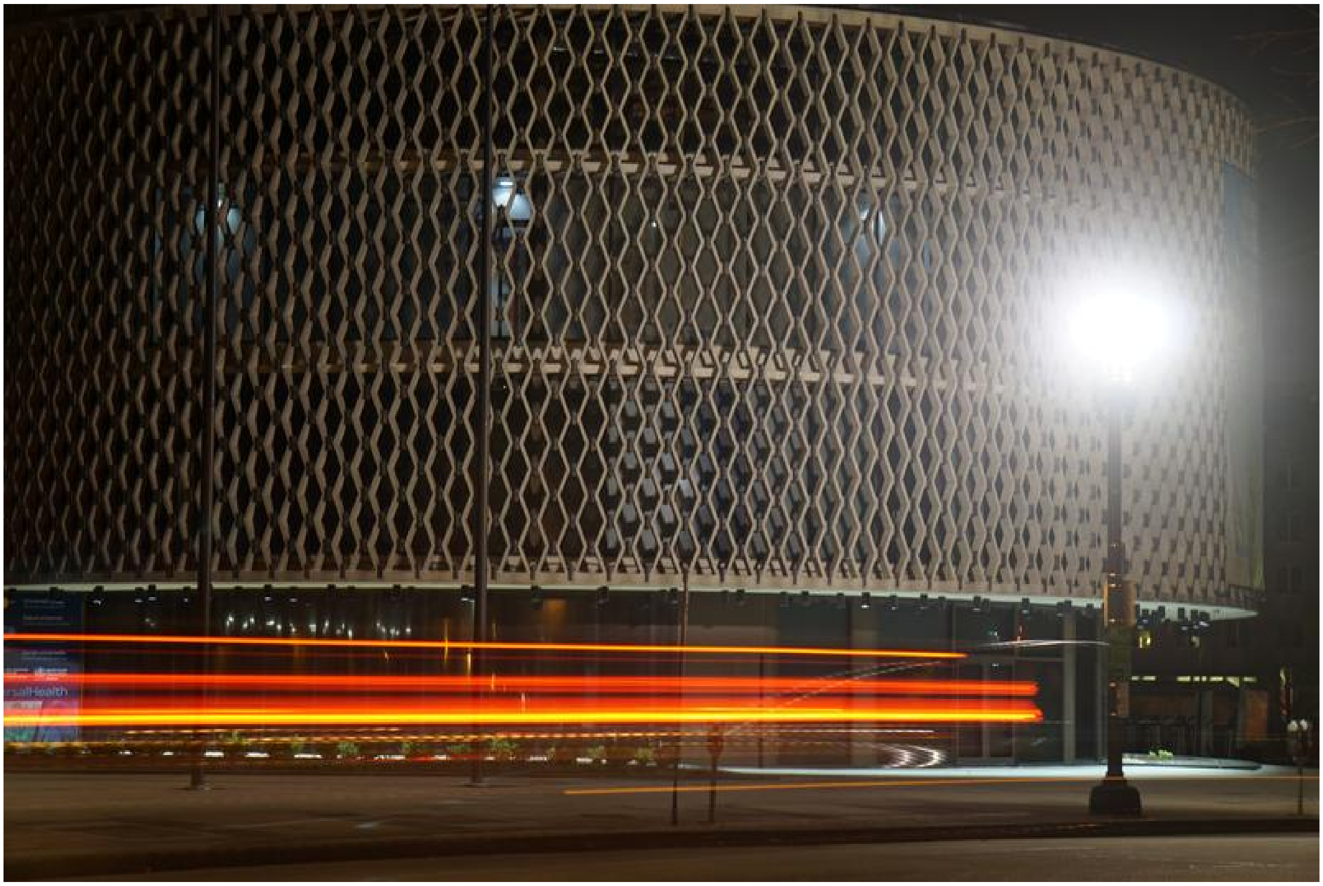
Exclusive: Elite hackers target WHO as coronavirus cyberattacks spike

reuters.com/article/us-health-coronavirus-who-hack-exclusive/exclusive-elite-hackers-target-who-as-coronavirus-cyberattacks-spike-idUSKBN21A3BN

Raphael Satter, Jack Stubbs, Christopher Bing



U.S. Legal News
Updated

By Raphael Satter, Jack Stubbs, Christopher Bing

4 Min Read

WASHINGTON/LONDON (Reuters) - Elite hackers tried to break into the World Health Organization earlier this month, sources told Reuters, part of what a senior agency official said was a more than two-fold increase in cyberattacks.

Traffic passes the Regional Office for the Americas of the World Health Organization (WHO) during the coronavirus disease (COVID-19) outbreak in Washington, D.C., U.S. March 22, 2020. REUTERS/Raphael Satter

WHO Chief Information Security Officer Flavio Aggio said the identity of the hackers was unclear and the effort was unsuccessful. But he warned that hacking attempts against the agency and its partners have soared as they battle to contain the coronavirus, which has killed more than 15,000 worldwide.

The attempted break-in at the WHO was first flagged to Reuters by Alexander Urbelis, a cybersecurity expert and attorney with the New York-based Blackstone Law Group, which tracks suspicious internet domain registration activity.

Urbelis said he picked up on the activity around March 13, when a group of hackers he'd been following activated a malicious site mimicking the WHO's internal email system.

"I realized quite quickly that this was a live attack on the World Health Organization in the midst of a pandemic," he said.

Urbelis said he didn't know who was responsible, but two other sources briefed on the matter said they suspected an advanced group of hackers known as DarkHotel, which has been conducting cyber-espionage operations since at least 2007.

Messages sent to email addresses maintained by the hackers went unreturned.

When asked by Reuters about the incident, the WHO's Aggio confirmed that the site spotted by Urbelis had been used in an attempt to steal passwords from multiple agency staffers.

"There has been a big increase in targeting of the WHO and other cybersecurity incidents," Aggio said in a telephone interview. "There are no hard numbers, but such compromise attempts against us and the use of (WHO) impersonations to target others have more than doubled."

The WHO published an alert last month - available here here - warning that hackers are posing as the agency to steal money and sensitive information from the public.

And government officials in the United States, Britain and elsewhere have issued cybersecurity warnings about the dangers of a newly remote workforce as people disperse to their homes to work and study because of the coronavirus pandemic.

The motives in the case identified by Reuters aren't clear. United Nations agencies, the WHO among them, are regularly targeted by digital espionage campaigns and Aggio said he did not know who precisely at the organization the hackers had in their sights.

Cybersecurity firms including Romania's Bitdefender and Moscow-based Kaspersky said they have traced many of DarkHotel's operations to East Asia - an area that has been particularly affected by the coronavirus. Specific targets have included government employees and business executives in places such as China, North Korea, Japan, and the United States.

Costin Raiu, head of global research and analysis at Kaspersky, could not confirm that DarkHotel was responsible for the WHO attack but said the same malicious web infrastructure had also been used to target other healthcare and humanitarian organizations in recent weeks.

“At times like this, any information about cures or tests or vaccines relating to coronavirus would be priceless and the priority of any intelligence organization of an affected country,” he said.

Officials and cybersecurity experts have warned that hackers of all stripes are seeking to capitalize on international concern over the spread of the coronavirus.

Urbelis said he has tracked thousands of coronavirus-themed web sites being set up daily, many of them obviously malicious.

“It’s still around 2,000 a day,” he said. “I have never seen anything like this.”

Additional reporting by Hyonhee Shin in Seoul; Editing by Chris Sanders and Edward Tobin