forbes.com

‘Elite Hackers’ Thought Behind Cyber Attack On World Health Organization

Davey Winder

3–4 minutes

World Health Organization targeted by suspected 'elite hackers' in the midst of this pandemic

NurPhoto via Getty Images

The World Health Organization (WHO) plays a vital role during the coronavirus pandemic. Abhorrent hackers don't give two hoots as cyber attacks against the WHO double.

The World Health Organization is a vital hub for advice, research, factual reports and response coordination during the coronavirus pandemic. That it should be the target of cyber attacks during a time of crisis is, frankly, reprehensible. The fact that those attacks have more than doubled, according to World Health Organization CISO, Flavio Aggio, more so. One such attack is thought to have been carried out by a group of elite hackers, an advanced persistent threat (APT) actor called DarkHotel that has been in the business of cyber-espionage for more than a decade. Reuters has reported that the attempt to steal passwords belonging to WHO agency staff was first spotted March 13 by Blackstone Law Group cybersecurity expert, Alexander Urbelis. "I realized quite quickly that this was a live attack on the World Health Organization," Urbelis told Reuters, "in the midst of

a pandemic."

Is the DarkHotel APT group behind the WHO cyber attack?

The attack seems to have started when hackers, thought to be DarkHotel by anonymous sources briefed by Reuters regarding the matter but not confirmed by Urbelis, established a fake site that impersonated the internal email system used by the WHO. This site went live on March 13, but Urbelis was already tracking the hackers and their domain registration patterns. The unsuccessful password-stealing attack itself was confirmed by Aggio in a conversation with Reuters reporters.

The same web infrastructure has, however, been spotted by security researchers at Kaspersky, targeting healthcare and humanitarian agencies recently. As global law enforcement agencies combine to thwart the criminals exploiting the pandemic, with 121 arrests and 37 criminal groups disrupted in just one recent operation against fake COVID-19 'cure' sellers, so cybercriminals continue

to ramp up their despicable actions. I've already reported, just this week, about a medical facility on standby to test COVID-19 vaccines that was hit by cyber-attackers who then published stolen data online.

Can technology companies and cybersecurity volunteers help protect the WHO?

I've also reported that cybersecurity volunteers such as CV19 are offering help to healthcare organizations in the fight against such opportunistic criminals. As Jake Moore, a cybersecurity specialist at ESET, said: "Cybercriminals show no ethical boundaries and will continue to attack wherever there could be a vulnerability." With the WHO playing a vital role in the fight against the coronavirus pandemic, a successful attack that took its online capability down could potentially lead to the crisis lasting longer and so put lives at risk. "

Large technology companies sharing technologies

at a time like this will help protect lives," Moore said, "this approach could, in fact, pave the way to a better future in security."

Follow me on Twitter or LinkedIn. Check out my website or some of my other work here.