Majority of UK firms unprepared for DDoS attacks, study finds

Summary: A new survey suggests that most UK businesses are ill-equipped to cope with DDoS attacks.

By Charlie Osborne for Zero Day | May 7, 2014 -- 09:13 GMT (02:13 PDT)

New research released by Neustar suggests that the majority of UK businesses are unprepared to cope with the threat of DDoS attacks.

Distributed Denial of Service (DDoS) attacks are a common method for cyberattacks to disrupt an online businesses. A DDoS attack uses compromised computer systems to attack a single target, sending traffic from multiple points of origin in a flow, which often overwhelms a system, causing it to deny authentic traffic access to services.

According to research released by Neustar, a third of UK businesses estimate losses of £240,000 per day when hit with DDoS attacks. After surveying 331 companies in the United Kingdom across numerous industries including financial services, technology, and the public sector, the analytics provider says larger DDoS attacks are becoming more frequent with a 200 percent increase in attacks affecting bandwidth between 1-20Gbps, in addition to a significant increase in attacks on bandwidth with a magnitude of 100Gbps or more.

Neustar's report, "*United Kingdom DDoS Attacks & Impact Report. 2014: The Danger Deepens*," also states that DDoS attacks are a "growing threat to organisations with potentially calamitous consequences for companies" without proper protection. Not only can DDoS attacks have an immediate impact on sales and business revenue, they can have long-lasting detrimental effects on brand value, customer trust, and public reputation.

High-profile DNS amplification attacks have taught attackers how to become better at denial-of-service attacks, but organisations largely haven't learned their lesson.

Key findings from the survey include:

- DDoS attacks often disrupt multiple business units, with public-facing areas like call centres, customer service, and marketing absorbing over 40 percent of DDoS-attack related costs.
- Over 35 percent more UK companies were hit by DDoS attacks in 2013 compared with 2012.
- In 2013, there was an increased number of longer attacks, with 28 percent lasting up to two days or more.

- Once attacked, there is an estimated 69 percent chance of a repeat attack. While 31 percent of these companies were DDoS-attacked once, over 48 percent were targeted two to 10 times.
- In 2013, attacks requiring over six people to mitigate rose to 39 percent compared to 25 percent in 2012, a 56 percent increase.

In addition, Neustar's research highlights an increase in a trend dubbed "smokescreening." These types of DDoS attacks are used by cybercriminals in order to divert IT department attention while malware and viruses are inserted within a business network, with the overall aim of stealing valuable data or funds.

Rodney Joffe, Senior Vice President and Technology Fellow at Neustar commented:

Organisations must remain constantly vigilant and abreast of the latest threats. As an example, Neustar’s UltraDNS network suffered an attack just last week peaking at over 250Gbps — a massive attack by industry standards. Even with proper mitigations in place, the attack caused an upstream ripple. It is a constantly changing threat landscape.

In February, Web performance company CloudFlare reported the mitigation of a DDoS attack on a French website which reached a record-setting attack of at least 325Gbps, and a potential reach of 400Gbps.