Irish police seize Conti domains used in HSE ransomware attack

By Sabina Weston

Published: 2021-09-06 · Archived: 2026-04-05 19:45:37 UTC

Ireland's Garda National Cyber Crime Bureau has announced that it had "seized several domains" used in the ransomware attack on the Irish Health Service Executive (HSE) earlier this year.

The attack, which took place in mid-May, forced the national health and social services provider to shut down its entire IT system, which lead to appointments being delayed or cancelled. The Irish Department of Health was also targeted but managed to prevent Conti from encrypting its network.

On Sunday, almost four months after the attack, the Garda's cyber crime unit confirmed that it had disrupted the IT infrastructure of the Conti hacking group, which had claimed responsibility for the attack. Thought to be deployed by a Russian group known as Wizard Spider, Conti functions as a type of ransomware as a service (RaaS) operation.

"The Garda National Cyber Crime Bureau have seized several domains used in this and other ransomware attacks," a Garda spokesperson told *IT Pro*, adding that the seizure "has directly prevented a large number of further ransomware attacks across the world".

Latest Videos From IT Pro

The Bureau has also notified potential victims of the ransomware gang and is working with Europol and Interpol to ensure that other states are aware of the systems targeted by Conti.

RELATED RESOURCE

The ultimate law enforcement agency guide to going mobile

Best practices for implementing a mobile device program

FREE DOWNLOAD

A Garda spokesperson described the operation as “crime prevention”, adding that to date there had been “a total of 753 attempts (...) made by ICT systems across the world to connect to the seized domains”.

“In each instance, the seizure of these domains by the GNCCB investigation team is likely to have prevented a Conti Ransomware Attack on the connecting ICT system, by rendering the initially deployed malware on the victims system, as ineffective,” they said.

Sign up today and you will receive a free copy of our Future Focus 2025 report - the leading guidance on AI, cybersecurity and other IT challenges as per 700+ senior executives

HSE wasn’t the only healthcare provider targeted by the Conti ransomware group. Days after the attack was reported, the US Federal Bureau of Investigations (FBI) found that the gang had also attempted to breach 16 US services, including law enforcement agencies, 911 dispatch services and municipalities, with the attempted attacks all taking place since May 2020.

The FBI Cyber Division stated that the targeted healthcare and first responder networks were “among the more than 400 organisations worldwide victimised by Conti”, out of which “over 290” are based in the US.

Source: https://www.itpro.co.uk/security/ransomware/360786/irish-police-seize-conti-domains-used-in-hse-ransomware-attack