Distributed Denial-of-Service (DDoS) Attacks and Website Defacement

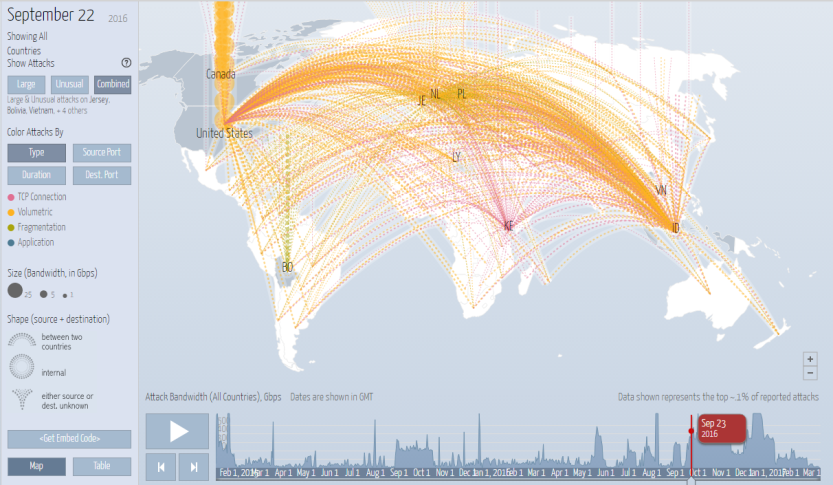
DDoS attacks and the defacement of websites are methods sometimes used by hacktivist groups such as Anonymous and LulzSec and are one of the more controversial hacktivist activities.

# What is a DDoS attack?

DDoS attacks target one or more web-servers, usually of a legitimate business, in an attempt to prevent access to it by legitimate or otherwise authorised users. This is done by flooding the target server with malformed packets or HTTP/TCP requests in an attempt to exhaust the server bandwidth or hardware resources as it attempts to respond the massive flood of incoming requests. Once the bandwidth or resources are exhausted the server is unable to service any more requests, legitimate or otherwise.

They are a distinct form of Denial-of-Service (DoS) attack as they utilise a distributed, co-ordinated network of computers (Botnet) that are usually themselves hijacked computers (but can be any internet-connected device) exploited by the use of backdoors, worms or Trojans. The owners of these computers are usually unaware that their system has been compromised and exploited to this end. The benefit of the Botnet to the attack perpetrator is that the attack intensity is massively increased by this distribution, and any attempt to locate the original attacker by security services or law enforcement is made much harder.

Such acts are often carried out by hacktivist groups as retaliation for real or perceived unethical activity by the target organisation. The October 2016 DDoS cyberattack of Dyn, a DNS Provider, was purportedly carried out by Anonymous (who claimed responsibility) in retaliation for the Ecuadorian governments’ prohibition of the internet access of Julian Assange while he resided at the Ecuadorian embassy in London. The attack affected services of hundreds of major internet services such as Amazon, BBC and Netflix.



*Fig 1. KrebsOnSecurity (cybersecurity research group) DDoS attack map – 21/09/2016*

# What is Website Defacement?

Website Defacement is a form of digital vandalism in which the unauthorised altering of a targeted websites code in order to change its appearance and sometimes also its behaviour. This is achieved by exploiting weaknesses in the websites security using SQL injections, compromised content management services (e.g WordPress) or by hacking the web server hosting the site.

The sites’ original content might be replaced with the perpetrators’ own content, in the case of a hacktivist group often with a political message of their own stating their motives for the act and promoting the individual or groups own political ideals.

One example of this is the April 2014 defacement of hundreds of Israeli websites by the hacktivist group Anonymous as part of its so-called #OpIsrael campaign. The targeted websites’ content was replaced with images promoting Anonymous and their demands for Israel to cease what Anonymous claimed was unwarranted aggression by Israel towards Palestine.



*Fig 2. Israeli website defacement by Anonymous -April 2014*

## Impact of DDoS Attacks

DDoS attacks are a phenomenon that has been steadily on the increase in recent years. To resolve an attack a business must expend manpower to “fire-fight” the issue to bring their servers back online. Also customer support sees the largest surge in activity due to unhappy customers flooding call-centres with enquiries, which also reflects the loss of customer confidence in the brand, which is a longer-lasting after-effect.

During the time the services are down, revenue is lost by the organisations inability to service legitimate requests.

There is also theft of funds, data or intellectual property which has a massive impact on an organisation.

The social impact of hacktivist DDoSing is seen in the media coverage of such events.

This has led to many hacktivist groups targeting companies because of their brand visibility rather than their policies.

In 2014 LulzSec targeted various organisations such as the Sony Playstation network with a DDoS attack that brought down websites, networks and also allowed them to steal huge quantities of sensitive user data. While no direct motive against the organisations targeted existed; LulzSecs’ fame grew and they were then able to promote their political ideologies more easily.