Sweden drops Russian hacking investigation due to legal complications

therecord.media/sweden-drops-russian-hacking-investigation-due-to-legal-complications/

April 13, 2021

The Swedish government dropped today its investigation into the 2017 hack of its sports authority, citing the legal constraints that would have prevented prosecutors from charging the Russian hackers responsible for the intrusion, which officials claimed were mere pawns operating on behalf of a “foreign power.”

This marks the first time that such a legal clause is cited by prosecutors investigating cyber-espionage hacking groups.

SSC hack part of Russia’s anti-WADA campaign

Today’s statement from the Swedish Prosecution Authority also marks the first time that Swedish officials formally blamed the Russian government for the 2017 hack of the Swedish Sports Confederation (SSC).

Citing a recently-concluded investigation from the Swedish Security Service, which also involved foreign intelligence services, Swedish prosecutors said that one of Russia’s military hacker groups breached its sports body between December 2017 and May 2018 and stole medical records for Swedish athletes.

“The investigation shows that the Russian military intelligence, **GRU** who, via its **85th Center**, also known as **unit 26165**, has planned and carried out the serious breaches of data secrecy against the Swedish Sports Confederation,” public prosecutor Mats Ljungqvist said today.

Ljungqvist said the SSC hack was part of a larger Russian hacking campaign that targeted sports bodies all over the world, including national and international anti-doping organizations such as WADA, USADA, and FIFA.

Russian military hackers stole athletes’ medical records and then published the information online.

Posing as a hacktivist group, the Russian hackers claimed they were exposing a secret conspiracy in sporting federations across the world that allowed certain professional athletes to take doping substances using medical conditions as an excuse.

“The information has been published openly and, based on these details, Swedish media have written articles which follow GRU’s narrative of discrediting athletes and sports organisations in the West,” Ljungqvist said.

But the hacking campaign was later exposed as a Russian influence operation orchestrated by the Russian government through its GRU service as revenge after Russian athletes had been banned from the Rio Olympics after a whistleblower exposed a Russian state-backed doping program in a 2014 ARD documentary.

Sweden says there’s no legal background to prosecute state hackers

The hacks touched many countries around the world, and the US Department of Justice filed legal charges against seven GRU intelligence service members in October 2018.

But Ljungqvist said today that Swedish authorities wouldn’t be following the US lead’s on this case, citing that the hackers acted on behalf of “a foreign power.”

As such, Ljungqvist says there is no legal backing to support Swedish authorities in charging the hackers and requesting their extradition to face charges for their crimes.

This marks the first time that a country claims it can’t file charges against hackers acting on behalf of a government due to a lack of legal background.

Until now, countries like Germany and the US are the only ones who formally charged Russian state hackers for intrusions carried out against their networks. Countries like the UK, Australia, New Zealand, Canada, and Norway have blamed Russian state hackers for attacks against their infrastructure but have not yet formally filed charges against specific individuals.

Smart political maneuver on the part of Swedish officials

In an online conversation today, Stefan Soesanto, Senior Cyber Defence Researcher at the Center for Security Studies at the Swiss Federal Institute of Technology (ETH) in Zurich, told *The Record* that he agreed with the Swedish government's decision.

"The way I interpret Ljungqvist announcement is that simply because the GRU (i.e., a foreign power) conducted the operation, there is (a) a zero chance of success for requesting extradition of the GRU operators from Moscow so they can be prosecuted on Swedish soil. And (b) there is literally zero chance that the Russian public prosecutor will open up a case and charge the GRU operatives if the Swedish Sports Confederation (or the Swedish government) goes to court in Russia," Soesanto told us.

> In that sense all the legal avenues for successfully prosecuting the GRU operators are non-existent.
>
> *Stefan Soesanto, Senior Cyber Defence Researcher at the Center for Security Studies at the Swiss Federal Institute of Technology (ETH) in Zurich*

"In my opinion that is a very realistic assessment by Ljungqvist, which also additionally helps the Swedish government to avoid unnecessary political confrontation with Moscow over an incident that happened four years ago," Soesanto added.

"Granted, the Swedes could have gone the US and German route, but then again, those approaches have not resulted in the successful extradition and prosecution of GRU operators either."

Article updated with comments from Mr. Soesanto.

Tags

- APT
- GRU
- hacking
- legal
- nation-state
- Russia
- Sweden

Catalin Cimpanu is a cybersecurity reporter for The Record. He previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.