Irish health system struggling to recover from cyberattack

May 18 2021, by Sylvia Hui, Danica Kirka and Frank Bajak

A general view of St Luke's Hospital which has been affected by a ransomware attack, in Rathgar, Dublin, Saturday, May 15 2021. Ireland's health system is struggling to restore computers and treat patients four days after it shut down its entire information technology system in response to a ransomware attack. Authorities said hundreds of people were assigned to respond to the attack but it could be weeks before the public health service will return to normal. The chief clinical officer of Ireland's public health service said Tuesday, May 18 that the intrusion was having "a profound impact on our ability to deliver care" and that

disruptions would undoubtedly "mount in the coming days and weeks." Credit: Niall Carson/PA via AP

Ireland's health system struggled to restore computers and treat patients Tuesday, four days after it shut down its entire information technology system in response to a ransomware attack.

Thousands of diagnostic appointments, cancer treatment clinics and surgeries have been canceled or delayed since Friday's cyberattack. Authorities said hundreds of people were assigned to respond to the attack but it could be weeks before the public health service will return to normal.

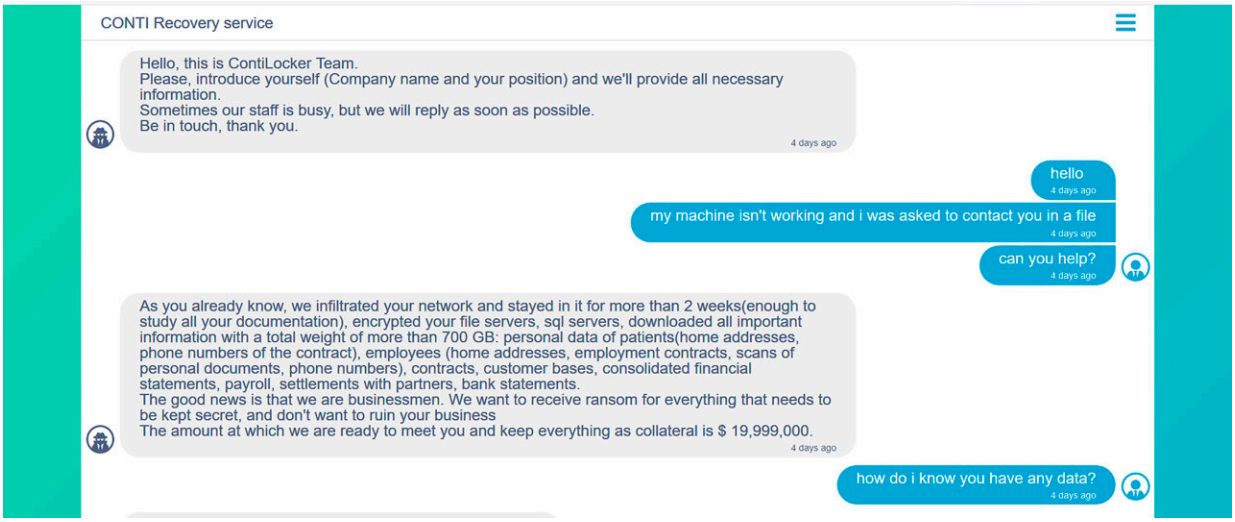
Irish Prime Minister Micheal Martin said the attack was a "heinous" one that targeted patients and "the Irish public." The chief clinical officer of Ireland's Health Service Executive, Colm Henry said the intrusion was having "a profound impact on our ability to deliver care" and that disruptions would undoubtedly "mount in the coming days and weeks."

More than 2,000 patient-facing IT systems were affected, and around 80,000 devices were linked to such systems throughout the health service, Henry told Irish broadcaster RTE. Authorities are prioritizing the recovery of systems involved in patient diagnostics, such as radiology, radiotherapy and maternity and newborn services.

"That's what our experts are focusing on this week, with external help, to ensure those services are not reliant on manual exchange of information," he said.

Ransomware attacks are typically carried out by criminal hackers who scramble data, paralyzing victims' networks, and demand a large

payment to decrypt the information. Irish officials say a ransom was demanded but they will not pay it.



Screenshot made on Tuesday May 18, 2021 showing part of the ransom negotiation page on the darknet site of Conti, a Russian-speaking ransomware group, demanding $20 million from Ireland's publicly funded health care system. Ireland's health system struggled to restore computers and treat patients Tuesday, four days after it shut down its entire information technology system in response to a ransomware attack by Conti. The gang had threatened on Monday to "start publishing and selling your private information very soon," if it did not receive the money. Credit: Photo via AP

Conti, a Russian-speaking ransomware group, was demanding $20 million, according to the ransom negotiation page on its darknet site viewed by The Associated Press. The gang threatened Monday to "start publishing and selling your private information very soon," if it did not receive the money.

"The government will not be paying any money," Justice Minister

Heather Humphreys told RTE. "We will not be blackmailed."

The Irish Association for Emergency Medicine urged people not to turn up at hospital emergency rooms unless they had a genuinely urgent need. The association said electronic ordering of blood tests, X-rays and scans was unavailable and clinicians had no access to previous X-rays or scan results.

Many hospital telephone systems also were not working because they are carried on computer networks, it added. The attack has also shut down the system used to pay health care workers.

Patients have expressed frustration at the attack, describing it as another torment thrown into the already difficult struggle accessing health care during the COVID-19 pandemic.

Eimear Cregg, 38, a primary school teacher who is receiving treatment for breast cancer, had her radiation therapy briefly postponed while doctors sought to restore her records so they could treat her properly.

A general view of the Naas General Hospital in County Kildare, Dublin, Saturday, May 15 2021. Ireland's health system is struggling to restore computers and treat patients four days after it shut down its entire information technology system in response to a ransomware attack. Authorities said hundreds of people were assigned to respond to the attack but it could be weeks before the public health service will return to normal. The chief clinical officer of Ireland's public health service said Tuesday, May 18 that the intrusion was having "a profound impact on our ability to deliver care" and that disruptions would undoubtedly "mount in the coming days and weeks." Credit: Niall Carson/PA via AP

"This is a very cruel thing to do to vulnerable people," Cregg told The Associated Press. "We're fighting every day as it is, and this was just another curve ball that wasn't needed."

Ireland's publicly funded health care system, the Health Service Executive, said in a statement late Monday that there were "serious concerns about the implications for patient care arising from the very limited access to diagnostics, lab services and historical patient records."

The health service said it was working methodically to assess and restore its computer systems.

The Ireland attack comes as ransomware gangs persist in identifying "big game" targets in search of lucrative payouts and data that can help them identify new victims—and even determine the amount of cyber-insurance coverage they carry.

Operations of four Asian affiliates of the Paris-based insurance company AXA were hit in recent days by by ransomware attacks: in Thailand, Malaysia, Hong Kong and the Philippines. The attackers claimed to have stolen 3 terabytes of data, including medical records, customer IDs and privileged communications with hospitals and doctors.

The hackers threatened to leak documents within 10 days if AXA does not pay an unspecified ransom.

In this Feb. 21, 2019, file photo, people stand in front of the logo of AXA Group prior to the company's 2018 annual results presentation, in Paris. The Thai affiliate of Paris-based insurance company AXA said Tuesday, May 18, 2021 it is investigating a ransomware attack by Russian-speaking cybercriminals that has affected operations in Thailand, Malaysia, Hong Kong and the Philippines. Credit: AP Photo/Thibault Camus, File

AXA said this month that it would stop writing cyber-insurance policies in France that reimburse customers for extortion payments made to ransomware criminals, saying the practice encourages more such attacks.

In a new case, ransomware took down IT systems across five hospitals south of Auckland, New Zealand, forcing staff to cancel some elective surgeries preventing doctors from accessing clinical records, authorities

said.

Ransomware attacks have surged in the past year, though there may be a dip following the worst attack to date on U.S. critical infrastructure. A nearly week-long shutdown of the Colonial Pipeline, which supplies the east coast with 45% of its petroleum products, led U.S. President Joe Biden to vow retaliation.

That prompted the moderator of one of the most popular darknet criminal forums, XS, to disavow ransomware syndicates and to ban them from recruiting and conducting other business on the forum. But experts say it's typical for criminals to lay low when law enforcement scrutiny gets acute.

Ransomware reached epidemic levels last year as the criminals, who enjoy safe harbor in former Soviet states, increasingly turned to "double extortion," stealing sensitive data before activating the encryption software that paralyzes networks—and threatening to dump it online if they don't get paid.