Why Did Iran Hack the Computers of the Company That Has Come Up with Drug to Treat Coronavirus?

by Hugh Fitzgerald

Gilead is the American company with an Israeli-sounding name that has come up with an antiviral drug to treat coronavirus, remdesivir, that in clinical trials accelerated the recovery of patients with severe cases of coronavirus. It is now being given to select patients in this country. The company has just recently been the target of Iranian hackers. Their success is unknown. But a question remains: why did those Iranians choose to target Gilead?

The story, from Reuters, is here:

> *Hackers linked to Iran have targeted staff at US drugmaker Gilead Sciences Inc in recent weeks, according to publicly-*

available web archives reviewed by Reuters and three cybersecurity researchers, as the company races to deploy a treatment for the COVID-19 virus.

In one case, a fake email login page designed to steal passwords was sent in April to a top Gilead executive involved in legal and corporate affairs, according to an archived version on a website used to scan for malicious web addresses. Reuters was not able to determine whether the attack was successful.

Ohad Zaidenberg, lead intelligence researcher at Israeli cybersecurity firm ClearSky, who closely tracks Iranian hacking activity and has investigated the attacks, said the attempt was part of an effort by an Iranian group to compromise email accounts of staff at the company using messages that impersonated journalists.

Two other cybersecurity researchers, who were not authorized to speak publicly about their analysis, confirmed that the web domains and hosting servers used in the hacking attempts were linked to Iran.

Iran's mission to the United Nations denied any involvement in the attacks. "The Iranian government does not engage in cyber warfare," said spokesman Alireza Miryousefi. "Cyber activities Iran engages in are purely defensive and to protect against further attacks on Iranian infrastructure."…

Reuters has reported in recent weeks that hackers with links to Iran and other groups have also attempted to break into the World Health Organization….

The hacking infrastructure used in the attempt to compromise the Gilead executive's email account has previously been used in cyberattacks by a group of suspected Iranian hackers known as "Charming Kitten," said Priscilla Moriuchi, director of strategic threat development at US cybersecurity firm Recorded Future, who reviewed the web archives identified by

> *Reuters.*
>
> *Access to even just the email of staff at a cutting-edge Western pharmaceutical company could give … the Iranian government an advantage in developing treatments and countering the disease," said Moriuchi, a former analyst with the US National Security Agency….*

All the evidence, from many different cybersecurity experts (Ohad Zaidenberg, Priscilla Moriuchi, two others who were not allowed to be publicly identified) points to Iranian hackers. The web domains and hosting servers used in the hacking attempts had previously been linked to Iran. "The hacking infrastructure used in the attempt to compromise the Gilead executive's email account has previously been used in cyberattacks by a group of suspected Iranian hackers known as 'Charming Kitten,'" according to Moriuchi. Of course Iran's U.N. mission denied any involvement: "The Iranian government does not engage in cyber warfare," said spokesman Alireza Miryousefi. Some, familiar with the long litany of lies coming from Iran, might even conclude that *because of that denial*, we know Iran was behind it.

What were they looking for? They wanted to find out everything they could about Gilead's therapeutic drug remdesivir: what it is made from, and how it is made, and what its efficacy has been, and how easy it might be to copy, and what potential problems arise from its use.

Iranian hackers are hoping, ideally, to be able to steal this knowledge, and not only from Gilead but from every research laboratory now at work on coronavirus vaccines and therapies, and to replicate – and proudly claim as Iran's achievement – whatever they manage to steal. It's a question of Iranian, and Muslim pride. How infuriating it must be to the Iranians that it is almost always Western countries, and often in absurdly creative Israel, that medical advances of every kind have been

and are being made. But from the Muslim states there are no such advances, not in medicine, and not in any other scientific field. Tehran wants to change that. But it knows only one way to ensure success – through theft of intellectual property. What better way to earn admiration and prestige for Iran and, by extension, for the entire Muslim world, that suffers from a (well-deserved) inferiority complex, than to come up with a vaccine, or treatments, for coronavirus? How deeply disturbing and even disorienting it must be for Muslims to know that they are the "best of peoples" and yet it is the Infidels, who are "the most vile of created beings," who are responsible for all the major breakthroughs in medicine.

Iranian hackers chose Gilead as their first target because in clinical trials, its drug remdesivir performed best in accelerating recovery from advanced coronavirus, and is already being used on American patients. They may have thought – not necessarily correctly – that it is the therapeutic drug farthest along in development. And remdesivir had Dr. Fauci's cautious endorsement. A good place for Iran to start stealing. But what would be most satisfying for the Iranian hackers would be to steal not a therapeutic drug, but a vaccine and, especially, a vaccine being developed by the talented and hated Israelis. Iran could even jump the gun and make the announcement of upcoming clinical trials prematurely, in order to establish priority for "its" vaccine. For the Israelis will be more scrupulous, and take more time to ensure patient safety before starting such trials. What a thrill for the Supreme Leader to announce that this "Iranian" vaccine, "which will save the lives of billions of people all over the world," is now ready for clinical trials. And Iran will have previously announced that for months it had been detecting attempts by Israeli hackers on its medical personnel and projects, which would explain the copycat vaccine that Israel announces shortly after Iran does.

Many people will be properly scornful of Iran's claim, just as

they were when in mid-April, the Islamic Revolutionary Guards Corps (IRGC) unveiled what it described as a new technology, which it claimed could detect people within a 100-metre radius carrying the coronavirus and diagnose it within seconds. Pathetic, yes. Absurd, of course. But how many people in the infinitely credulous Muslim world believed it? And how many Muslims would leap at the chance to believe – "please Allah, please let it be us, the best of peoples" – that Muslims had saved the world from the coronavirus?

First published in