Homes filled with smart devices could be exposed to thousands of hacking attacks in a week

A home filled with smart devices could be exposed to thousands of hacking or unknown scanning attacks in a single week, according to a report.

Homes in the UK have an average of more than 10 different connected devices, from televisions to thermostats.

But, while these products have benefits, they can also be a potential target for hackers.

Consumer publication Which? set up a fake home with connected products bought online, including smart TVs, printers, wireless security cameras, and wifi kettles.

They were then connected to the internet, exposing them to cyber threats and malware.

Working with cyber security specialists NCC Group and the Global Cyber Alliance, Which? saw 1,017 unique scans or hacking attempts from around the world in just the first week, with at least 66 of these being malicious.

That figure rose to 12,807 in the busiest week, including 2,435 specific attempts to maliciously log into the devices with a weak default username and password.

More from UK

R number in England falls slightly to 1.1 to 1.3 despite rise in case numbers

COVID-19: Delta variant cases up 46% in a week – as expert warns mutant strain will hit UK 'soon'

Dalian Atkinson death: CPS seeks retrial of police officer accused of assaulting the former footballer after jury discharged

Oxford Circus stabbing: 60-year-old man dies after being stabbed in London's Regent Street

England squad fly to Rome today ahead of Euro 2020 quarter-final against Ukraine

Professor Chris Whitty : Man charged with assault after video of park incident

Most attempts were blocked by security protections in the devices but this was not always the case.

Which? said most attempted came from the US, India, Russia, the Netherlands, and China.

The most common motivation is to create botnets which look for new unsecure devices such as routers, wireless cameras and printers before using weak default passwords to get in.

They can then be used as a powerful hacking tool, Which? said.

Kate Bevan, Which? computing editor, said: “While smart home gadgets and devices can bring huge benefits to our daily lives, consumers should be aware that some of these appliances are vulnerable to hackers and offer little or no security.

“There are a number of steps people can take to better protect their home, but hackers are growing increasingly sophisticated.

“Proposed new government laws to tackle devices with poor security can’t come soon enough – and must be backed by strong enforcement.”