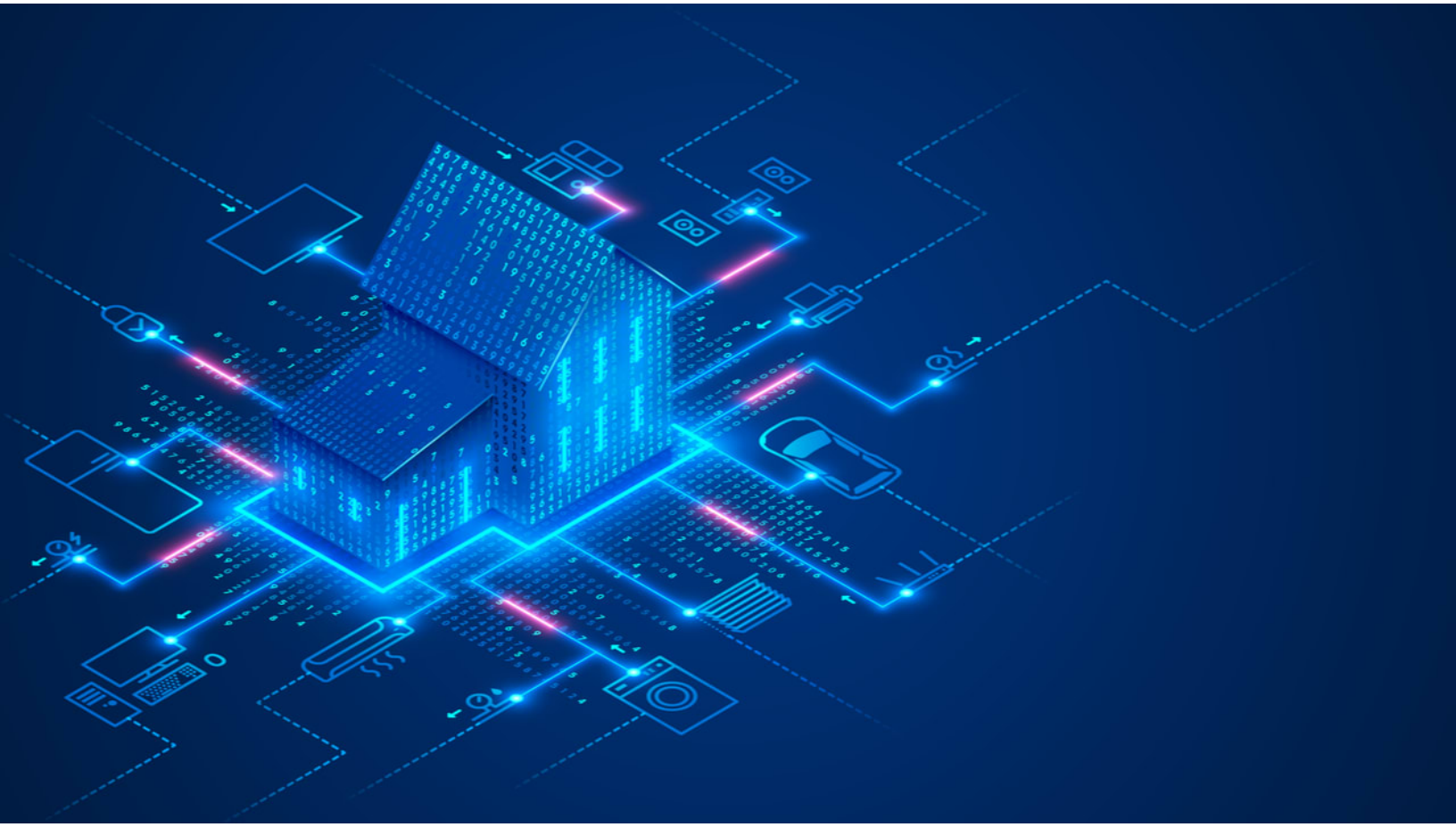

Royalty-free stock vector ID: 1565456593

Jul 02, 2021 07:07 BST

# Honeypot research reveals the connected life might not be so sweet

Smart TVs, fridges, toothbrushes, heating, plugs, cameras, kettles – these are just a few of the connected devices that have made their way into our homes. This list will no doubt continue to grow as technology evolves and consumers demand more connectivity.

But what are the security implications of introducing more of these smart devices into our homes?

For several years now, we have been working with the consumer champion Which? to test the security and privacy of connected devices we use in our day-to-day lives. So far, we've found vulnerabilities in connected toys, cameras, smart plugs and doorbells, and their associated applications.

And despite many calls for security by design over the years, the same issues have been flagged again and again – namely weak encryption and the use of default passwords. This time, we wanted to put these findings into a wider real-world context and scenario which would demonstrate the susceptibility and impact of these vulnerabilities.

Working with Which? and the Global Cyber Alliance, we created a honeypot – a network set up to detect the unauthorised access of networks and devices. Using devices selected by the consumer champion, which included smart TVs, printers and wireless security cameras and Wi-Fi kettles, we connected these to the internet to see what unique scans or hacking attempts they could attract…

**Honeypot success**

Within the first week alone, we saw 1,017 unique scans or hacking attempts from locations across the globe – of which 66 were for malicious purposes. As the exercise progressed, this figure rose to 12,807 unique scans or attack attempts in one week, with 2,435 of these being attempts to log into one device which had a weak default username and password.

Most of the devices in the 'hackable home' environment were able to prevent attacks through basic security protections, although this doesn't mean they'll never be at risk. The most concerning issue we found though was a connected camera which had a weak default password, which allowed a suspected hacker to gain access to the camera stream – luckily though, the camera lens was taped over…

**Why are smart devices a target?**

There are a number of reasons why smart devices might be targeted by malicious actors – in many cases it is to harness them and create botnets – a network of connected devices infected with malicious software which are then controlled without the user's knowledge to perform wider, more powerful hacking attempts.

Mirai is one off the most prolific botnets currently around, and in one 24-hour period, we saw 91,701 instances of the botnet across our surveillance tools.

**Why do research and findings like this matter?**

It goes without saying that the implications of insecure devices are huge – especially with botnets like Mirai sprawling across the internet and our devices. Our findings highlighted that just one device with a weak password could provide a perfect gateway for an attacker. This is a basic issue that can be easily resolved and is something the UK's Product Security and Telecommunications Infrastructure Bill will make illegal when it comes into force in 2022.

**Commenting on the research, Matt Lewis commercial research director at NCC Group said:** "Honeypot exercises like this are guaranteed to attract a multitude of scans and attacks powered by bots, but the scale at which this happens and number of attempts we experienced was staggering.

"The most concerning thing this exercise has highlighted is that all it takes is one weak password or unpatched device for an attacker to compromise and potentially affect the wider connected network. For years as consumers, we've expected security by design in the products we purchase, but this exercise and ongoing research into the security of connected devices has countlessly proven that this isn't the case.

"While we look forward to the introduction of the Product Security and

Telecommunications Infrastructure Bill in 2022, there's still much to be done in the interim to ensure device developers, manufacturers and consumers understand the impact of vulnerabilities like these.

"We're pleased that the vulnerable camera has now been withdrawn from the marketplace and hope that this research helps consumers to assess the security features of IoT devices before purchase and empowers them to change default passwords and understand the importance of patching."

Keep tabs on our research blog in the coming weeks if you'd like to find out more about the results and how we built the honeypot itself.

You can read the Which? article here: https://www.which.co.uk/news/2...

---

## About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 14,000 customers to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience, and investment in research and innovation, it is best placed to help organisations assess, develop and manage their cyber resilience posture.

With circa 2,000 colleagues in 12 countries, NCC Group has a significant market presence in North America, Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia, Japan and Singapore.

## Contacts

**NCC Group Press Office**
Press Contact
All media enquires relating to NCC Group plc
press@nccgroup.com
+44 7824 412 405
+44 7976 234 970