“Internet of Things” Now the Biggest Cyber Weapon On Earth

In Silicon Valley’s quest to use it’s out-dated technology to exploit everything, it’s “asset” has been turned into an ultra-weapon. The “Internet of Things” turns out to not only be a bad idea but also the biggest cyber-risk on Earth.

Massive web attack hits Krebs, the security blogger, using the “internet of things”

EXPLAINED: What is a DDoS attack?

One of the biggest web attacks ever seen has been aimed at a security blogger after he exposed hackers who carry out such attacks for cash.

The distributed denial of service (DDoS) attack was aimed at the website of industry expert Brian Krebs.

At its peak, the attack aimed 620 gigabits of data a second at the site.

Text found in attack data packets suggested it was mounted to protest against Mr Krebs' work to uncover who was behind a prolific DDoS attack.

Web protest

In a blogpost, Mr Krebs detailed the attack, which began late on Tuesday night and quickly ramped up to its peak attack rate.

DDoS attacks are typically carried out to knock a site offline - but Mr Krebs' site stayed online thanks to work by security engineers, who said the amount of data used was nearly twice the size of the largest attack they had ever seen.

"It was among the biggest assaults the internet has ever witnessed," added Mr Krebs.

Security firm Akamai said the attack generated such a huge volume of data by exploiting weak or default passwords in widely used net-connected cameras, routers and digital video recorders. Once in control of these "smart" devices the attackers used them to swamp the site with data requests.

"These new internet-accessible devices can bring great benefits, but they are also an increasingly easy and lucrative targets for cybercriminals," said Nick Shaw from security firm Symantec.

The security firm has carried out research which shows swift growth in the number of malware families scouring the net for vulnerable devices. Typically, said Mr Shaw, malicious hackers who take over gadgets are not interested in stealing personal data.

"Cybercriminals are interested in cheap bandwidth to enable bigger attacks," he said.

Mr Krebs speculated that the attack could have been prompted by an article he published, in early September, that named two young men allegedly associated with a service called vDos that carried out DDoS attacks for cash.

Soon after the article was published, Israeli police arrested the two men named by Mr Krebs. Released on bail, the pair were barred from using the net for 30 days.

Buried inside many of the data packets despatched towards Mr Krebs' site was text calling for the release of one of the men named in that article.

"I can't say for sure, but it seems likely (to be) related," said Mr Krebs.

Topics: Internet of things, krebs, krebs on security, fire-eye, Russian hackers, Nick Shaw