NEWS

NHS ransomware attack spreads worldwide

■ Cite as: *CMAJ* 2017 June 5;189:E786-7. doi: 10.1503/cmaj.1095434

A cyber-attack that affected more than 60 trusts within the United Kingdom's National Health Service (NHS) has spread to more than 200 000 computer systems in 150 countries, including Canada. One hospital in Ontario — Lakeridge Health in Oshawa — reported that its computer system was threatened by the ransomware. The hospital's antivirus software contained the threat, however, and patient care and access to health records were not affected.

Hospitals and general practitioners' offices in the UK were not as fortunate, however. On May 12, the "WannaCry" ransomware began affecting dozens of NHS facilities. Eventually, more than 60 NHS trusts were hit. Many facilities could not access patient records, which led to delays of non-urgent surgeries and cancelled patient appointments. Some hospitals had to divert ambulances to other facilities.

According to UK Health Secretary Jeremy Hunt, there has not been a second wave of attacks, and 80% of the NHS was unaffected. About 16 NHS trusts, however, were still affected on May 15. Patients have been advised to show up for appointments unless instructed otherwise.

Some commentators have been swift to blame the NHS for failing to invest in technology that could have prevented the attack. Although the NHS does not appear to have been specifically targeted by whoever is behind the WannaCry ransomware, it was vulnerable to attack because some of its Windows operating systems are more than 15 years old and were no longer updated or supported by Microsoft.

According to cyber-crime expert Charles Arthur, most NHS trusts spend a "paltry" amount each year on securing their computing systems, and some spend nothing at all. "All that made the events of the past few days a disaster waiting to happen," Arthur wrote in *The Guardian*, further suggesting that part of

kaptnali/iStock

Cyber attack on UK hospitals causes delayed surgeries and cancelled appointments.

the problem is that nobody, even those inside the NHS, will acknowledge the extent of their security issues.

Though this attack was the largest, many NHS facilities have been threatened by ransomware in recent years. According to Arthur, who is writing a book on hacking incidents like the WannaCry virus, 88 of the NHS' 260 trusts were hit by ransomware between mid-2015 and the end of 2016.

Since hitting the NHS on May 12, the WannaCry ransomware has spread rapidly, affecting many businesses around the world, including the shipping company FedEx. The virus is downloaded to a computer when a user clicks a link in an email or opens an attachment. Files on the computer are then encrypted and can only be unlocked if the user pays a ransom.

The party behind the WannaCry virus demanded US$300 in bitcoin to unlock each affected computer, with a doubling of the charge after three days, and the threat of all data being lost if payment was not received within a week. Cyber-crime experts warn against making such payments, saying there are no guarantees that users will regain access to their data if they pay up.

Nobody yet knows who is behind the attack. Some pointed fingers at Russia, but Russian President Vladimir Putin has denied any involvement. The technology required to create the virus appears to have been stolen by hackers from the United States National Security Agency. The spread of the virus was slowed, but not stopped, by the work of Marcus Hutchins, a 22-year-old self-taught cyber-security expert, who discovered a "kill switch" inside the virus.

Roger Collier, *CMAJ*