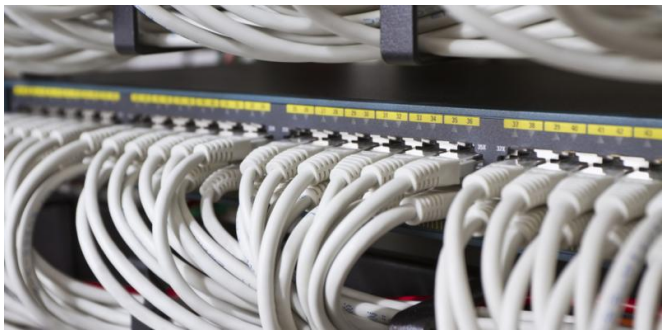
By attacking DNS, hackers can bring down many websites for the price of one

25 October 2016, by Rob Miles



Credit: Kjetil Kolbjornsrud/shutterstock.com

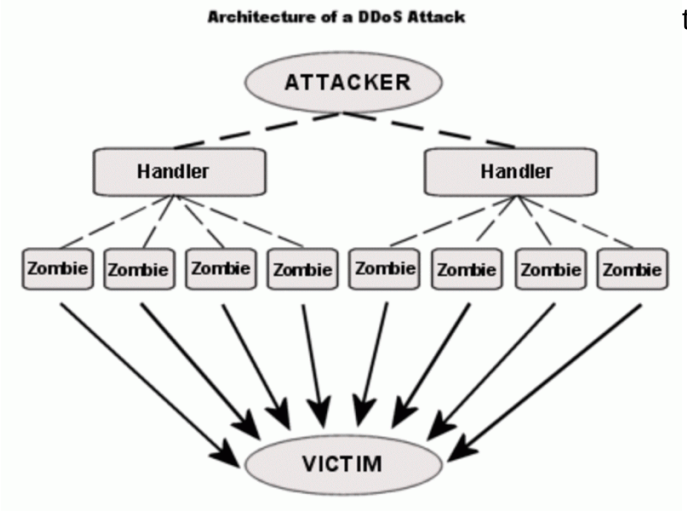
When hugely popular websites and services such as Netflix, Spotify, Twitter, PayPal and Amazon Web Services are taken offline, it affects millions or even billions of internet users. The cyberattack that brought down these and other sites in the US and Europe focused on a particular component of the internet's architecture that is known to be vulnerable: DNS.

To understand how such attacks are possible today you have to remember that the internet was designed decades ago, when there were very few computers in the world – and even fewer connected to a network. As a research project funded by the US military in the 1960s, the original internet was designed to be a network that could survive a nuclear attack. It was distributed, didn't rely on a central hub, and messages could still be routed through the network even if large parts of it had been damaged or destroyed.

But while this design made the internet resilient to attacks from outside the network, its design placed a great deal of trust in those using it – all its users were to be US military or associated staff, after all. Consequently the internet was never designed to withstand attacks from inside the network, yet today it is used across the world – including by, for example, both the US military and its adversaries.

The incidents that are becoming common today revolve around DNS – the Domain Name System – a sort of internet address book. DNS records contain the unique IP network address of the web server that is the physical location of a website, and the human-friendly URL or domain name which points to it. This is because it's a tough ask for users to remember an IP address such as 192.168.15.23, and much easier to remember something like theconversation.com. It is DNS that stores these records and converts a URL into its corresponding network address.

DNS management can be tricky, particularly for very popular web sites, so companies are frequently employed to do this: one popular company is Dyn, and it was this company that found itself on the end of a massive distributed denial of service attack recently, in which the target is bombarded by a huge number of requests at the same time. The idea is to overwhelm the service to prevent legitimate traffic getting through. It's rather like every person in the country calling directory enquiries at once – it would become unusable. As DNS companies like Dyn typically provide services for thousands of websites, an attack that puts them offline can have a very wide impact.



How a denial of service attack works. Credit: VicktoR

Of course, the internet's original designers never considered that systems with access to the network would go rogue and act against it, nor in such enormous numbers. But today that is exactly what's happening: almost anyone in the world can connect to the internet and start sending messages, be they harmless or malicious.

More devices, more problems

In recent year things have got a lot worse, because huge numbers of devices are now being connected to the internet that could be used for these sorts of attacks. These are not computers or smartphones – they are devices such as internet-connected security cameras (as was used in Dyn's case), but also baby monitors, and even kettles. Essentially, each of these devices contains a small, internet-connected computer which, if insufficiently secured from being tampered with, could be hacked and remotely controlled. These so-called Internet of Things devices can then become the footsoldiers in the hacker's "botnet": a network of thousands or hundreds of thousands, even millions of devices that have been compromised in this way and can be used to flood the hacker's target with messages as part of a denial of service attack.

Unfortunately many of these systems are poorly secured, with default usernames and passwords that their owners don't get around to changing – for hackers to take control is as easy as pushing an open door. There is also software available online that helps to manage these botnets and "weaponise" them – in this case, software called Mirai – and anyone with the skills can find it and use it. As it is, commentators such as Bruce Schneier have suggested that this sort of activity currently appears to be state sponsored, with national governments' trialling their cyberwarfare capabilities – a deeply troubling development.

Denial of service attacks on websites and companies that offer infrastructure services such as Dyn will only increase. The arrival of more and more Internet of Things devices designed to be connected to the internet will hugely increase the potential recruits available to attackers from which to build a botnet. It's very difficult and costly to fend off huge denial of service attacks, and software like Mirai gets better and better at defeating countermeasures deployed against it.

What is required is to redesign how DNS functions in the internet's architecture, to work around what has become a few vulnerable points of failure in what was designed to be a highly distributed, de-centralised network. And legislators need to persuade manufacturers, and users, to take the security of their devices seriously in order to prevent malicious forces turning devices against them.

This article was originally published on The Conversation. *Read the* original article.

Source: The Conversation