The latest wave of DDOS Attacks.

Firstly it might be helpful to define a DDOS Attack. DDOD stands for Distributed Denial Of Service. In the simplest of terms the attack is launched by a series of automated Bots from a large number of infected machines at a specific pre-scheduled time. The objective of these attacks is to drown the server which hosts a given Website in millions of page requests over a very short period of time and force it to Deny Service. Or more likely crash monumentally. There are many reasons an attacker might want to do this. Some are personal, others are much more complex, are totally impersonal and to some extent random.

There have been several large corporations and many smaller businesses attacked by the latest version of this form of attack over the last month or so. Larger corporations are unlikely to admit that they have been successfully attacked unless they are forced by publicity to do so. Unfortunately these attacks can be as dramatic and costly for smaller businesses. They can also put the business at risk of prosecution under the General Data Protection Regulation 2018 if they are in Europe. The reason for this risk will become clear shortly.

The wave of DDOS Attacks which emerged in early March 2019 have been given the relatively bland title of ?Memcached Q4?. What they are called is quite academic. Their objective is where the potential GDPR2018 liability takes effect. The reason for this specific wave of attacks is the extraction of name and email details en masse from as many servers as possible. Eventually these will find their way to ?Spam List? which are supposedly segregated info specific lists based on geographic location, interest, gender etc. and are available in some of the darker areas of the Internet. Generally information gathered by form pages on websites is stored securely encrypted in a database well out of sight of any would-be extraction Bots. But as a server is overwhelmed by a DDOS attack there is a possibility for a Bot to access the databases undetected by the usual security systems as the server struggles to deal with an ever increasing but momentary spike in demand.

There are several stages to these attacks and the delivery mechanism is becoming very sophisticated.

A brief list of some steps involved in one particular attack process is as follows. (Although there are many other processes.)

(1) A Bot finds your URL by randomly generating possible Domain Names and ?Spidering? those which work, looking for form pages. You are likely to receive a bunch of spam form returns which often appear to have a Russian origin and include a great deal of Cyrillic text.

(2) After determining that your site collects name and email information your URL is added to a list of possible target sites.

(3) This list is sent to another Bot which has only one objective. That is to determine the ?Colour? of the Operating System your hosting server is running. A .php suffix on your URLs indicates a Linux variant. A .net suffix indicates a Windows variant. There are various other more exotic Operating Systems, but these are the two main players. The means of attack are similar, but the database systems are different and need to be targetted in different ways.

(4) Once this initial data mining is complete everything might well seem to go quiet for several months. In fact you might never be targetted as these mined lists are sold on the Black Market. If your site appears to have few visitors or is unlikely to yield useful contact data then the details are unlikely to have an saleable value. If however your site details are bought and your site attacked you'll probably suffer a brief period of outage and a few choice warning emails from your hosting provider about over quota data usage. This is the stage at which your site is attacked by numerous DDOS Bots with the intention of forcing the server to fall over.

All very clever. But also costly for you in terms of Data Bandwidth, potentially very annoying for your customers who are likely to find themselves the target of vast amounts of Spam email. Also there is the potential of prosecution under GDPR2018 as you have unknowingly allowed your customers details to be sold for malicious ends.

So what can you do to prevent this from occurring?

There very little that can be done to prevent Data Mining. It is an unfortunate fact that there are now more Bots active on the Internet than there are humans.

However it is well worth speaking to your hosting provider and requesting the installation of ?Flood Protection? Software. These packages are usually propitiatory and there will be a small registration cost. But once installed the software will detect the early stages of a DDOS attack and effectively Firewall your entire server account. ?Flood Protection? software should also log the IP

address ranges from which the attack originates which allows your hosting provider or in-house data manager to block IP ranges and effectively prevent further attacks from the same origin.