Conti ransomware also targeted Ireland's Department of Health

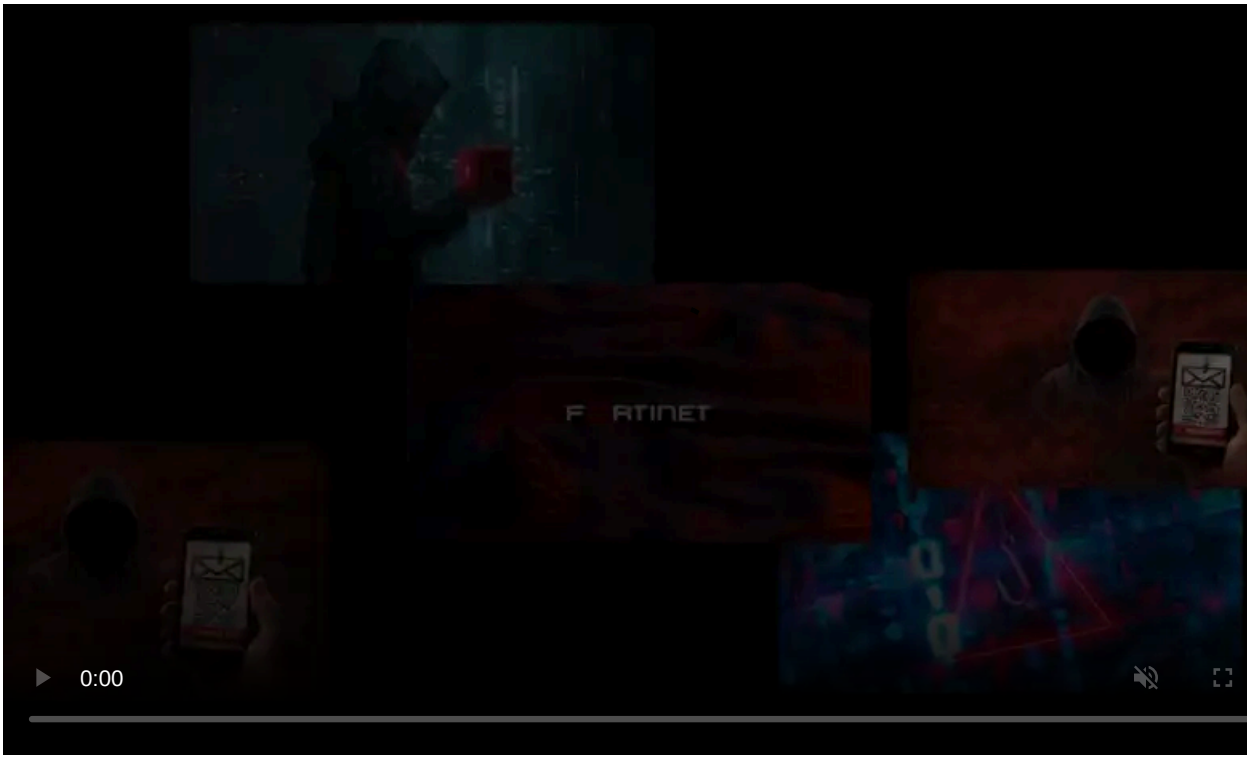
By Sergiu Gatlan

Published: 2021-05-17 · Archived: 2026-04-05 20:56:47 UTC

The Conti ransomware gang failed to encrypt the systems of Ireland's Department of Health (DoH) despite breaching its network and dropping Cobalt Strike beacons to deploy their malware across the network.

On the same day, Conti operators breached the network of Ireland's Health Service Executive (HSE), the country's publicly funded healthcare system, and forced it to shut down all IT systems to contain the incident.

"The National Cyber Security Centre (NCSC) became aware on Thursday of an attempted cyber attack on the Department of Health," the Irish Department of the Environment, Climate and Communications said.


F RTINET
0:00

"This attempted attack remains under investigation, however there are indications that this was a ransomware attack similar to that which has affected the HSE."

Ransomware execution blocked

In a separate security advisory [PDF], NCSC provided more technical details on the attack and confirmed the link between the two incidents saying that the two "attacks are believed to be part of the same campaign targeting the Irish health sector."

The NCSC was alerted of potentially suspicious activity on the Department of Health's network on Thursday afternoon.

Investigators discovered Cobalt Strike beacons deployed on the network, a tool commonly used by ransomware gangs to deploy their malicious payloads and encrypt systems across the network.

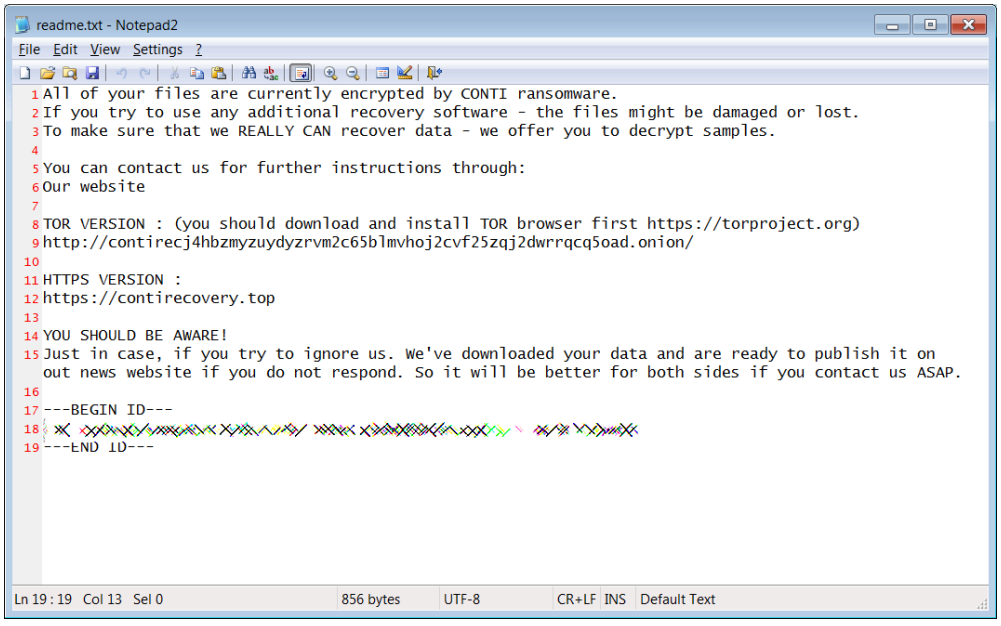
The next day, at 07:00 AM, a human-operated Conti ransomware attack disabled some of HSE's devices, forcing the health service to shut down its entire IT infrastructure to limit the impact.

Around the same time, a second Conti attack attempting to execute ransomware payloads to encrypt the systems of Ireland's Department of Health was blocked by anti-virus software and the tools deployed by investigators the day before.

'The Department of Health has implemented its response plan including the suspension some functions of its IT system as a precautionary measure," the Irish government added.

The NCSC also confirmed BleepingComputer's report that the ransomware sample used during these attacks appends the .FEEDC extension to encrypted files.

The NCSC also shared indicators of compromise [PDF] linked to the Conti ransomware attack on Ireland's health systems.



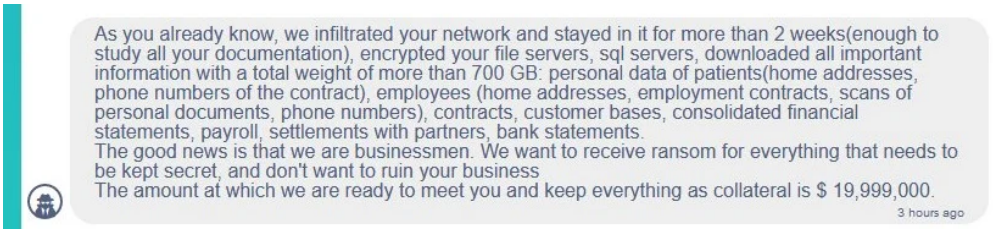
Conti HSE ransom note

HSE will not pay Conti's $20 million ransom

After the HSE ransomware incident, the Conti gang claimed to have had access to HSE's network for over two weeks and that they were able to steal 700 GB of unencrypted files, including employee and patient info, financial statements, payroll, contracts, and more.

They also said that HSE would need to pay a $19,999,000 ransom for Conti to delete all the stolen data from their servers and provide a decryptor.

Even though the incident has led to widespread disruption affecting Ireland's healthcare services, Taoiseach Micheál Martin, the Prime Minister of Ireland, said that the HSE would not be paying any ransom.



Conti ransomware's demands

Conti ransomware is a private Ransomware-as-a-Service (RaaS) operation believed to be run by a Russian-based cybercrime group known as Wizard Spider.

Conti shares code with the notorious Ryuk Ransomware, whose TrickBot-powered distribution channels they took over after Ryuk activity dwindled around July 2020.

Previously, Conti ransomware hit the Scottish Environment Protection Agency (SEPA), leaking roughly 1.2 GB of stolen data on their dark web leak site.
