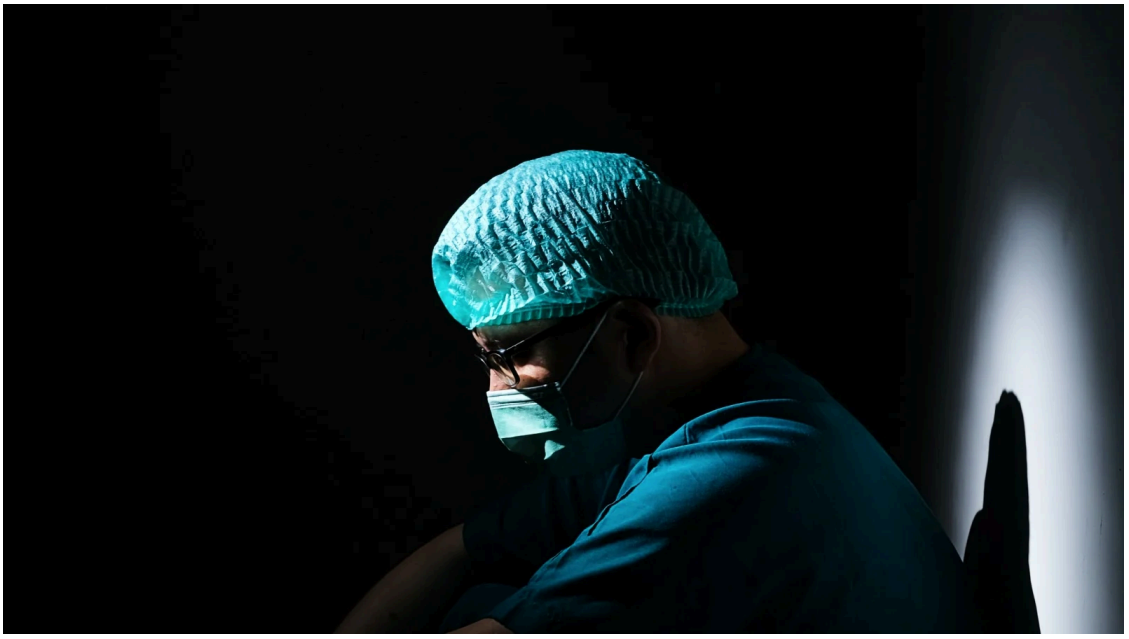
Ireland's Health Services hit with $20 million ransomware demand

By Lawrence Abrams

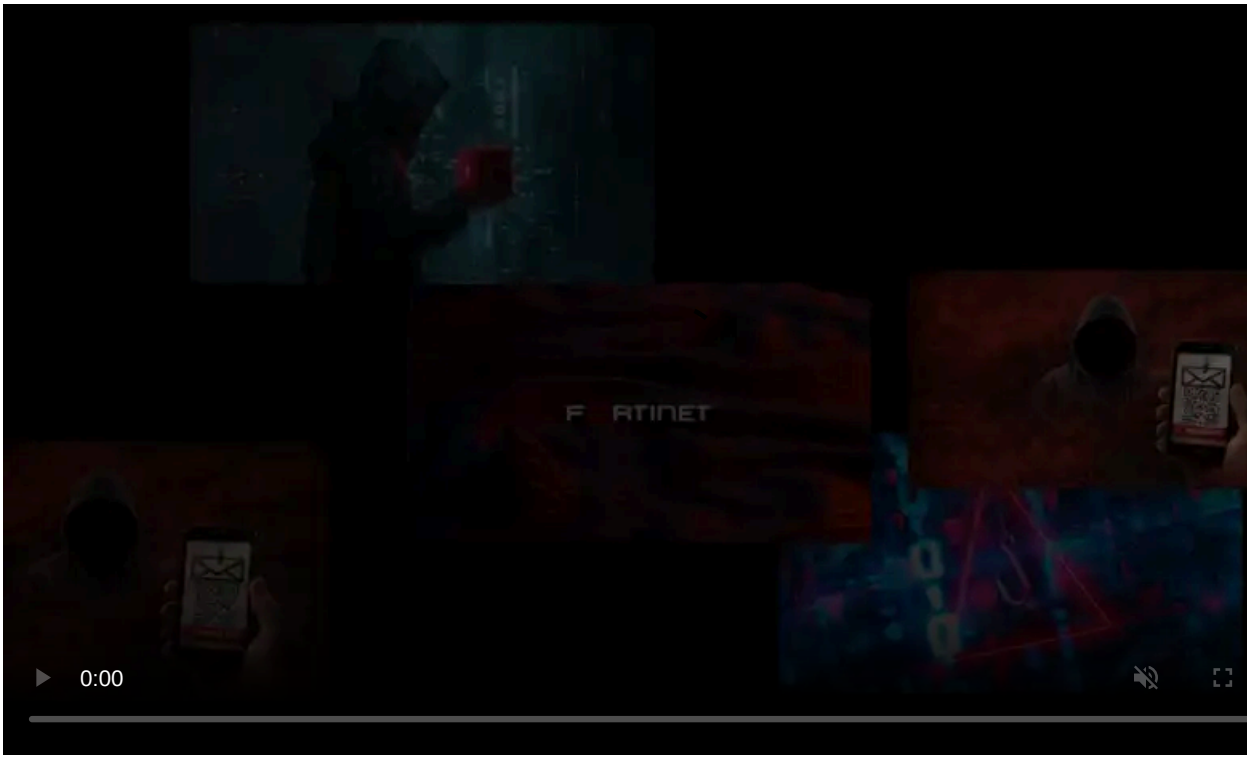
Published: 2021-05-15 · Archived: 2026-04-05 20:44:33 UTC



Ireland’s health service, the HSE, says they are refusing to pay a $20 million ransom demand to the Conti ransomware gang after the hackers encrypted computers and disrupted health care in the country.

Ireland's Health Service Executive (HSE), the country's publicly funded healthcare system, shut down all of their IT systems on Friday after suffering a Conti ransomware attack.

"We have taken the precaution of shutting down all our IT systems in order to protect them from this attack and to allow us fully assess the situation with our own security partners," the Irish national health service said.


F RTINET
0:00

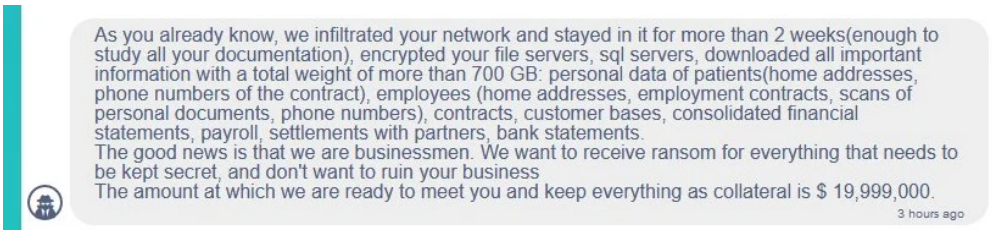
This IT outage has led to widespread disruption in the country's healthcare, causing limited access to diagnostics and medical records, transcription errors due to handwritten notes, and slow response times to healthcare visits.

Hackers demand a $20 million ransom

Yesterday, a cybersecurity researcher shared a screenshot of a chat between Conti and Ireland's HSE with BleepingComputer.

In the screenshot, the Conti gang claims to have had access to the HSE network for two weeks. During this time, they claim to have stolen 700 GB of unencrypted files from the HSE, including patient info and employee info, contracts, financial statements, payroll, and more.

Conti further stated that they would provide a decryptor and delete the stolen data if a ransom of $19,999,000 is paid to the threat actors.



Conti ransomware demands of HSE

BleepingComputer was also told that the threat actors shared a sample of stolen documents in the chat. However, BleepingComputer did not receive these documents and cannot confirm if they contain legitimate data belonging to the HSE.

In a press statement yesterday, Taoiseach Micheál Martin, the Prime Minister of Ireland, said that they would not be paying any ransom.

Who are Conti?

The Conti ransomware operation is believed to be run by a Russia-based cybercrime group known as Wizard Spider.

This group uses phishing attacks to install the TrickBot and BazarLoader trojans that provide remote access to the infected machines.

Using this remote access, the threat actors spread laterally through a network while stealing credentials and harvesting unencrypted data stored on workstations and servers.

Once the hackers have stolen everything of value and gained access to Windows domain credentials, they wait for a quiet time during the week and deploy the ransomware on the network to encrypt all of its devices.

The Conti gang then uses the stolen data as leverage to force a victim into paying a ransom by threatening to release it on their ransom data leak site if they are not paid.

Other high-profile ransomware attacks conducted by Conti in the past include FreePBX developer Sangoma, IoT chip maker Advantech, Broward County Public Schools (BCPS), and the Scottish Environment Protection Agency (SEPA).
