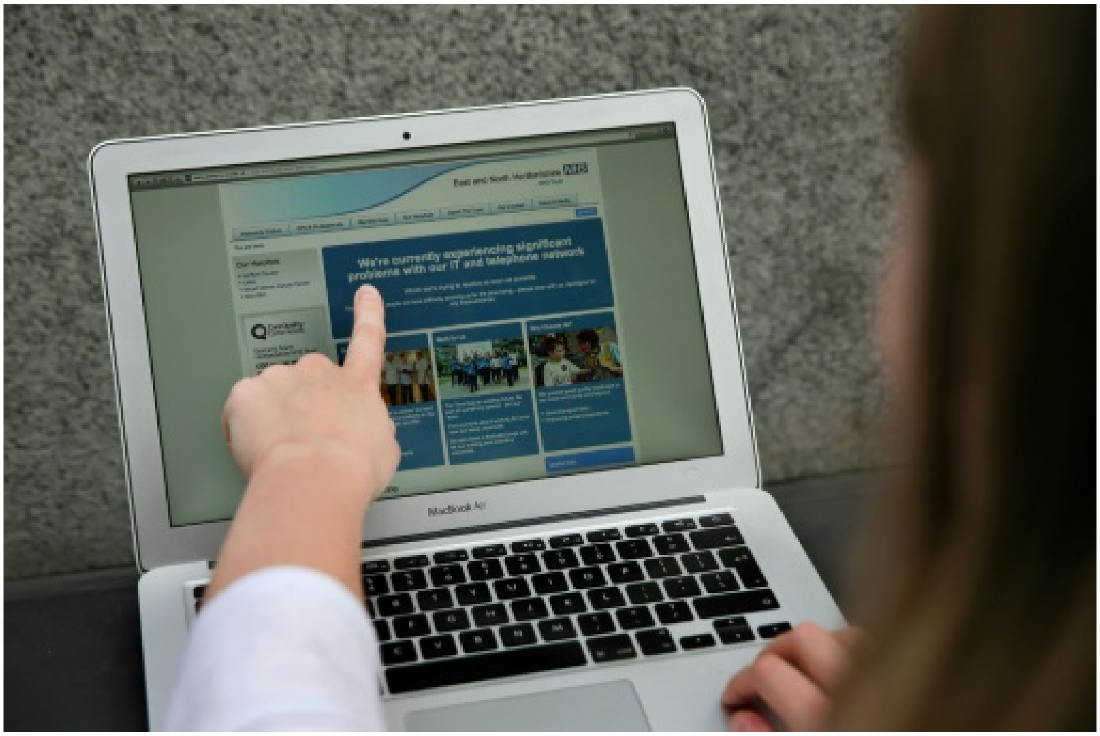
Watch out in a world of connected objects, cyber specialists warn

May 21 2017, by Jean Liou



A major wave of cyberattacks hits dozens of countries around the world earlier this month

The massive global cyber attack that wreaked havoc in computer systems earlier this month caused plenty of visible disruption, not least in Britain's National Health Service.

But in the brave new inter-connected world heralded by the internet of things (IoT), so-called "ransomware" attacks could have as their source something quite mundane and yet present in ever more modern households.

In a not so far-off future, the source of a software glitch with serious consequences for the simple consumer could be anything from a connected coffee machine or refrigerator to a techie toy or an outsmart-you television.

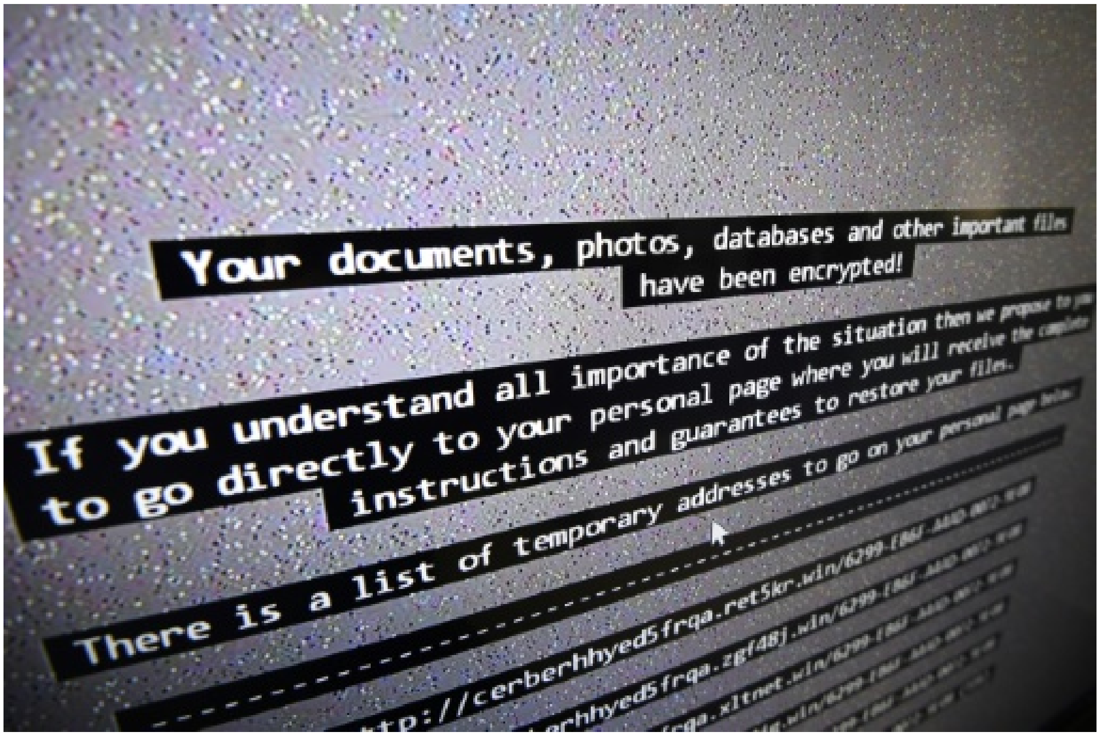
Web-connected gadgets are becoming all the rage with tech-aware professionals.

But the mere idea that it only needs a hacker to give the software a malevolent tweak to send them on the blink with disastrous consequences may yet threaten the development of such goods' popular take-up.

"Regarding last weekend's attack there is no risk for connected objects. That in particular hit systems running Windows ...and today there are no mass market gadgets with Windows loaded in order to function," says Gerome Billois, a consultant with Wavestone.

"In contrast, there have already been massive attacks on connected objects," Billois told AFP.

The Mirai malware strain made from hacked IoT devices including badly secured routers and internet connected cameras recently infected hundreds of thousands of poorly secured connected objects.



Your documents, photos, databases and other important files have been encrypted!

If you understand all importance of the situation then we propose to you to go directly to your personal page where you will receive the complete instructions and guarantees to restore your files.

There is a list of temporary addresses to go on your personal page below:

```
---------------------------------------------------------
ttp://cerberhhyed5frqa.ret5kr.win/6299-
erhhyed5frqa.zgf48j.win/6299-
frqa.xltnet.win/6299-
```

A ransomware demand after one's computer or other connected object has been hacked might look like this

The idea was not to stop them from working but to transform them into zombies or botnets with a view to using them as relay stations for future cyber attacks.

Last week at a timely cyber security conference in The Netherlands, American wunderkind Reuben Paul, just 11, stunned an audience of security experts by hacking into a teddy bear via bluetooth to show how interconnected smart toys "can be weaponised".

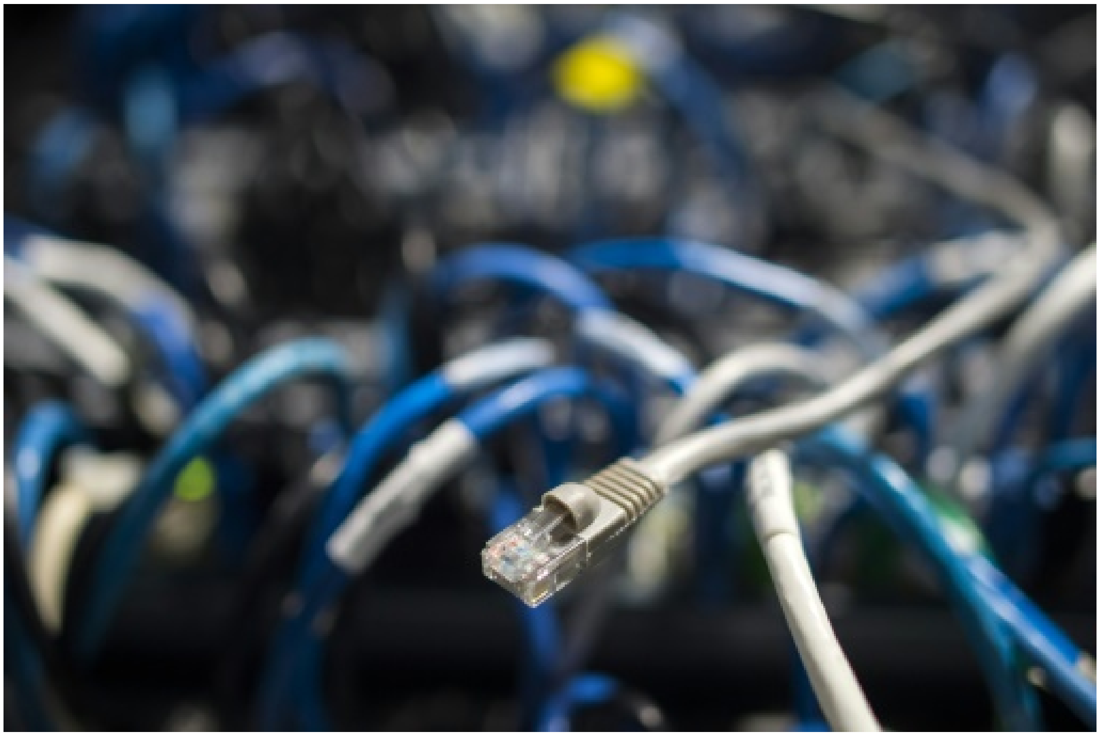
His prowess showed just how easy it is for tech savvy individuals to use everyday objects to harvest data or use them as spy holes for covert surveillance.

According to documents released in March by Wikileaks, US intelligence can hack smartphones, computers and smart, web-connected TVs, to pilot them and eavesdrop.

"All the other connected objects can be pirated, that has been shown, be it a coffee machine, a refrigerator, a thermostat, electronic entry systems, the lighting system...," warns Loic Guezo, a cyber security analyst for southern Europe with Japanese security software company Trend Micro.

Mikko Hypponen, head of research at Finnish security specialists F-Secure, has for his part come up with his eponymous Hypponen's Law.

This states that "once a device is described as 'intelligent', you can consider it as vulnerable."



Are your links to the web safe?

Neglected security

The future might well spell connected cars—but they too are subject to potential remote hacking, the consequences of which barely need stating.

When hackers lurking with their laptops have finished conjuring what havoc they might wreak on distant roads there are plenty of other things to which they could turn their attention.

These include vases which tell you when they need fresh water, insulin pumps—or how about sex toys?

So, the worried tech consumer may be asking him or herself—can a cyber hacker deprive me of my morning slug of caffeine?

Or maybe keep my thermostat blocked at 10 Celsius (50 Fahrenheit) —a chilling thought—or even take over my GPS if I don't hand over a ransom?

Theoretically, yes, specialists tell AFP.

"The logic of a cybercriminal is to make money," says Wavestone's Billois. Such an individual will not feel the need to make do with small-scale attacks.

The internet of things can connect our homes, our coffee machines, our fridges, all kinds of appliances, to the outside world—where a hacker might be lurking

Connected TVs, having rapidly become widespread, are an ideal portal for making ransom demands.

"Tomorrow, one can imagine devices which attack your connected house, bringing it under control, and then you get sent a message by another channel," muses Guezo.

All that would required would be to perfect the sort of virus one can find on offer within the murky confines of the "darknet", off the beaten track for day to day netizens.

Cyber security specialists are very much aware of the need to keep working on solutions offering protection as more and more homes go "smart" and "connected" with various boxes as add-ons to their usual routers.

The specialists' plan is to work with the makers of connected goods in order to incorporate a security interface right from the start, thereby offering what the profession calls "security by design".

Some experts feel that, in the rush to bring fascinating and cutting edge technologies into the home, the need for commensurate security has been rather left behind.

"It is extremely difficult to calculate the solidity of a connected object in terms of cybersecurity," Billois regrets.

"As a consumer it is today impossible to know if you are buying a secure connected object or not," he adds.

"There's no label such as a made in Europe kind of tag guaranteeing an object won't catch fire, or won't pose a risk to children."

Citation: Watch out in a world of connected objects, cyber specialists warn (2017, May 21) retrieved 24 April 2024 from https://phys.org/news/2017-05-world-cyber-specialists.html