EnglishWaves.fr
The French radio station that speaks English !

TechTalk

Cyber Security, Part 1 ©

by John McCarthy

Hi and welcome. In this edition of Tech Talk we'll be taking a brief look at cyber security, or rather the worrying lack thereof, following what has been described as the largest distributed denial-of-service attack in history just a fortnight ago. This incident affected some of the most popular websites in the world, including Netflix, Twitter, PayPal, CNN, The Guardian, The New York Times and the Wall Street Journal, by literally taking them offline.

DDoS attacks basically exploit the power of a network of tens or even hundreds of thousands of compromised computers – known as a 'botnet' in the IT vernacular – and these literally flood a website's servers with viewing requests leaving potential customers unable to get through. The idea, therefore, is to target and overwhelm a certain company's servers causing them to fail and crash their website, losing the victims tens of thousands of Euros for every hour that their websites are offline.

In order to add an unsuspecting computer to a botnet, the potential hacker has first to gain control of the machine, and this can be done by exploiting vulnerabilities within the operating system to install malware on the computer which will then provide permanent access to the PC. The inherent dangers of this are self-evident: attackers can exploit your computer to use it as part of a DDoS attack, or access it and retrieve usernames, passwords, your bank details and a whole host of sensitive data. The malware used to exploit devices can be installed without your knowledge by merely clicking on a malicious link or simply visiting a website serving infected adverts. Hence the importance of ensuring that your computer's antivirus is up-to-date and that you install all the latest security patches for your Operating System, and even install a firewall to control what software can and cannot gain access to the internet. Most anti-virus programmes, such as McAfee, Bitdefender, Norton and Kaspersky can scan your computer to ascertain whether it's part of a botnet.

What was and remains particularly worrying about the cyber-attack which recently brought down much of America's internet – the so-called Mirai botnet – is that unlike other botnets which typically comprise thousands of computers, Mirai is largely made

up of Internet of Things devices, such as webcams, DVR systems, thermostats and household items. Because it has so many internet-connected devices to choose from, Mirai DDoS attacks have the potential for unprecedented ferocity.

So why do DDoS attacks occur? Sometimes, they're conducted by people in protest against whatever company they're targeting; they might disapprove of what this company stands for and to express their displeasure, they shut their websites down. For more sinister reasons, cyber criminals are known to use botnets for blackmail – they could, for example, threaten a company with a DDoS attack during the potentially highly lucrative weeks leading up to Christmas unless they pay a large ransom to stay online. DDoS strikes can also be used to engage in cyber warfare and were in fact employed in attacks during the conflict between Georgia and Russia, although the perpetrators remain unknown to this day.

Some US government departments believe the Mirai botnet was a practice run for the launching of a huge wave of cyber attacks on and after election day and have warned that any attempt to manipulate voting or undermine the results will be viewed as a serious breach. There are further fears that Russia may disseminate rumours about the legitimacy of the electoral process, could attempt to shut down power grids or even spread false news reports about either candidate. With the unwelcome prospect of another Cold War looming ominously over the horizon, the possibility of a cyber war metamorphosing into a far more belligerent one is an extremely disturbing prospect that we may have to contend with in the coming years.