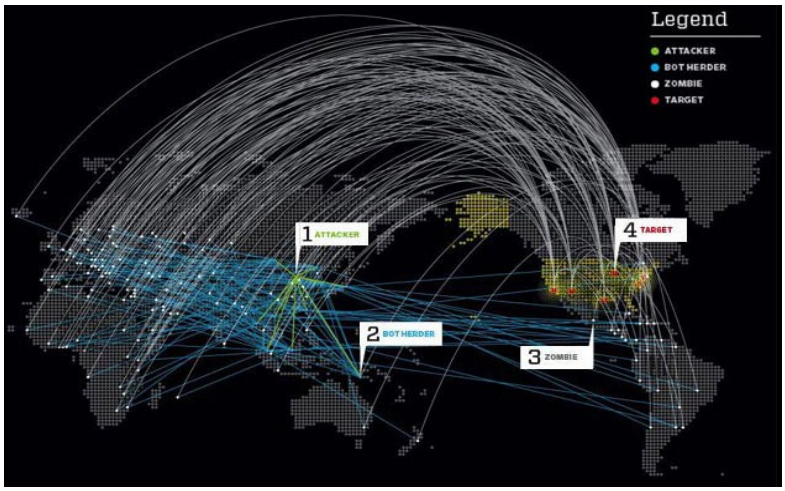
Title: “DDoS and Cloud”

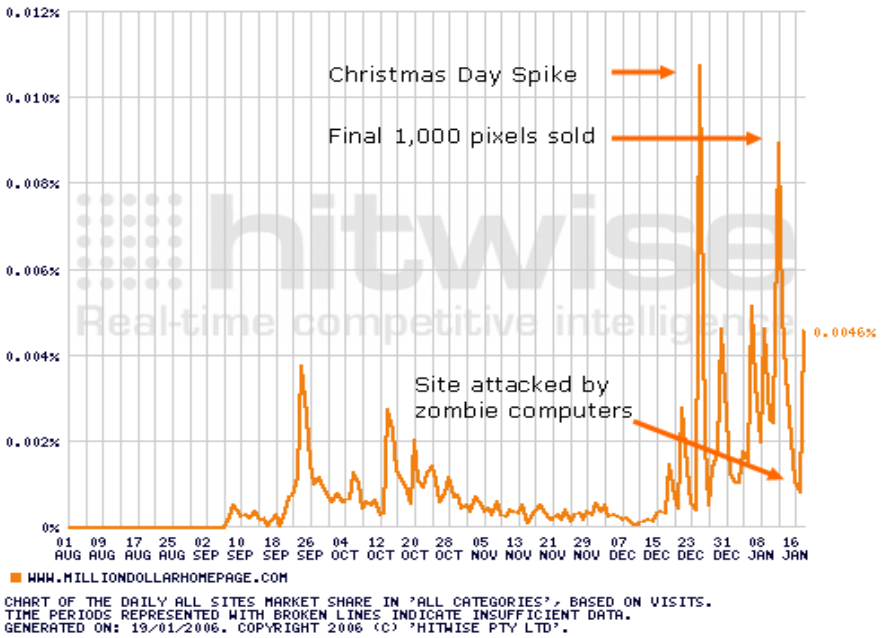
Description

Distributed DoS attacks pose an interesting *trade-off* to the services hosted on cloud, independently of the facility protection guaranteed by your cloud provider.

Botnets are being used in increasingly creative ways to deny service, which makes it much more difficult to resolve this sort of attack. Moreover, modern attackers do not need to attack your entire infrastructure. They can choose the most resource-intensive application that you are running on the cloud and use low-bandwidth attacks to take out your access to that service. Co-location poses other unique threats. When your cloud services reside on a cloud provider, you need to worry not only about attacks on your cloud resources, but on the resources of other tenants.



On the other hand, cloud computing offers unique opportunities to recover quickly from DDoS attacks because a provider has the ability to rapidly provision resources. If the agility of the cloud can really come into play during a DDoS attack, you should avoid to use elastic capacity to serve a large amount of *undesired traffic* because it may cause a huge bill from your cloud provider, even higher than the cost of the attack itself.



Objectives

Assume the you manage a Web-based service through a cloud provider.

- *Scenario 1*: No economy-relation between your service and your users is involved in the service.
- *Scenario 2*: A basic form of payment is required to access to portions of your Web-based service (e.g., annual inscription fee).
- *Scenario 3*: The Web-based service includes some e-commerce transactions.

State of the art

- Outline in at most 2 pages the main solutions proposed to **detect** and **mitigate** the effects of DDoS attacks. [Avoid to consider the traceback problem unless it is useful to address the detection and mitigation issue.]
- Focus on solutions that can be integrated with cloud platforms and motivate your choices by taking into account the three scenarios. Separate the detection from the mitigation issues.

Design a "technological-based" solution

Possible ways of investigations

- Network-based mechanisms (see [2])
- Is an overlay scheme, such as that proposed in [3], extensible to clouds?
- Is it possible/convenient to use an intermediate entity (*broker*) operating through multiple cloud providers.

Integrate a "cost-based" solution

1. Analyze the trade-off of the attack *vs* defense costs from an economic point of view. Pick one or more scenarios. Take into account the costs related to the infrastructure, traffic, elasticity, etc. of one popular cloud provider (e.g., Amazon)
2. Then,
    - If you have investigated multiple technological-based solutions, evaluate which is more convenient from an economic point of view.
    - If you have investigated one technological-based solution, evaluate whether it is feasible from an economic point of view.

References (*just as a starting point*)

[1] "Above the Clouds: A Berkeley View of Cloud Computing" - *A must-read introduction*

[2] "Survey of network-based defense mechanisms countering the DoS and DDoS problems"

[3] "OverDoSe: A Generic DDoS Protection Service Using an Overlay Network"