BIZCOMMUNITY

Hacked by your fridge: the Internet of Things could spark a new wave of cyber attacks

By Mihai Lazarescu

7 Oct 2016

The past few weeks have seen a remarkable and somewhat alarming development in cyber security. It comes in the wake of a distributed denial of service (DDoS) attack that has forced a rethink of how we can deal with attacks of this nature in the future.

© cheskyw – 123RF.com

The attack was aimed at the Krebs on Security website, a well established source of valuable information on cyber crime.

What was remarkable about this particular attack was the sheer volume of traffic involved. According to the author himself, the attack reached around 620 gigabits per second, which is nearly twice the amount seen in the previous record-breaking DDoS attack.

To put things in perspective, this is like the website being hit by one and a half Blu-ray discs' worth of data every second. The average DDoS in 2014 involved traffic of around 7.5Gb/s, and yet only two years later the volume has increased by a factor of 10-15.

The sustained attack eventually forced the website's DDoS protection provider, Akamai cloud services, which had been providing security for the site free of charge, to admit that it could not handle that sort of attack pro bono, and thus the Krebs on Security site had to move.

However, since the Krebs attack, there has been a claim made of yet another attack that involved more than 1 terabit per second of traffic.

The claim is currently being investigated, and if it is confirmed, it highlights the challenge that organisations face in dealing with massive DDoS attacks.

Apart from the record volume of data involved, the Krebs attack also set an unfortunate precedent by forcing a high-profile security website offline for several days. The attack was successful and has demonstrated the vast potential of this type of weaponised DDoS attack.

Internet of threats

This DDoS was also remarkable in terms of how it was executed. Most DDoS attacks use a tried-and-true method called amplification or reflection. This involves using a number of computers on the internet – often in the form of a "botnet" of compromised computers – to exploit quirks in the internet's domain name server (DNS) system to turn a small amount of data into a torrent directed at the target website or server.

However, in the Krebs attack, we saw something new: it wasn't executed by conventional computers, but rather by Internet of Things (IoT) devices – including innocuous things like digital video recorders and security cameras.

This is an important and worrying development for two reasons. First, the devices themselves are not designed with security as a key focus; convenience and cost are the main considerations.

It is true that many of the IoT devices lack the computational and memory resources that are common in devices such as mobile phones, which reduces their capability from a hacker's point of view. However, IoT devices are still susceptible to malware, and an enterprising criminal group can build a vast botnet given the time and relatively low investment.

Second, even though their capabilities are lower than a regular computer, they are still more than capable of executing a DDoS attack if employed in sufficient numbers. And those numbers are growing daily. It is expected that more than 50 billion IoT devices will be plugged into the internet by 2020.

Unless the security measures and settings improve significantly in the next four years, there will be literally billions of devices that could be compromised and used for malicious purposes. As Joseph Stalin is reputed to have said: quantity has a quality all of its own.

These IoT DDoS attacks can be mitigated to some extent, but if the attack is well organised then the best we can aim for is damage mitigation. The nature of DDoS attacks makes them very difficult to handle, especially if the instigator is competent.

Presently, we are not ready to handle large scale attacks of this nature. Most organisations, including major financial institutions, would be at least partially crippled by a sustained attack similar to the Krebs one.

The reason for the lack of readiness is simple: the cost involved is, in most cases, beyond the financial capabilities of most organisations.

However, one thing that is more affordable, and thus can be done to increase the readiness, is planning for such attacks. Rather than hoping that nothing significant will happen, it is best to plan for such attacks so that when they occur (and they will), everyone will know what they should be doing to mitigate the damage.

ABOUT THE AUTHOR

Mihai Lazarescu is associate professor and head of the Department of Computing, Curtin University.