# The science behind DDoS extortion

*By* Bryan Hamman, Territory Manager - Sub Saharan Africa at Arbor Networks

'Pay up or we'll take your Website down', so goes the adage that usually accompanies ransom-based cyber-attacks. Top of the news agenda in recent weeks, well-known names such as Evernote and Feedly have all fallen victim to extortion attacks, but these companies are just the tip of the iceberg when it comes to this very lucrative criminal activity. Whilst digital ransom attacks come in all sorts of types and forms, Distributed Denial of Service (DDoS) attacks are top of the list of methods used by attackers to force money from targeted companies.

According to Arbor's ninth annual Worldwide Infrastructure Security Report (2013), DDoS extortion attacks account for 15 percent of all DDoS attacks. While it may seem like a relatively small percentage, one must consider that as much as 10,000 DDoS attacks occur world-wide every day and that the potential cost in damages and reputation can have a significant impact on a targeted organisation. DDoS extortion attacks are generally volumetric, high bandwidth attacks that are launched with the aim of crashing a company's Website or server by bombarding it with packets, which originate from a large number of geographically distributed bots. The size of volumetric DDoS attacks continues to increase year over year, and they remain a major threat to enterprises and Internet Service Providers (ISPs) alike. In fact, Arbor's research shows that the average size of DDoS attacks was 20 percent higher in 2013 than in 2012.

Traditionally, DDoS extortion attacks were used against online gambling sites, around major sporting events. Criminal gangs would initiate attacks that would bring the Website down just before the event was to start, thus forcing the companies to choose between suffering a major loss in monetary and reputational terms or paying up. Increasingly, however, DDoS attacks are being used to extort money from all sorts of businesses and the reality is that no company should feel safe. Any business operating online – which means just about any type and size of organisation, can become a target, because of who they are, what they sell or who they partner with. Companies that are especially vulnerable to this type of attacks are those with no or limited DDoS protection or ones that lack the resources to deal with either volumetric or application layer based DDoS attacks.

Once the criminals choose a target, the attack usually follows one of two scenarios. Attackers either show off their skills by conducting a 'sample' DDoS attack on an organisation, which lasts for a short period of time and is followed by a threat of further attacks if ransom isn't paid, or simply skip the display of power and proceed straight to the ransom request. The targeted company is then faced with two obvious choices – either pay up or brace itself for further attacks.

So what *is* the right response when it comes to extortion demands? The answer is simple and always the same - not to give in. Organisations should under no circumstances agree to pay the ransom – it can set a dangerous precedent and encourage more attacks in the future and while it might make the pain go away in the short term, the long term results are generally not worth it. Declining to pay comes, of course, with severe consequences – as we saw from recent attacks on Feedly, who suffered from three, separate waves of DDoS attacks. However, the company has now recovered from the attack and is operating as normal. Furthermore, it has been praised for its brave decision by the security community and even its own customers.

Yet, rather than dealing with the aftermath of an extortion attempt, companies that rely on Internet availability to conduct business should be looking to invest in appropriate prevention. Many companies still rely on reactive measures such as router filters and firewalls, which are inefficient and not sophisticated enough to protect against organised cybercrime. Instead, organisations need to invest in preventive, multi-layered mitigation, which includes on premise and cloud protection, as well as allowing for co-operation with

their ISP or hosting company. In addition, putting a mitigation strategy in place, should the worst happen, is of crucial importance – especially as only 17 percent of organisations globally feel they are fully prepared for a security incident[1] <#_ftn1> .
By building defences, implementing plans ahead of time and refusing to give in, businesses needn't feel threatened anymore – attackers wanting to make easy money will have to look elsewhere!