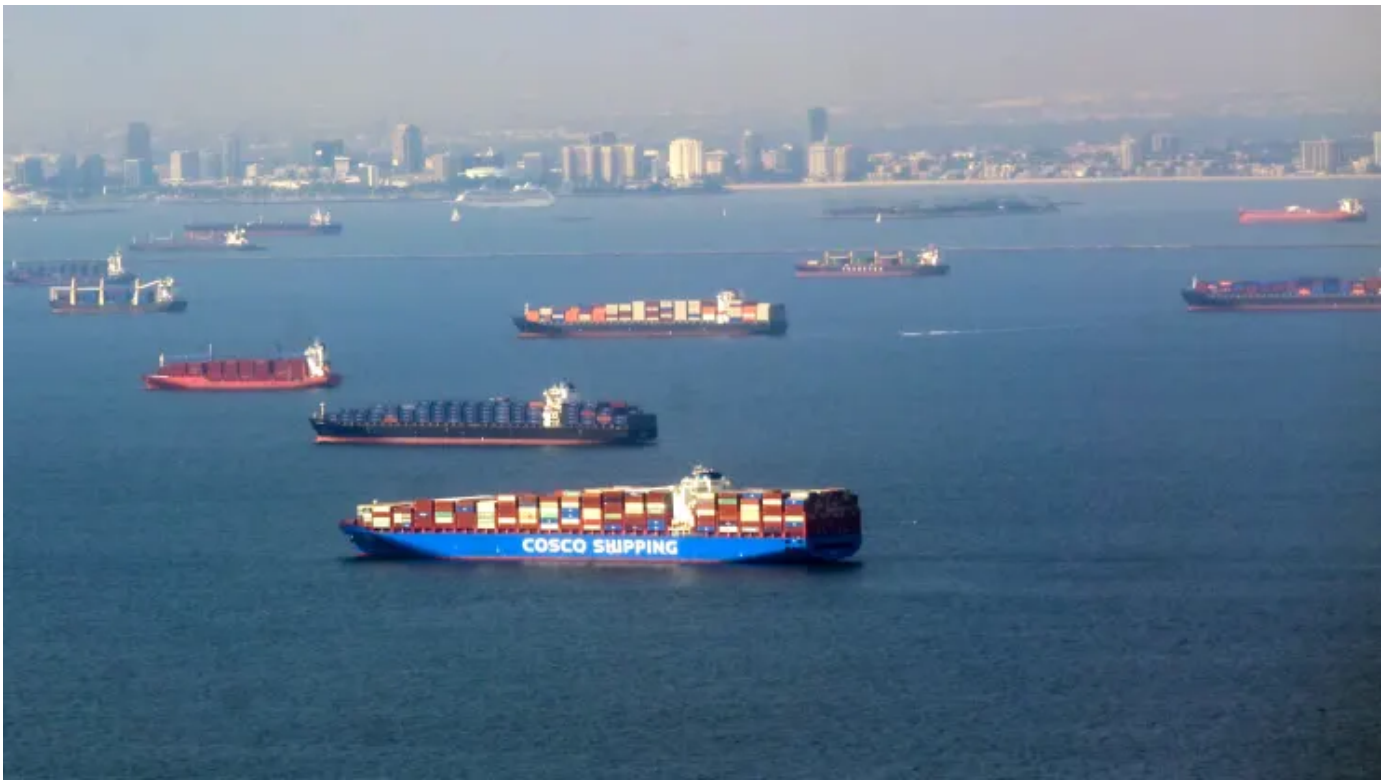
PUBLISHED MON, JUN 27 2022•2:14 AM EDT | UPDATED MON, JUN 27 2022•2:14 AM EDT

Sam Shead
@SAM_L_SHEAD

WATCH LIVE

KEY POINTS

- Vast container ships and chunky freight planes — essential in today's global economy — can now be brought to halt by a new generation of code warriors.
- "The reality is that an aeroplane or vessel, like any digital system, can be hacked," David Emm, principal security researcher at Kaspersky, told CNBC.
- In December, German firm Hellmann Worldwide Logistics said its operations had been impacted by a phishing attack.



Container cargo ships sit off shore from the Long Beach/Los Angeles port complex in Long Beach, CA, on Wednesday, October 6, 2021.
Jeff Gritchen | MediaNews Group | Getty Images

Armed with little more than a computer, hackers are increasingly setting their sights on some of the biggest things that humans can build.

Vast container ships and chunky freight planes — essential in today's global economy — can now be brought to a halt by a new generation of code warriors.

security researcher at cyber firm Kaspersky, told CNBC.

Indeed, this was proven by the U.S. government during a "pen-test" exercise on a Boeing aircraft in 2019.

Hacking logistics

Often it's easier, however, to hack the companies that operate in ports and airports than it is to access an actual aircraft or vessel.

In December, German firm Hellmann Worldwide Logistics said its operations had been impacted by a phishing attack. Phishing attacks involve sending spoof messages designed to trick people into handing over sensitive information or downloading harmful software.

The company, which offers airfreight, sea freight, road and rail, and contract logistics services, was forced to stop taking new bookings for several days. It's unclear exactly how much it lost in revenue as a result.

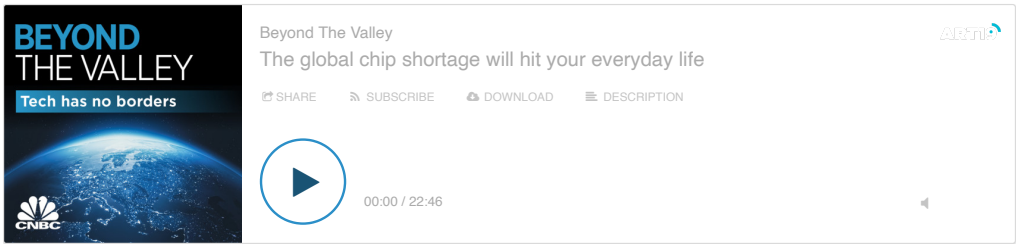
Hellmann's Chief Information Officer Sami Awad-Hartmann told CNBC that the firm immediately tried to "stop the spread" when it realized it had fallen victim to a cyberattack.

"You need to stop it to ensure that it's not going further into your [computing] infrastructure," he said.

Hellmann, a global company, disconnected its data centers around the world and shut down some of its systems to limit the spread.

"One of the drastic decisions we then made when we saw that we had some systems infected is we disconnected from the internet," Awad-Hartmann said. "As soon as you make this step, you stop. You're not working anymore."

Everything had to be done manually and business continuity plans kicked in, Awad-Hartmann said, adding that some parts of the business were able to handle this better than others.



Awad-Hartmann said the hackers had two main goals. The first being to encrypt Hellmann and the second being to exfiltrate data.

"Then they blackmail you," he said. "Then the ransom starts."

Hellmann did not get encrypted because it moved swiftly and closed down from the internet, Awad-Hartmann said.

"As soon as you're encrypted, of course your restarting procedure takes longer because you may need to decrypt," he explained. "You may need to pay the ransom to get the master keys and things like this."

Hellmann is working with legal authorities to try to determine who is behind the cyberattack. There's some speculation but no definitive answers, Awad-Hartmann said.

NotPetya attack

The notorious NotPetya attack in June 2017, which impacted several companies including Danish container shipping firm Maersk, also highlighted the vulnerability of global supply chains.

Maersk first announced that it had been hit by NotPetya — a ransomware attack that prevented people from accessing their data unless they paid $300 in bitcoin — in late June of that year.

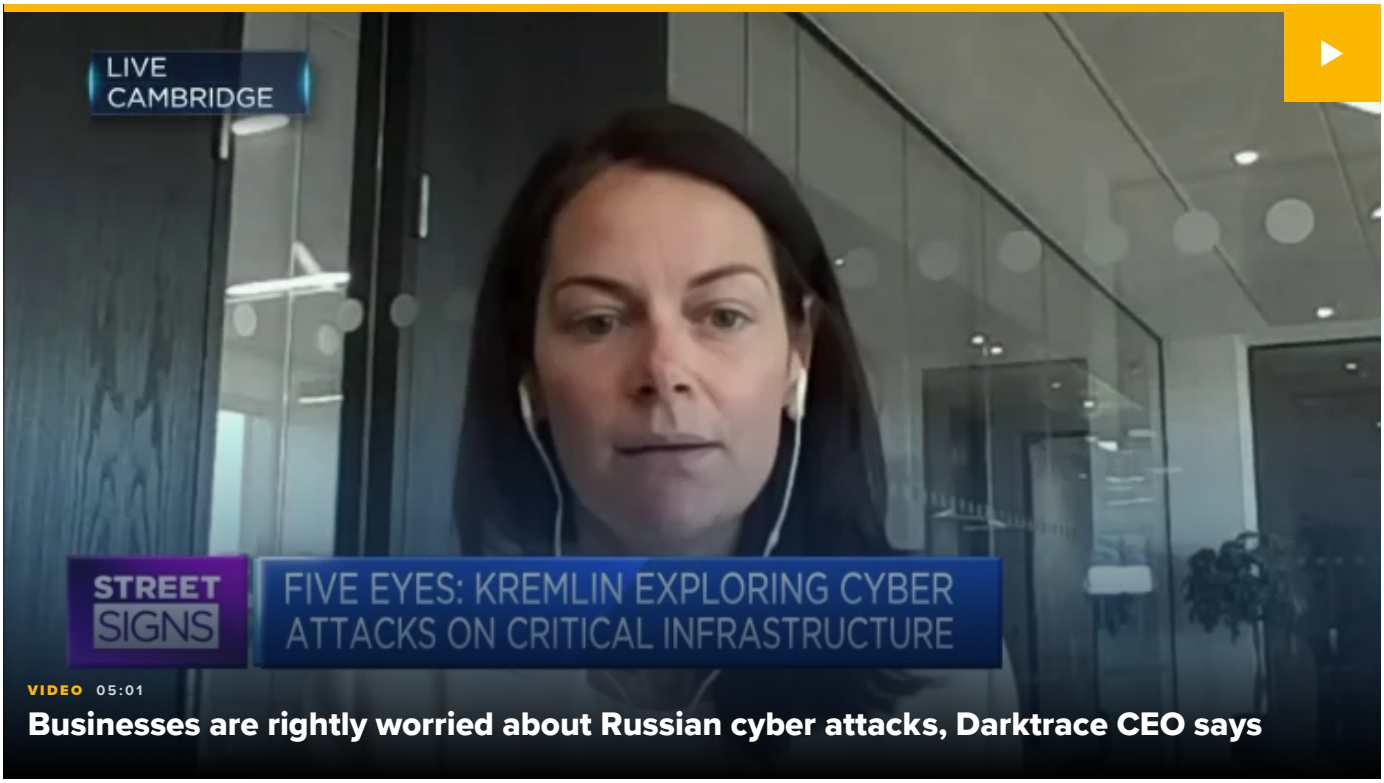
APM Terminals and Damco," Maersk CEO Soren Skou said in a statement in Aug. 2020.

"Business volumes were negatively affected for a couple of weeks in July and as a consequence, our Q3 results will be impacted," he added. "We expect that the cyber-attack will impact results negatively by $200 - $300 million."

The ransomware attack took advantage of certain security vulnerabilities in the Windows software platform that Microsoft had updated after they leaked.

"This cyber-attack was a previously unseen type of malware, and updates and patches applied to both the Windows systems and antivirus were not an effective protection in this case," Maersk said.

"In response to this new type of malware, A.P. Moller Maersk has put in place different and further protective measures and is continuing to review its systems to defend against attacks."



In a follow-up article, Gavin Ashton, an IT security expert at Maersk at the time, wrote that it's "inevitable" you will be attacked.

"It is inevitable that one day, one will get through," Ashton continued. "And obviously, you should have a solid contingency plan in place in case of the worst. But that's not to say you don't attempt to put up a damn good fight to stop these attacks in the first case. Just because you know the bad actors are coming, doesn't mean you leave your front door open and make them a cup of tea when they walk in. You could just lock the door."

Meanwhile, in February 2020, Japan Post-owned freight forwarder, Toll Group was forced to shut down certain IT systems after suffering a cyberattack. Toll Group did not immediately respond to a CNBC request for comment.

Disguising drug shipments

Sometimes the hackers aren't necessarily looking for a ransom.

In 2013, criminals hacked systems at the port of Antwerp in order to manipulate the movement of containers so that they could conceal and move their drug shipments.

containers that had the drugs in them.

The smugglers then sent their own drivers to pick up the drug-loaded shipping containers before the legitimate hauler could collect them.

The hackers used spear phishing and malware attacks — directed at port authority workers and shipping companies — to obtain access to the systems.

The whole scheme was uncovered by police after shipping firms detected something wasn't right.

Awad-Hartmann said hackers have realized how important global supply chains are, and they now know what happens when they get disrupted.

"It impacts the whole world economy," he said. "You see goods are not flowing. You have gaps in the supermarkets. Of course I think the hackers do see the dependency on this supply chain. And then of course a logistics company is a target for them."

He added that logistics is in focus at the moment because global supply chains are in the news.

"But I think it's a general threat," he said.

"And this will not go away. It will increase. You constantly need to check. Are you still prepared? This is something which keeps us quite busy and costs us a lot of money."

RELATED

The housing market slowdown is showing up in shipping data from China

Hackers can bring ships and planes to a grinding halt. And it could become much more common

Chinese manufacturing orders decline, according to shippers, as consumers pull back on buying goods

How President Biden's Ocean Reform Act could impact shipping and inflation

Latest Shanghai quarantines add more pressure to global supply chain

MORE IN STATE OF FREIGHT