Denial of Service Insurance Scheme Concept Outline

Perhaps one of the greatest threats to freedom of speech online, and in particular to human rights organizations and other voices critical of governments, comes from the increasing prevalence of denial of service (DoS) attacks. These attacks temporarily take websites down by overwhelming the site's servers with a large amount of bogus requests or by exploiting a vulnerability to tax a site's resources. Moreover, the perpetrators of such attacks may achieve "censorship by economics," given the limited financial capacity of many sites to pay for the increased costs associated with mitigating DoS attacks.

Indeed, DoS has emerged as a favorite cyber weapon of repressive governments and patriotic hackers as this kind of attack is a more subtle form of censorship. It's very hard for anyone other than the sysadmin of the site to tell why the site has gone down, and most users only see a generic timeout error message, which can occur for a large number of reasons. Moreover, since the attacker is taking the target site's servers down, rather than blocking it (that other favorite tool of repressive governments), no amount of circumvention software will help an end-user gain access to the site.

However, it is not just small activist websites that get DoSed, this form of attack is one of the most significant threats to cyber security of private corporations as well. While there have been some very high-profile DoS attacks on Amazon, Visa, Master Card, and PayPal perpetrated by Anonymous, small and medium sized companies are frequently coming under attack as well. Just last month, the FBI's Cyber Crimes Task Force conducted an investigation into a series of DoS attacks against websites of US-based battery retailers, such as batteriesplus.com and batteries4less.com. The investigation blamed the attack on a pair of botnets using two Russian web domains and an ISP in Romania.[1]

While data on bank security practices is understandably difficult to obtain, industry insiders tell Access that banks and governments are spending small fortunes defending themselves from DoS attacks as well.

While there are several strategies to successfully mitigating the effects of a DoS attack (see Access' guide "Defending Against Denial of Service")[2], the key cost associated with such attacks – whether the site remains online or not – is the extra time and resources (e.g., bandwidth) required to mitigate a determined attack. Moreover, while DoS attacks for most sites are few and far between, just one hour of a site being unavailable can be devastating for business and tremendously expensive in terms of wasted staff and server resources. Given the incredible investment websites large and small are making in DoS protection, Access believes that there

[1] http://www.infosecurity-us.com/view/20346/DoS-attacks-increasingly-target-small-and-mediumsize-firms/

[2] https://www.accessnow.org/page/-/docs/Defending_Against_Denial_of_Service.pdf

would be ample interest in a DoS insurance scheme.

While many corporations and some civil society sites invest in installing Denial of Service Protection (DoSP) on their own servers, this is 1) prohibitively expensive for most websites (profit and not-for-profit alike) and 2) virtually all upstream providers already have DoSP from providers, such as Arbor Networks[3] and CiscoGuard[4]. Put another way, DoSP is already in place on the pipes of nearly all upstream providers and these providers are currently paying the full cost of such protection. Thus, DoSP could be deployed immediately upon entrance to the DoS insurance scheme, with the beneficiaries of this protection now sharing some of the cost of this technology, but at a significantly lower rate than if they installed DoSP on their own servers (further downstream). Moreover, the funds generate under this scheme, could be reinvested to fuel the development of more efficacious and cost-effective DoS mitigation technologies.

Under this scheme, websites interested in obtaining this service would undergo regular monitoring to gauge their baseline of normal bandwidth usage. A new baseline would be calculated regularly, say every two weeks, and the insurance scheme would cover any additional bandwidth costs associated with a DoS attack. To be clear, the DoS insurance scheme would not cover normal increases in site usage which may occur as sites become more popular. However, by doing rolling assessments of baseline bandwidth usage, it should be easy to make this distinction.

Given the tremendous amounts of money that corporations and activists sites alike are currently spending on DoSP, this insurance scheme would offer a far more cost-effective, easy, and efficient means of defending against such attacks.

This concept is still in development and Access welcomes feedback from the sector.
For questions, comments, or more information, please email: info@accessnow.org

[3] http://www.arbornetworks.com/Access
[4] https://www.cisco.com/en/US/products/ps5888/index.html