

# Investigation of Russian hack on London hospitals may take weeks amid worries over online data dump

June 22 2024, by Pan Pylas

---



Credit: CC0 Public Domain

An investigation into a ransomware attack earlier this month on London hospitals by the Russian group Qilin could take weeks to complete, the

country's state-run National Health Service said Friday, as concerns grow over a reported data dump of patient records.

Hundreds of operations and appointments are still being canceled more than two weeks after [the June 3 attack on NHS provider Synnovis](#), which provides pathology services primarily in southeast London.

The attack affected King's College and Guy's and St Thomas' hospital trusts, which run several south London hospitals, as well as clinics and doctors' practices across a swath of the city. A memo to staff called it a "critical incident" and said it had a "major impact" on services, particularly blood transfusions.

NHS England said Friday that it has been "made aware" that data connected to the attack have been published online. According to the BBC, Qilin shared almost 400GB of data, including patient names, dates of birth and descriptions of blood tests, on their darknet site and Telegram channel.

"The National Crime Agency and National Cyber Security Centre are working to verify the data included in the published files as quickly as possible," NHS England said in a statement. "These files are not simple uploads and so investigations of this nature are highly complex and can take weeks if not longer to complete."

According to Saturday's edition of the Guardian newspaper, records covering 300 million patient interactions, including the results of blood tests for HIV and cancer, were stolen during the attack.

A website and helpline has been set up for patients affected.

"We understand the distress this will cause patients who have to re-test," NHS England said.

The National Crime Agency has confirmed that it is leading the [criminal investigation](#) but said it is unable to comment further.

Ransomware involves criminals paralyzing computer systems with malware, then demanding money to release them. Ransomware is the costliest and most disruptive form of cybercrime, affecting [local governments](#), court systems, hospitals and schools as well as businesses. It is difficult to combat as most gangs are based in former Soviet states and out of reach of Western justice.

Britain's state-funded health system has been hit before, including during a 2017 [ransomware attack](#) that froze computers at hospitals across the country, closing down wards, shutting emergency rooms and bringing treatment to a halt.

Qilin, also known as Agenda, advertises on dark web cybercrime forums and leases malware to affiliates who use it to conduct attacks for a percentage of ransom payments, said Louise Ferrett of Searchlight Cyber, a threat intelligence company. The group has listed more than 100 victims.

© 2024 The Associated Press. All rights reserved. This material may not be published, broadcast, rewritten or redistributed without permission.

Citation: Investigation of Russian hack on London hospitals may take weeks amid worries over online data dump (2024, June 22) retrieved 28 June 2024 from <https://techxplore.com/news/2024-06-russian-hack-london-hospitals-weeks.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.