What accounts for the success of the WannaCrypt ransomware attack on Britain's National Health Service?

By Steve James
23 May 2017

Britain's National Health Service (NHS) was among the most high-profile and serious victims of the recent global WannaCrypt ransomware attack.

The malware illegally encrypted files on Windows desktop PCs and servers, based on a Windows-vulnerability. The worm arrived by email and, once installed, scanned accessible machines and copied itself to its new targets while encrypting files on the original host. PC users globally were presented with the now infamous ransom demand for $300 and the threat that their files would be deleted.

Within the NHS, WannaCrypt caused and continues to cause chaos. Doctors and medical staff in hundreds of hospitals and general practices reported that access to saved files was impossible. Patient records were unavailable, scans and X-rays could not be transferred from scanners, appointments could not be confirmed or altered. Staff resorted to written notes and their own mobile phones.

In all 47 NHS trusts in England and Wales, and 13 NHS bodies in Scotland were disrupted. Ambulances were turned away and operations cancelled at St Bartholomew's hospital in London. Appointments were also cancelled at Newham University Hospital and at Whipps Cross in the capital. Patients at Stoke and Stafford hospitals were told to avoid Accident and Emergency units unless absolutely necessary.

In Scotland, NHS Lanarkshire told patients to stay away from hospitals. Dumfries and Galloway shut down its services to general practices. Radiology for NHS Western Isles was affected. Three days after the May 12 attack, seven trusts were still reporting problems, while many doctor's surgeries were still unable to accessing patient records. Key equipment such as MRI scanners could take several weeks to restore.

During last year's recent junior doctors' dispute, Britain's right-wing media seized every opportunity to slander and misrepresent doctors seeking to defend their working conditions and health provision. Doctors were regularly denounced for "putting patients at risk." NHS employers accused doctors of "causing distress, delay and pain to our patients."

Remarkable then that over the past few days no similar denunciation was forthcoming of those who made possible the crisis provoked by the WannaCrypt worm, which caused intense distress and genuine risk for tens of thousands of NHS patients and greatly increased the workload for NHS workers.

Most fundamentally, Wannacrypt is based on "weaponised" software, codenamed Eternal Blue, originally developed by the US National Security Agency to disrupt and destabilise the computer systems of Washington's rivals and political opponents. The damage it did is therefore a byproduct of the NSA and Britain's GCHQ's illegal surveillance of the world's population, exposed by whistleblower Edward Snowden, done in the name of the so called "war on terror." The NSA has systematically collected vulnerabilities within operating systems and software in order to allow its spies to gain access to computers, networks and devices around the world.

Critical commentary has centred on the continued use of the Windows XP operating system within the NHS, and whether the British government had, or had not, provided cash to NHS trusts to upgrade to newer versions of Windows.

It has emerged that the Government Digital Service failed to extend a £5.5 million one-year support deal with Microsoft or to secure a replacement package. This is only one example of the impact of multi-billion pound

cuts being carried out by the Conservatives—in the name of "efficiency savings"—that are threatening the NHS with collapse.

But the fact that Tory cuts led to the extended use of Windows XP also points to the way major international conglomerates are able to exercise astonishing power over computer networks and data systems vital to the wellbeing of entire populations. The National Health Service is used by a population of no less than 60 million people.

Although Microsoft issued a patch earlier this year for the Eternal Blue vulnerability that WannaCrypt's authors exploited, it was only initially made available for the tech giant's latest operating systems. No patch was offered for Windows XP, which, although first released in 2001, is still widely used.

According to the *Digital Health* web site, "as many as 20 percent of NHS organisations could still be relying upon it as their primary operating system, and around 90 percent are thought to run something on it somewhere in the organisation..."

The affair also points to the way that IT companies have now joined with Big Pharma in milking billions out of publicly funded health care. Microsoft stopped updating and supporting XP in 2014 in order to force users onto its later and more lucrative operating systems. As a result, NHS XP users have been running with an insecure operating system. It was only after the WannaCrypt crisis that Microsoft belatedly issued a one-off patch for XP.

Microsoft's behaviour is comparable to that of the ransomware authors—save only that it is immeasurably more powerful and better organised.

This is only one aspect of the subordination of the NHS and public health care systems around the globe to private profit. For nearly two decades, IT services within the NHS have become the target of a gold rush for companies seeking to turn public health into a source of stable revenue streams for their shareholders. Much of this has centred on attempts to deploy an electronic records system which could safely, efficiently and securely allow full records for the millions of NHS users to be accessible from whichever hospital department or surgery the patient was currently attending. The result has instead been chaos, which increased vulnerability to attacks such as WannaCrypt.

In 2011, the Tory government finally abandoned a nine-year National Programme for IT in the NHS launched by the previous Labour government. A 2013 report concluded that the Lorenzo care records system, intended to cover all of England, was only going to be available for 22 of over 180 trusts. It described the project as "one of the worst and most expensive contracting fiascos in the history of the public sector."

One contract intended to cost £3.1 billion, with US IT services giant CSC, had spiraled to £9.8 billion. Despite the project's collapse, legal wrangles with CSC and rivals Fujitsu and Accenture are expected to continue for years. CSC also has contracts with the police, the Ministry of Defence, HM Passport Office and the Department of Work and Pensions. It recently announced its intention to lay off hundreds of its 5,500 UK-based staff.

In 2015, a poorly conceived NHS apps library was finally abandoned following reports of incorrect insulin doses and asthma readings being provided to patients. This year, personal details of 4,766 NHS staff, former staff and customers were stolen from IT contractor Landauer, which provides ionising radiation monitoring. Another report claimed that there had been as many as 140 data losses between January and April this year.

Ever larger amounts of NHS data are being hived off to the private sector. The Royal Free Hospital in London has negotiated a deal with Google's Deepmind project. Presented as a health care triumph, the deal was criticised for having provided "unexamined access to population-wide health datasets to 'private prospectors.'"

Nor are even paper records safe at the hands of the profiteers. Earlier this year, it was revealed that as many as 500,000 documents containing patient data, diagnosis and screening results had been dumped in a warehouse instead of being delivered. The NHS internal postal service was at the time run jointly by the Department of Health and private contractor Sopra Steria.