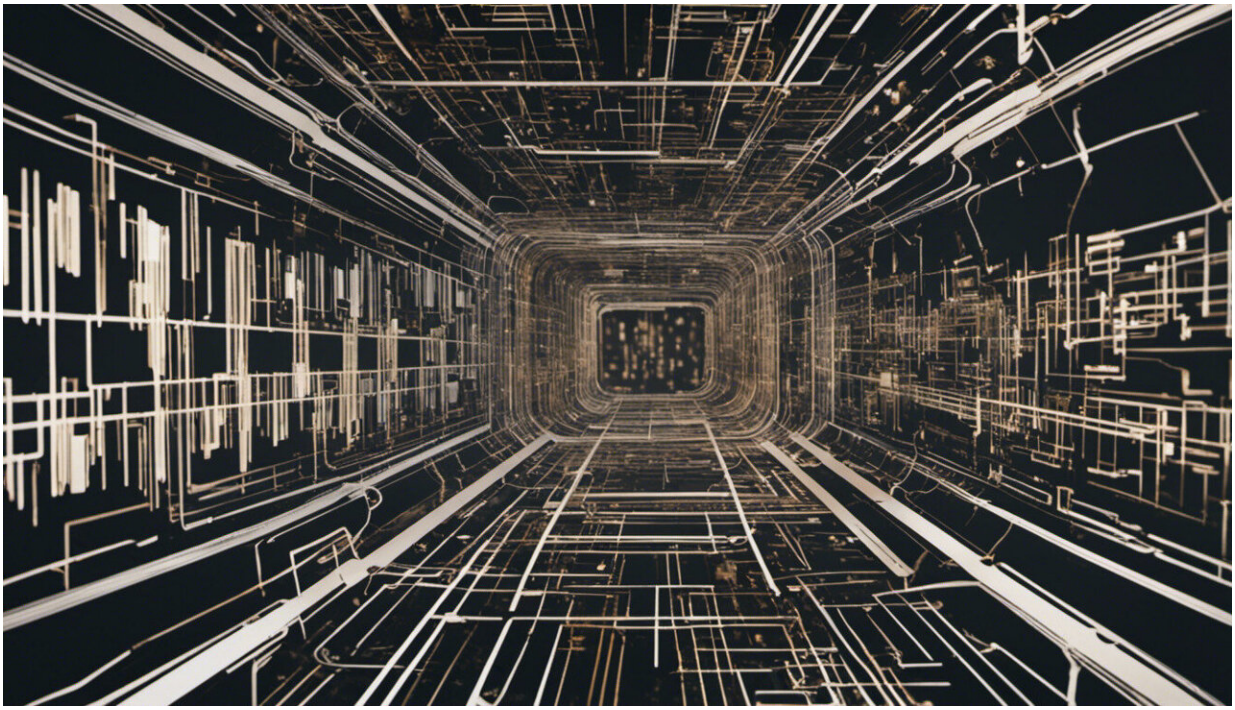
When secret government talks are hacked it shows no one is secure in the connected age

June 16 2015, by Carsten Maple



Credit: AI-generated image (disclaimer)

Hotel rooms aren't as private as they used to be. Recent reports suggest luxury hotels may have been targeted by national intelligence services trying to spy on negotiations over Iran's nuclear programme.

The talks weren't bugged in the traditional way of hiding microphones in

the room. Instead, hackers infected hotel computers with a computer virus that its discoverers say may have been used to gather information from the hotels' security cameras and phones.

The virus was discovered by cyber-security firm Kaspersky Labs when the company itself was infected by a sophisticated worm known as Duqu2. Kaspersky went about investigating which other systems around the world might have been attacked. Among the huge range of systems they checked, thousands of hotel systems were analysed. Most of these had not been subjected to an attack, but three luxury European hotels had also been hit by Duqu2.

Each was compromised before hosting key negotiations between Iran and world leaders regarding the country's nuclear programme. Having previously been accused by the US of spying on the talks, Israel – which was not involved in the discussions – is now under suspicion of (and denies) deploying the virus.

Hacking a hotel room

Of course, full details of exactly what information has been leaked will take some time to understand. As we saw when Sony was hacked, further revelations are likely to emerge over time. What is apparent is that parts of the worm were designed to compress video, and others to collect communications data from phones and Wi-Fi networks.

Many hotels, especially luxury ones, use computerised camera surveillance and have many other sensor devices collecting and transmitting data, such as smart TVs. The fact that these three hotels were all scheduled to hold very sensitive talks before being attacked by highly sophisticated malware is unlikely to be a coincidence.

There are a number of ways the worm could have been spread to the

hotel computer systems. Viruses can, of course, be sent as attachments to emails and often spread in this way. Up-to-date security software can stop most known viruses. But in cases such as this, where the malware and the vulnerability it exploits were previously unknown, the virus is not detected and so can infect the machine.

Another possibility is that an employee or contractor or someone masquerading as such could have infected a machine at the hotels. Duqu2 is thought to be related to the virus Stuxnet, which brought down Iranian nuclear facilities and was spread, at least in part, through USB drives used by people working in the nuclear industry. Coincidentally, it is thought the infected USBs were likely to have been picked up from in hotels in India and Iran.

We are now living in a highly connected world that is increasingly dominated by smart devices and the so-called internet of things, where many objects and appliances gather data and are connected to the internet. These devices have all types of sensor and actuators and can be controlled remotely and without human intervention.

No escape

If these devices are controlled by someone other than the owner, they can be used to pass interesting information to the person in control. Last year, a Russian website streamed data from over 500 internet-connected video devices, including baby monitors. Accessing these devices didn't even require advanced malware. Instead, hackers abused the failure of the devices' owners to set a complex password in order to gain control.

Numerous actors, from terrorists to cyber-criminals have an interest in accessing information from governments, companies and individuals. But Edward Snowden, who leaked details of the US and UK's official data-capture programme, revealed just how much nation states also have

a thirst for information, using both targeted and more blanket attacks to provide intelligence.

Clearly, in such a "smart" world, we need to get better at protecting access to our systems and devices, and that includes ensuring that the users smarten up too. This means not only ensuring our anti-virus software, firmware on our hardware, and operating systems are fully up-to-date, but also that we take care ourselves using USB devices or opening unknown attachments.

We are seeing an increase in political groups compromising the systems of companies, governments and individuals, as well as attacks for notoriety or financial gain. No system is beyond being a target, no matter how small or large.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation