Cyberattacks Discovered on Vaccine Distribution Operations

David E. Sanger and Sharon LaFraniere

A series of cyberattacks is underway aimed at the companies and government organizations that will be distributing coronavirus vaccines around the world, IBM's cybersecurity division has found, though it is unclear whether the goal is to steal the technology for keeping the vaccines refrigerated in transit or to sabotage the movements.

Johanna Geron/Reuters The European Commission's Directorate General for Taxation and Custom in Brussels was one of the targets of the attack.

The findings are alarming enough that the Department of Homeland Security plans to issue its own warning on Thursday to Operation Warp Speed, the Trump administration's effort to develop and distribute coronavirus vaccines, federal officials said.

Both the IBM researchers and the department's Cybersecurity and Infrastructure Security Agency said the attacks appear intended to steal the network credentials of corporate executives and officials at global organizations involved in the refrigeration process necessary to protect vaccine doses, or what the industry calls the cold chain.

Josh Corman, a coronavirus strategist at the cybersecurity agency, said in a statement that the IBM report was a reminder of the need for "cybersecurity diligence at each step in the vaccine supply chain." He urged organizations "involved in vaccine storage and transport to harden attack surfaces, particularly in cold storage operation."

The cyberattackers "were working to get access to how the vaccine is shipped, stored, kept cold and delivered," said Nick Rossmann, who heads IBM's global threat intelligence team. "We think whoever is behind this wanted to be able to understand the entire cold chain process."

Many of the approaches came in the form of "spear phishing" emails that impersonated an executive at a major Chinese company, Haier Biomedical, which is a legitimate participant in the distribution chain. The email says "we want to place an order with your company," and includes a draft contract containing malware that would give the attackers access to the network.

Researchers for IBM Security X-Force, the company's cybersecurity arm, said they believed that the attacks were sophisticated enough that they pointed to a government-sponsored initiative, not a rogue criminal operation aimed purely at monetary gain. But they could not identify which country might be behind them.

Outside experts said they doubted it was China, which has been accused of trying to steal vaccine information from universities, hospitals and medical researchers, because it would be unlike Chinese hackers to impersonate executives at a major Chinese firm.

If they are correct, the lead suspects would be hackers in Russia and North Korea, both of which have also been accused by the United States of conducting attacks to steal information about the process of manufacturing and distributing vaccines. Sometimes it is hard to tell the difference between official hacking operations for the Russian or North Korean governments and those run for private gain.

The motive is also unclear. The attackers may simply be looking to steal technology to move large amounts of vaccine across long distances at extraordinarily low temperatures, which would constitute a classic form of intellectual property theft.

But some cybersecurity experts say they suspect something more nefarious: efforts to interfere with the distribution, or ransomware, in which the vaccines would be essentially held hostage by hackers who have gotten into the system that runs the distribution network and locked it up — and who demand a large payment to unlock it.
"There is no intelligence advantage in spying on a refrigerator," said James Lewis, who runs the cybersecurity programs at the Center for Strategic and International Studies in Washington. "My suspicion is that they are setting up for a ransomware play. But we won't know how these stolen credentials will be used until after the vaccine distribution begins."

The IBM researchers provided an account of their efforts in an interview before the company posted its findings. They said the attackers sent out various requests for price and product information, some purportedly on behalf of Gavi, the Vaccine Alliance, a public-private partnership that helps provide vaccines to developing countries.
Many of the targets were in Asia, but some were European, including the European Commission's Directorate General for Taxation and Customs Union. IBM noted that the organization has "direct ties to multiple national government networks," showing that the attackers had a sophisticated understanding of how to identify targets that could get them into many nations.

But other organizations were also targeted, from Taiwan and South Korea to Germany and Italy. Some were involved in the solar panel-driven cooling systems for the vaccine.
The attackers' emails were addressed to companies that provide key components of the cold chain process. Those include ice-lined boxes for vaccines and the solar panels that can power refrigerated vaccine containers — an important feature in poor countries where electricity can be scarce.

The researchers said the effort seemed aimed at stealing credentials that could have ultimately led the attackers to a trove of information, including timetables for vaccine distribution, lists of vaccine recipients and where doses are being shipped.

IBM could not determine whether the attacks were successful, the company said. The researchers said the attackers targeted one Gavi program started in 2015, before the advent of the coronavirus, to upgrade cold chain equipment for vaccines in dozen of nations.

UNICEF, which is planning vaccine delivery for poorer countries, appears to have been another target. Najwa Mekki, a spokeswoman for the organization, said the IBM researchers alerted officials to the threat to the cold chain system, and "we notified our supply networks and alerted relevant teams to the need to increase vigilance."

There is no indication so far that the attackers were aiming at Pfizer or Moderna, whose vaccines are expected to be the first ones approved for emergency use in the United States. A spokeswoman for Pfizer said Wednesday that the company's cold storage equipment was designed by security-conscious experts and custom-built to match the specific requirements of Pfizer's vaccine, which must be stored at extremely cold temperatures.

David E. Sanger and Sharon LaFraniere - The New York Times