INC Ransom threatens to leak 3TB of NHS Scotland stolen data

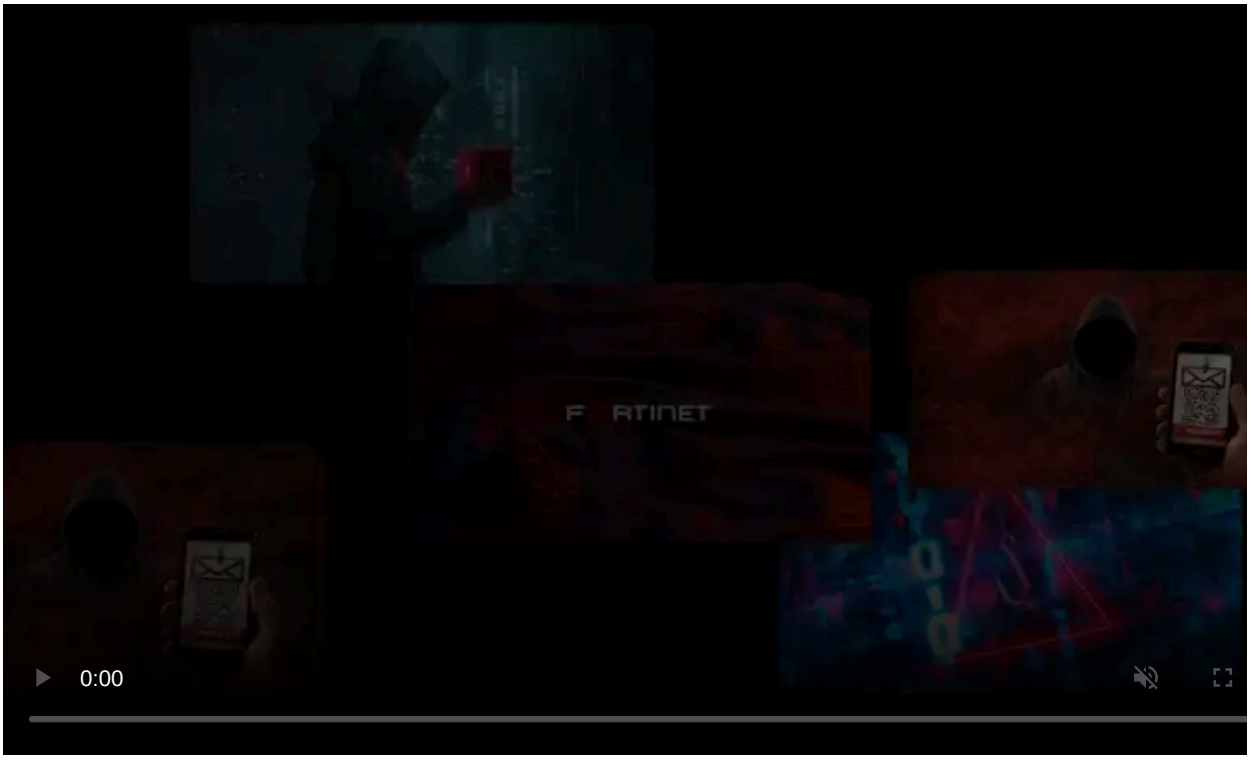
By Bill Toulas

Published: 2024-03-27 · Archived: 2026-04-05 21:45:25 UTC

The INC Ransom extortion gang is threatening to publish three terabytes of data allegedly stolen after breaching the National Health Service (NHS) of Scotland.

In a post yesterday, the cybercriminals shared multiple images containing medical details and said that they would leak data "soon," unless the NHS pays a ransom.

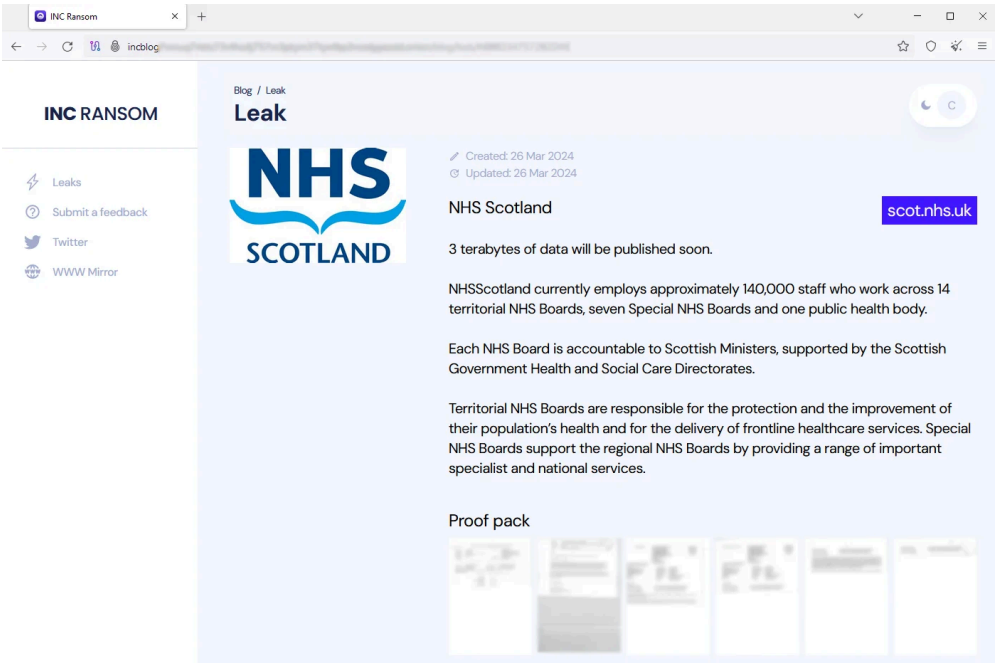
Scotland's NHS is the country’s public health system, providing services ranging from primary care, hospital care, dental care, pharmaceutical, and long-term care.


F RTINET
0:00

INC Ransom is a data extortion operation that emerged in July 2023 and targets organizations in both the public and the private sector. Among the victims are education, healthcare, and government organizations, and industrial entites like Yamaha Motor.

Reports about a cybersecurity incident disrupting NHS Scotland services appeared on March 15, likely when the attack occurred.

In yesterday's post, the threat actor published several sample documents with sensitive information about doctors and patients, including medical assessments, analysis results, and psychological reports.



INC Ransom extortion page *(BleepingComputer)*

Only one regional health board affected

A spokesperson for the Scottish Government told BleepingComputer that the cyberattack impacts only NHS Dumfries and Galloway, one of the regional health boards that make up NHS Scotland.

"We are aware of some data published on the web that is linked to the recent cyber-attack on NHS Dumfries and Galloway. This incident remains contained to NHS Dumfries and Galloway and there have been no further incidents across NHS Scotland as a whole," - Scottish Government

The spokesperson added that the government is working with multiple entities, including the health board, Police Scotland and other agencies (e.g. National Crime Agency, National Cyber Security Centre) to determine the impact of the breach "and the possible implications for individuals concerned."

Meanwhile, NHS Dumfries and Galloway has confirmed today that a ransomware group leaked clinical data relating to a small number of patients.

The organization states that this was the result of the cyberattack that occurred two weeks ago, which compromised its IT systems and resulted in the unauthorized access of “a significant amount of data including patient and staff-identifiable information.”

“We absolutely deplore the release of confidential patient data as part of this criminal act,” stated NHS Dumfries and Galloway Chief Executive Jeff Ace.

“This information has been released by hackers to evidence that this is in their possession.”

Ace said that patient-facing services are operating normally, and the organization is working with the police and the National Cyber Security Center (NCSC) to formulate a response to the situation.

Moreover, he assured that all patients who had their info leaked online will be informed directly by the NHS so they may take the appropriate measures to protect themselves.

Source: https://www.bleepingcomputer.com/news/security/inc-ransom-threatens-to-leak-3tb-of-nhs-scotland-stolen-data/