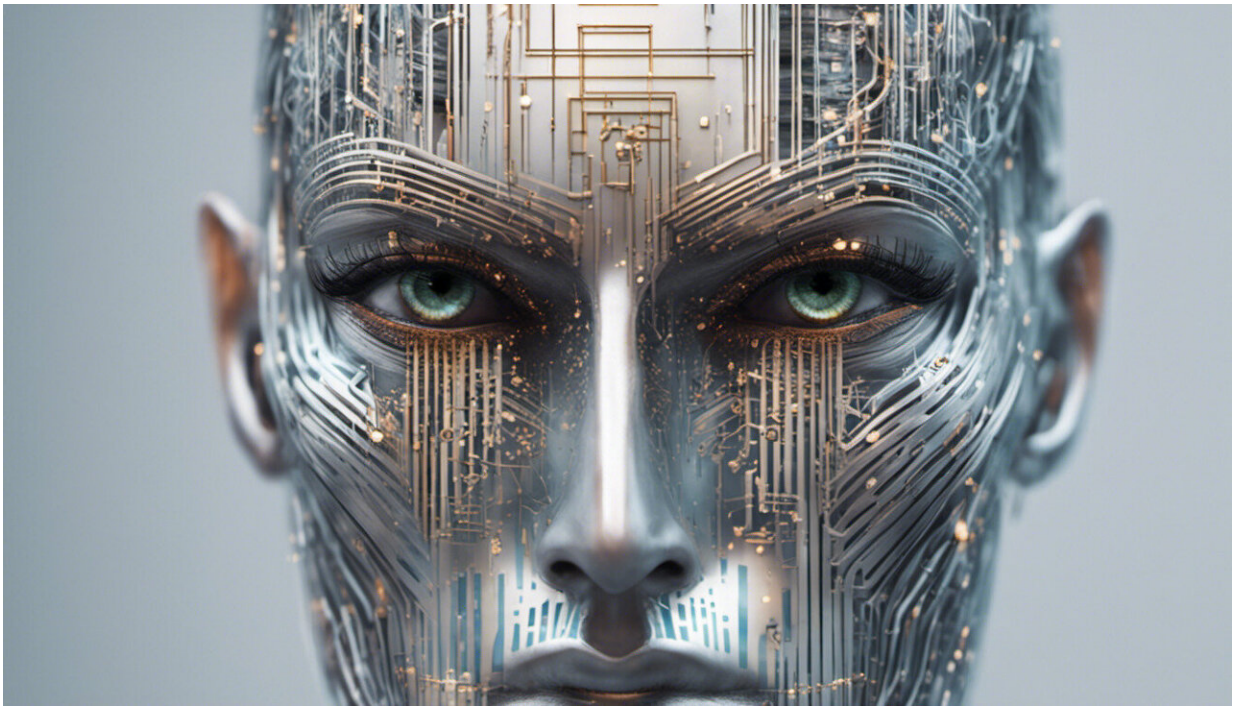
Why has healthcare become such a target for cyber-attackers?

July 18 2017, by Myrsini Athinaiou



Credit: AI-generated image (disclaimer)

More than 16m patient records were stolen from healthcare organisations in the US and related parties in 2016. That year, healthcare was the fifth most targeted industry when it came to cyber-attacks. And earlier this year, Britain's National Health Service was crippled by a ransomware attack that locked up the computers holding many of its

records and booking systems.

But it's not just health data and services that are at risk from cyber-attacks – it's also human lives. In 2007, the then US vice-president, Dick Cheney, had his implanted heart defibrillator modified in order to avoid "death by hacking", a technology weakness that US officials warned of again just recently. Any medical device connected to a network is potentially at risk from being taken over and exploited by hackers, from MRI machines to electric wheelchairs.

As connected technology becomes even more embedded in healthcare, this cyber-threat is only likely to grow. But if we want to protect our health from cyber-attacks, we shouldn't fear technology. Instead, we need to understand it better and realise that the threat becomes much worse when people make simple mistakes.

What is the risk to healthcare?

The most common cyber-threats to healthcare are data theft attacks. They typically start from something like a phishing attack. For example, if you are a doctor with access to patients' records, an attacker may send you an e-mail and convince you to click a link or attachment that downloads a piece of software known as malware to your computer.

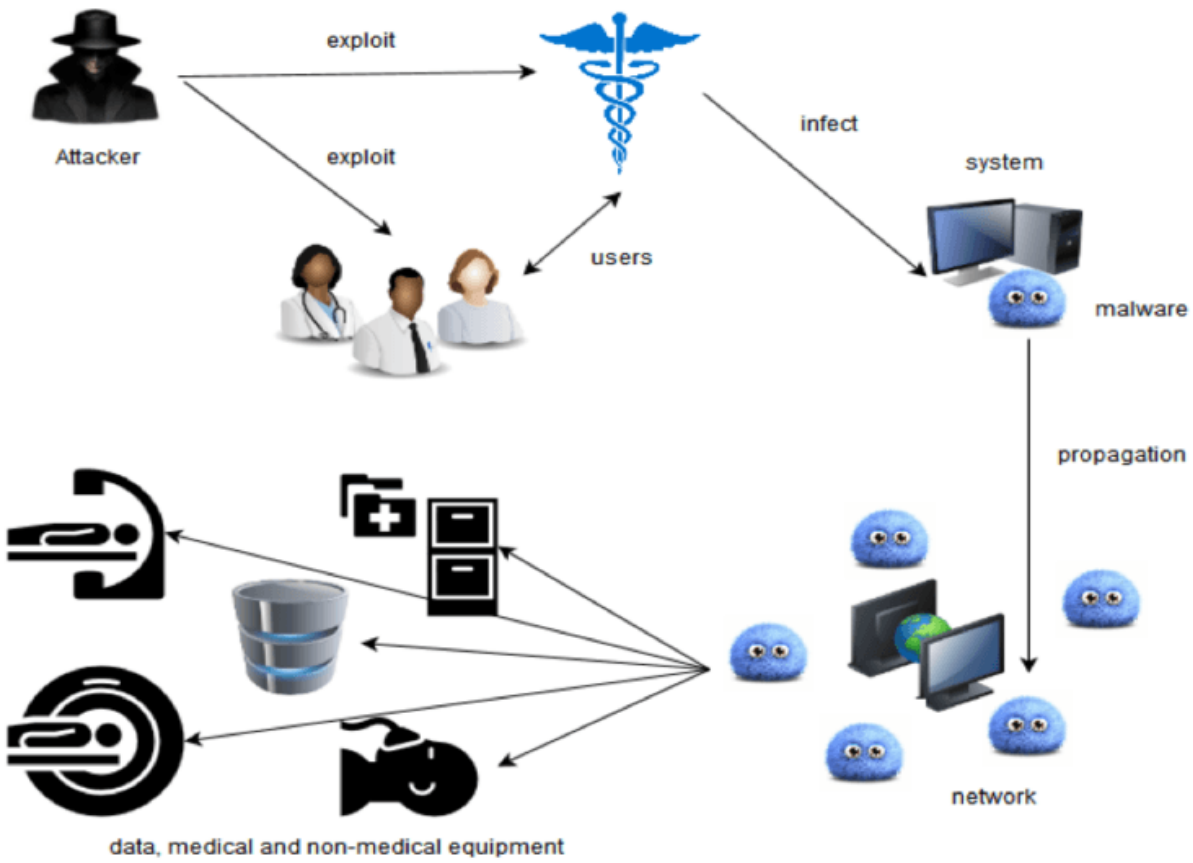
The attacker can then use this software to gain access to the organisation's financial, administrative and clinical information systems. In the case of the recent "Wannacry" attack that affected the NHS, the malware (in this instance "ransomware") locked users out of their computers and demanded money to release them.

These attacks can also develop into "advanced persistent threats" against healthcare networks. These occur when malware enters a health network and remains there unnoticed while keeping in contact with the attacker.

From there it can spread throughout the network, even if the original download is detected and removed. Then it can steal data and direct network traffic to the attacker so they can see exactly what is happening in the system in real time.

Attackers can also use the health network to spread into connected medical devices and equipment such as ventilators, X-ray machines and medical lasers. From here they can create a "back door" that will allow them to maintain access even if software is updated to improve security.

It's also possible that attackers could one day use artificial intelligence to mount more complex attacks. For example, hackers could use an intelligent system to block algorithms in the healthcare network that manage prescriptions or drug libraries and replace them with fakes.



How the risk spreads. Credit: Alexey Turchin

Why is healthcare such a target?

Yet any organisation with a computer is at risk from cyber-attacks and there are arguably far more obvious targets for those wanting to extort money. The recent attack on the NHS, for example, yielded very little ransom.

Part of the reason for the threat against the healthcare sector is that it is classed as national critical infrastructure, alongside water, electricity and transport networks. This makes it an attractive target for those hackers wanting to cause chaos, especially from a hostile foreign country. Attacking a healthcare organisation that is part of a wider network of infrastructure could also provide a way in to other critical facilities.

There are also a huge number of opportunities for attacks on healthcare systems simply due to the extent to which they rely on technology. Healthcare today makes massive use of expensive technology, not just in computer systems and hospital equipment but also devices attached to and even embedded in the human body, such as fitness monitors or digital pacemakers. There are also many ways in for a healthcare hacker, from data networks to mobile applications and even non-medical systems such as CCTV.

In particular, the spread of the Internet of Things, the connection of increasing numbers of devices and objects to the internet, is increasing the number of potential access points for hackers. Unlike many of the more trivial uses for the Internet of Things, connected medical devices

have obvious benefits because they can instantly exchange useful data or instructions with medical staff. This is where some of the greatest dangers lie because the devices are often involved in critical procedures or treatments. Interference with the signals to a robotic surgical tool, for example, would be devastating.

How can we protect healthcare from attacks?

Most of the attacks against health systems fall under the category of missile attacks. They cannot spontaneously harm the attacker and leave limited traces, but can cause significant damage. This makes it very difficult to track down the attackers or predict future attacks.

But healthcare organisations have already become more aware of the danger they are in and started to take measures to protect themselves, for example by building cyber-security into their information technology strategies. At a delivery level, hospitals can establish new security standards and better ways to effectively integrate the new interconnected systems as they emerge.

But healthcare systems suffer from the same inherent problems as any technology. Even when a security team thinks is has a grip on a problem, another often appears. When one is solved, many more are often generated. What's more, they are designed by humans for humans, and so it's fair to assume they are vulnerable by default thanks to human error.

Although you can train staff as best you can, it only takes one person clicking on a rogue attachment to let in malware that can disrupt the whole system. What's more, the fear of legal costs and responsibilities might lead some organisations to under-report incidents and take action that could increase the threat, for example by paying ransoms to hackers. In reality, the reputation and trust of healthcare organisations depends on

them understanding the true extent of the threat and taking sufficient measures to guard against it.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation

Citation: Why has healthcare become such a target for cyber-attackers? (2017, July 18) retrieved 20 April 2024 from https://phys.org/news/2017-07-healthcare-cyber-attackers.html