Security’s Not Just About Defense
Gain an Advantage over Cyber Attacks with a Counter-Offense

Expert Commentary By Avi Chesla
Chief Technology Officer, Radware
September, 2011

Today’s attacks have demonstrated a valuable lesson: companies will not stop attacks with their current defenses - they will only “absorb” them. This will not be enough in the future!

Imagine there was a way to dissuade or even “neutralize” your attacker wherever they are… this is what a counter-attack operation is all about.

Overview
In any conflict, defensive forces are never designed or reasonably expected to withstand an attack indefinitely. Among the reasons why a long-term defensive operation is a losing strategy are as follows:

- Limited Resources - the amount of resources required to absorb an attack and resupply
- Maintaining Performance Levels - in a war of attrition, endurance is king
- Morale or “Espirit-de-corps”- the morale of a group decreases when no progress is shown

Most successful strategists are aware that in order to beat an enemy you must take the battle to them. The goal of long-term persistent and sustained attacks is to “hold” the enemy until such time whereby you can launch and sustain offensive operations. The front line of defense in any battle will eventually be breached and this assumption is also true in the realm of the information security battle of defense.

So the question now is, back to corporate information technology, how does this apply to us in our daily lives?

As a defender protected by network security products, you may never feel confident that your product will provide sufficient security protection under all circumstances. The cyber enemy will try to surprise you in many ways and if persistent and intelligent, will eventually find one that you weren’t prepared for. As a result, this is exactly where the enemy will focus efforts in order to wear you down and penetrate through all your defense layers.

There is a strategy that was developed to address the inherent inferiority of a defending force versus an attacking force: it is called a “Counter-Attack”.

Counter- Attack
A counter-attack is the term used to describe large scale, usually strategic offensive operations by forces that had successfully halted an enemy’s offensive, while occupying defensive positions. A counter-attack is considered to be the most efficient means of forcing the attacker to abandon offensive plans.

1 A counter-attack is sometimes also called a counter-offensive
The counter attack operation should be well prepared in order to hit the attacking forces precisely in their weak spots, thus impeding the attacker’s capabilities, both physical and motivational, in the most effective way possible. These weak spots can and should be identified before and during the battle by field intelligence. There are three main conditions that need to be met in order for a counter offense to be successful:

- The enemy’s weak spots must be successfully identified
- The defense force must be well trained to conduct a counter attack operation
- The defense force must successfully halt the enemy’s offense

In the realm of cyber attacks, the concept of a counter-attack operation must also play a major role in the defense strategy against emerging cyber threats. The counter-attack approach could be a game changer, as it enables us to overcome limitations in existing defense strategies against cyber attacks.

This article explains Radware’s cyber attack mitigation strategy, with emphasis on the counter-attack operation – a unique approach to attack mitigation that Radware’s security technologies and Emergency Response Team (ERT) implement.

**Breaching the Perimeter Borders**

In the realm of information security, counter attack operations are all about reaching the origin of the attacks and impacting them in a way that will reverse the power relationship in favor of the defenders.

Cyber attackers are becoming more and more persistent. They are capable of harming online businesses, regardless of their motivations, with a wide arsenal of attack techniques and tools. Today’s attackers aim to deny service (DoS attack) take control or steal information through different attack methods at the network and application levels, through either highly visible large volume attacks or more low rate and stealthy types of attacks. Sometimes both attack types are used simultaneously in order to conduct as successful attack campaign against the target organization.

Persistent attackers will use different tools aiming to exploit weaknesses in the different layers of defense. Once a weakness is spotted in one of the layers, an effort that sometimes can take days (a persistent attack campaign will eventually discover a weakness), the attacker will focus his efforts on exploiting it as much as possible. Today’s attack operations can recruit an “infinite” amount of resources such as Bot infected machines, voluntary attackers who take part in larger coordinated campaigns such as hacktivists, and non-voluntary attackers who take part in the attack – This makes the power relationship between attackers and defenders extremely challenging.

The answer to the question of how on-line businesses and organizations can reduce the probability of becoming a victim of these persistent advanced attacks or how to resist these attacks in a way that will render them unsuccessful, has a lot to do with the counter attack operation approach.

Ideally we would like to get as close as possible to each attacker and neutralize his ability to generate the attack traffic, thus cleaning the “bad” traffic end to end – a very effective way to neutralize DDoS attacks. We also try to create a situation in which the attacker’s machines are slowed down or even halted, thus making them quit the whole attack campaign for obvious reasons. This last option can really reverse the “unfair” power relationship between the attackers and the defenders and result in a successful counter attack operation.
In order to do all of the above, the defense mechanisms should virtually “breach” the network perimeter borders – the following diagrams illustrate this:

As shown in the above illustrations (Figures 1 and 2), there are a few perimeter borders that the attack traverses from its origin to the target destination. The closer the mitigation process to the attack’s origin, the better the cleaning will be – this is what we define as end-to-end mitigation. Moreover, if the mitigation technique can naturalize the attack tool, through a counter attack technique, the effect becomes much stronger as it essentially “exhausts” the attacker – making him rethink the plausibility of continuing the attack effort on the target, or of launching a similar attack on the target in the future.
The main advantage of the counter-attack is that it reaches the source wherever it is, virtually breaching all network perimeter borders. All this is done without the need to physically deploy a network security device in each one of these perimeters.

To summarize, the main advantages of a counter-attack are:

1. Virtually extending the network perimeter of defense up to the attack origin
2. “Exhausting” the attacker in a way that will make him quit the attack campaign
3. Reversing the “impossible” power relationships between the attackers and defenders

**Notable Attack Campaigns**

By all indications, 2010 and 2011 will go down in the record books as one of the most active periods of cyber-hacktivism in the history of cyber threats. Moreover, given the current efficacy of hacktivist attacks such as the WikiLeaks revenge attacks (December 2010) and the South Korea DDoS attacks (March 2011), we believe this will only serve to encourage even more actors to enter the picture and spawn a vicious cycle of future malicious activity.

To demonstrate the rise in frequency of attacks, below is a list of notable attack campaigns that took place over the past year alone:

- September 2010, a new DoS & DDoS commercial Botnet (IMDDoS) based in China openly sells DDoS-for-hire services and manages to plant roots inside a number of major ISPs all over the world.
- December 7th 2010, DoS & DDoS attacks, undertaken by supporters of the WikiLeaks website (group Anonymous), on businesses including MasterCard, Visa, PayPal, the Swedish Prosecutors office, Swiss Post Finance bank, Amazon and others.
- March 4th 2011, DoS & DDoS attack on Wordpress.com severely disrupts operations
- March 6th 2011, DoS & DDoS attack on Korean e-Commerce and government institutions
- March 6th 2011, attack on the French government’s interest in the G20
- March 9th 2011, DoS & DDoS attack on Codero managed hosting provider – disrupting Twitter
- March 9th 2011, group Anonymous declares a new “Operation Payback” against BMI.com and calls for sustained and disabling attacks from its contributing members.

And more…

**Multi-Vulnerability Attack Campaigns**

The impact resulting from these attacks was significant. The attacks were difficult to defend against, as they were aimed at multi-vulnerability points in the network including network infrastructure equipment, TCP/IP stacks and server applications and were generated from multiple sources (distributed attacks). These multi-vulnerability attacks included high volume DDoS attacks as well as “Low & Slow” attacks – all which were generated simultaneously against multiple weakness points in the networks.

Each of the above attacks represented very effective attack campaigns and each of them was both simple in execution and difficult to defend against.

The whole concept of the counter-attack approach discussed in this paper brings another level of defense (or in our case offense activities) against these emerging threats.
Counter Attack Techniques
Effective cyber counterattack should follow the following steps:

1. **Attack detection and blocking**
2. **Attack tool identification**
3. **Identifying known attack tool weaknesses in real-time or based on previous information**
4. **Counterattack generation to exploit the tool’s identified weakness**
5. **Slow down or completely neutralize the attack tool**

The 1st attack detection and blocking steps construe the traditional way of handling cyber attacks. The following steps are characteristic of counter attacks:

**Attack tool identification** – Identification of the attack tool used as a vehicle to carry the attack campaign is done through pattern matching. There are hundreds of attack tools used in today’s “cyber attack market place”, each one of them can generate different types of attacks. Each attack tool has some kind of fingerprint, invariant to the attack content itself, which can be detected through different pattern matching algorithms.

**Identifying tool’s weaknesses** – Conducting research can expose inherent weaknesses in each attack tool. Counterattack motivated research will to find ways of neutralizing the tool in a “passive”, non intrusive way. There are different methods to manually or automatically discover tool weaknesses which are out of the scope of this paper.

One example of a weakness is the TCP congestion control mechanism that is discussed below.

**Exploiting the TCP Congestion Control “Weakness”**
Attack tools that rely on the operating system TCP congestion control algorithm would usually include a weakness that would allow the generation of a counterattack operation that can exploit it and thus “exhaust” the stack and CPU resources of the machine these tools reside on.

Without going into too many technical details, a TCP connection congestion control mechanism was designed to transfer larger chunks of traffic (packets) as long as no traffic congestion is identified (e.g., no packet drops, relativity short round trip time etc.). On the other hand if the mechanism identifies congestion, then it will automatically “slow down” the data transmission rate per each connection and will gradually accelerate it once the congestion ceases to exist - this process is called “slow start” and makes the whole data transmission longer.

Imagine an attack tool that tries to generate new attack connections (with data in them) as fast as the OS is allowing him to. If we can create a situation in which the “slow-start” process will kick in on every TCP connection, then the lifetime of each attack connection will become longer. This will create an increasing number of simultaneous connections that will eventually exhaust the OS memory and CPU resources. All this means that a good counterattack operation needs to create a condition in which the slow start process will be activated on any connection that the attack tool tries to generate, over and over again, thus slowing down or even crashing the attacker’s machine.
The following two diagrams illustrate the above slow start process and its impact on a single connection’s lifetime:

![Figure 3 – TCP connection without “slow-start”](image1.png)

![Figure 4 – TCP connection with multiple “slow-starts”](image2.png)

Figure 4 above shows what happens when we choose, for example, to drop a data packet inside a connection, in a certain offset, in order to simulate a congestion condition. In this case the “slow-start” process is initiated, meaning that it will take more time to transmit the same amount of data (see Figure 3 above).
Counterattack generation – The congestion simulation action discussed above is one example of a counterattack that exploits a weakness in an attack tool that utilizes the TCP congestion control mechanism. Different counterattack actions should be generated based on the identification of the attack tool and the attack that it is launches. Actions such as TCP reset, application challenge/response, manipulation of the window size (e.g., “tarpit” actions) and others are all applicable counter attack actions.

If the attack and attack tool are identified correctly, and mapped to the right counter attack action, then the final result is neutralization of the attack tool.

Conclusions
With the counterattack we aim to achieve the following:

- Remove the inherent advantage that offensive forces usually have over defense forces
- Exhaust the attackers’ resources, physically and mentally, wherever they are
- Clean the attack traffic end to end, breaching all network perimeters borders

Achieving these goals is far from trivial. It requires a strong security research team that is on top of the most advanced attack tools, security products that can accurately identify the attack, the tool that carries it and is then able to generate the counterattack action based on the pre-defined counterattack actions associated with each attack tool’s weakness.

However, the counterattack provides, perhaps for the first time, an opportunity to gain a real advantage over financially motivated cybercrime organizations, hacktivists, and other attackers with malicious intents.