

Assessing The Risk of Becoming a DDOS Target

In today's DDOS environment it is very difficult to evaluate the risk of an organization's becoming the target of an attack. In some cases one can discern a clear link between the attack and the nature of the organization's business, related to competition or attempted extortion. In some cases the general economic and political climate can trigger an attack. In other cases, however, the target may be chosen to mask an attack on another business; the victim may seem an innocent and unlikely target. A rising number of attacks appear to be truly accidental.

While there are no easy predictors of the likelihood of attack, it helps to understand that attacks can be classified as either DIRECT or INDIRECT.

REASONS FOR A DIRECT ATTACK:

1. Anti competitive business practices. Online competitors of the target organization may use DDOS to try to gain an unfair business advantage by disabling the target's web site.
2. Extortion. Attackers attempt to extort payment, usually for small dollar amounts, in exchange for stopping a DDOS attack and "protecting" the target from future interference. These attacks can be relentless and are often successful because the target is willing to pay a small amount to make the problem go away. As in other "protection rackets," victims are often reluctant to inform the authorities, and it is hard to know how widespread this illegal practice is.
3. Political manipulation. Parties or governments can use DDOS as a tool to hinder freedom of speech on the Internet.
4. To hoard on line discussion access. A participant in an online discussion who wishes to prevent further debate may DDOS the web site, in effect "freezing" the site for hours or days with his or her statement as the last point made in the discussion.
5. To obtain unfair advantage in on line games. It is very common for computer-savvy gamers to use a DDOS/DOS attack on the web site to knock a competitor off!
6. National interests.

REASONS FOR AN INDIRECT ATTACK:

1. To disguise other attacks. This is a new use of DDOS that is becoming more prevalent. An attacker desiring to steal information from a server will use a DDOS attack on another unrelated server located at the same hosting center. In responding to the DDOS attack, the server's traditional IDS/IPS becomes heavily loaded and cannot prevent the information theft.
2. Accidental attacks. A small but increasing number of attacks on the network are probably unintended, the result bugs in software that malfunctioned.
3. Wrong targets. In some cases, a coordinated attack may target the wrong name or IP address!
4. Shared facilities with a DDOS victim.

A few years ago, business organizations could legitimately say, "my site does no wrong" and therefore expect to be safe from DDOS attacks. Today, with indirect attacks rising in frequency, every organization faces a rising risk of DDOS attack.

How Bad Is The DDOS Environment?

In past years, the extent of a DDOS attack was measured by the “back scattering” effect: observing network responses to forged IP addresses used in the attack. This measurement was a very good approximation when most of the DDOS attacks uses forged, random IP source addresses. Today, attacks are much more focused and refined, including the use of real BOT IP addresses. Attacks with real IP addresses are not observable by scattering methods, resulting in a significant under-counting of DDOS events.

New tools, based on actual observation points in the network, have reported varying degrees of DDOS severity. Using this new observation method, RioRey has gathered data confirming that DDOS BOTs are everywhere. The map in Figure 1 plots the location of attacker IP addresses as observed by 25 RioRey observation points. The colors represent different attack types, and the color intensity reflects the intensity of attacks from that region of the map. The darker the color, the more attacks emanated from that region.

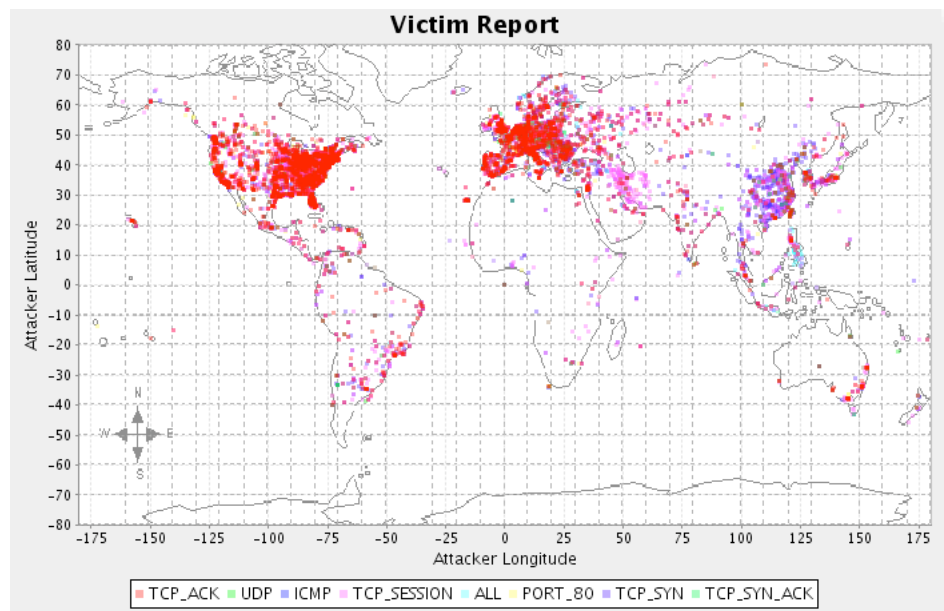


Figure 1. Map of DDOS attacker location, as observed by 25 RioRey observation points

Evaluating The Cost Of A DDOS Attack

A DDOS attack, if not mitigated, will disable a website for the duration of the attack. In dollar amount, the cost of this interference will vary with the size of the business or government organization. However, since DDOS disables all functions of the ebusiness for hours or days, the consequence is equally devastating. If an organization is caught unprepared, the effort to research and implement an effective solution while under fire is a formidable challenge and a drain on resources.

On an average basis, many estimate the potential loss to a large corporation as \$250k per hour of DDOS attack. Using this number, with an average attack duration of several days, the losses to the organization can be substantial.



RioRey Benefits

The RioRey algorithm is designed to detect and mitigate a DDOS attack within 90 seconds of the start of an attack. The RioRey system does not require base-lining network characteristics, nor does it require known signatures of an attack.

These unique feature allow RioRey to analyze and resolve new attacks quickly, in addition to addressing known attacks in a timely fashion. RioRey protection costs a fraction of the estimated \$250k a corporation may lose in one hour of down time during one attack.

RioRey has had dramatic success in a number of cases with persistent DDOS attackers who were able to vary their forms of attack.

A notable example is the case of a client in the UK which was the target of cyber extortion. In March 2008, company came under severe DDOS attack every week from Tuesday to Friday, and the attacker demanded payment in return for stopping the attack. The company refused to pay and tried many solutions, including migrating to larger hosting companies which were supposed to offer DDOS defense capabilities. They also requested help from Scotland Yard to identify and shut down the attacker. Law enforcement was in fact able to identify and suppress several active botnets used in the attacks; however, the attackers were resourceful and determined, and the attacks against the company continued. They company was realizing significant losses in their on line business.

When the company deployed the RioRey solution, we were able to mitigate the attacks, despite the attacker's resort to new forms of DDOS. The UK company was back in service; even though the attacks continued, they could not disrupt the web site. Two weeks after the RioRey installation, the attackers gave up and stopped their attacks all together, realizing that their attacks were no longer effective.

RioRey solution is the only real solution to this UK company and many others.