

SHARE THE ERT REPORT



## Table of Contents

# 01

### **Executive Summary**

- » Most important findings

# 02

### **Introduction**

- » Scope of the Report
- » Industry Security Survey
- » ERT Cases

# 03

### **Trends**

- » Organizations Are Bringing a Knife to a Gunfight
- » The Year of DNS Attacks
- » The HTTPS Challenge
- » Hackers Can See Through Your CDN
- » 2012 vs. 2011  
– Quick Trends

# 04

### **Attack Tool Trends**

- » DDoS Do It Yourself
- » Services Enlisted to the Botnets Army

# 05

### **Mitigation Trends**

- » Mitigating Attacks that Pass the CDN

# 06

### **Summary**

- » Recommendations for the Network and Security Community



## Executive Summary

Denial-of-service and distributed denial-of-service (DoS/DDoS) attacks are peculiar in the world of Internet security. First, they do not exploit a vulnerability that needs to be patched; second, each attack packet on its own is legitimate— with only the combination becoming destructive and third, the attacks are lengthy – lasting hours or days, rather than seconds and minutes.

For many years denial-of-service and distributed denial-of-service (DoS/DDoS) attacks did not receive much attention because they were considered niche attacks. This changed dramatically in 2011 when the Anonymous group selected DoS/DDoS as their primary attack method. Fueled by the attacks' power and destructive results, Anonymous turned this into its mainstream attack type by making it well known and widely available to not only the security community, but also the general public. Even though the group's activities decreased in 2012, it laid the groundwork and a precedent was set. Multiple groups have already adopted DoS/DDoS attacks - hackers, financially motivated criminal organizations, and even governments, attracted to its power. Unfortunately, it seems that DoS/DDoS attacks will remain a prominent and persistent threat in 2013.

This report is dedicated to sharing insights and knowledge about both sides of the DoS/DDoS battle – attackers and defenders. Hopefully, this research will provide useful intelligence about opponents, and more importantly - will allow organizations to better detect, mitigate, and win the extended and persistent DoS/DDoS battle. Furthermore, these insights have a larger scope, and can be applied to other security domains that are also turning into long 'attack campaigns'. What is known about DoS/DDoS today will be needed in other domains tomorrow – as the principles are the same.

## What Changed in Security in 2012?

In 2012, we saw a new cyber security trend – a consistent and steady increase in advanced and persistent DoS and DDoS attack campaigns. These campaigns have multiple attack vectors, are longer in duration and are more complex. Nowadays it's common to see attacks with four, five, or even ten attack vectors, lasting last three days, a week or even a month. This new trend of advanced and persistent threats creates big challenges and organizations are not prepared.

## Organizations Are Bringing a Knife to a Gunfight

When we say “Organizations are bringing a knife to a gunfight”, we mean that they are entering into a security battle without understanding the true nature of the fight and they are not adequately prepared. They invest in pre-attack phase preparation and excellent forensics for the post-attack phase. However, organizations have one critical blind-spot – they don't have capabilities or resources to apply during the attack phase, and can't sustain a long, complicated attack campaign. Attackers, on the other hand, understand this blind spot and use it to their advantage. The result is outage time, with service availability impacted, even in the most respectable online services.

## How to Stop Sophisticated Attack Campaigns

To stop these attack campaigns, organizations need to change their defense strategy from a two-phase security approach to a three-phase security approach.

A two-phase approach has a pre-attack phase and a post-attack phase. The pre-attack phase includes readying for an attack – securing mitigation solutions, deploying security systems, etc. The post-attack phase includes conducting forensics, drawing conclusions and improving for the next attack. This was sufficient as long as the attacks were short in time.

Now, with attack campaigns lasting days or weeks, organizations need to add a third phase – with the defense strategy planned **DURING** the attack. The most important component to support this is to have a dedicated team of experts who can not only dynamically respond during the attack, but also launch a counter measure to stop the attack and then learn from the information gathered, to mitigate future attacks. It is unreasonable for an organization to assemble the required manpower and expertise, considering that it may only experience a few attacks per year. Organizations should therefore search for additional competencies externally - from security experts, vertical alliances, or government services. It is only with such an on-demand service and force multiplier teams that organizations will be able to win in the security arena.

## What Can We Learn?

Advanced and persistent DoS and DDoS attack campaigns are indeed frustrating and dangerous, but they also provide some very valuable opportunities. For the first time ever, security experts can collect real-time and specific intelligence about the attacker – who they are and what tools they're using. This finally gives organizations the chance to fight back during an attack, deploy counter measure techniques against the attackers and stop the attackers at their base.



# Introduction

Radware's annual Global Application & Network Security Report provides insight into network security trends with a specific focus on DoS/DDoS attacks. Intended for the entire security community, this research is designed to deliver a comprehensive and objective summary of network security events and DoS / DDoS attacks that took place in 2012, with an analysis of attack types, trends and mitigation technologies. Altogether, the report draws its information from 274 organizations from two sources:

## Industry Security Survey

The first source for this annual report is an industry-wide security survey, which was conducted by Radware. The survey was sent to a wide variety of organizations globally – both Radware customers and organizations that are not associated with Radware. It was designed to collect objective, vendor-neutral information about issues faced by network operators while combating DoS/DDoS attacks during 2012. The survey consisted of 29 questions which addressed the following topics:

- **Background information** – about the organization and the responder of the survey
- **General security** – security information unrelated to DoS /DDoS
- **DoS / DDoS** – focused on attacks, impact, and mitigation techniques



### **Radware Emergency Response Team Cases**

The second source is an analysis of 95 key security cases –representing various organization types in globally dispersed areas – which were handled by Radware’s Emergency Response Team (ERT) security experts. This provided frontline, first responder testimonials for in-depth insight into attack trends and technical information.

Radware’s ERT provides emergency services with dedicated specialists that respond in real time offering proactive, hands-on mitigation for active threats. The ERT provides real-time assistance to customers under DoS / DDoS attacks by directly accessing customers’ network equipment, capturing files, analyzing the situation and offering various mitigation options.

While the main objective of Radware’s ERT service is to mitigate attacks and help customers recover, the team gets a unique view of each attack. Due to its hands-on involvement, the team views real-time information about attack internals and can measure the attack impact. Generally, the ERT is only called upon to respond to medium to high severity attacks. This provided a deep forensic examination of Dos/DDoS attacks that could not be achieved through the survey.





# Organizations Are Bringing a Knife to a Gunfight

Network attacks have been around almost since the emergence of the Internet. Today, it would be nearly impossible to find an IT organization that is not aware of the assortment of security threats. It would be as difficult to locate an IT security group that did not take precautionary measures, acquire protection gear, and set various lines of defense.

And yet, despite the awareness, preparation and preventive measures - we witness too many organizations that fail to adequately defend themselves against attacks. If you examine last years' press clippings, you'll notice some prominent companies that were under attack. These companies, which undoubtedly have high IT budgets and extensive resources, have succumbed to intense attacks that have taken down their network infrastructure.

We researched this phenomenon – why, despite all efforts, are organizations failing to defend themselves against attacks? What should be done differently?

Our assessment is that organizations are bringing a knife to a gun fight. They are entering into the security battle without being adequately equipped or prepared. They are using obsolete strategies without understanding the scale and power of their opponents, and without the ability to dynamically adjust their defense tactics during prolonged attacks that switch attack vectors. Yet, if we were to point out the single, most prominent reason behind an organizations' failure, it would be because organizations still do not fully grasp the type of battle they are fighting, its magnitude, circumstances and settings.

## High profile organizations that experienced outages over the past 18 months





## Two-Phase Defenses Are No Longer Sufficient

Traditionally, security organizations have focused their efforts and attention on two phases of the security warfare:

- **Pre- attack phase**, in which security groups acquire mitigation solutions, deploy security systems, pen test solutions, etc.
- **Post- attack phase**, in which security groups acquire logging and forensic systems, hire security personnel to analyze logs and conduct forensics, draw conclusions from security events and improve accordingly.

Industry Security Survey  
How much did your organization invest in each of the following security aspects in the last year?

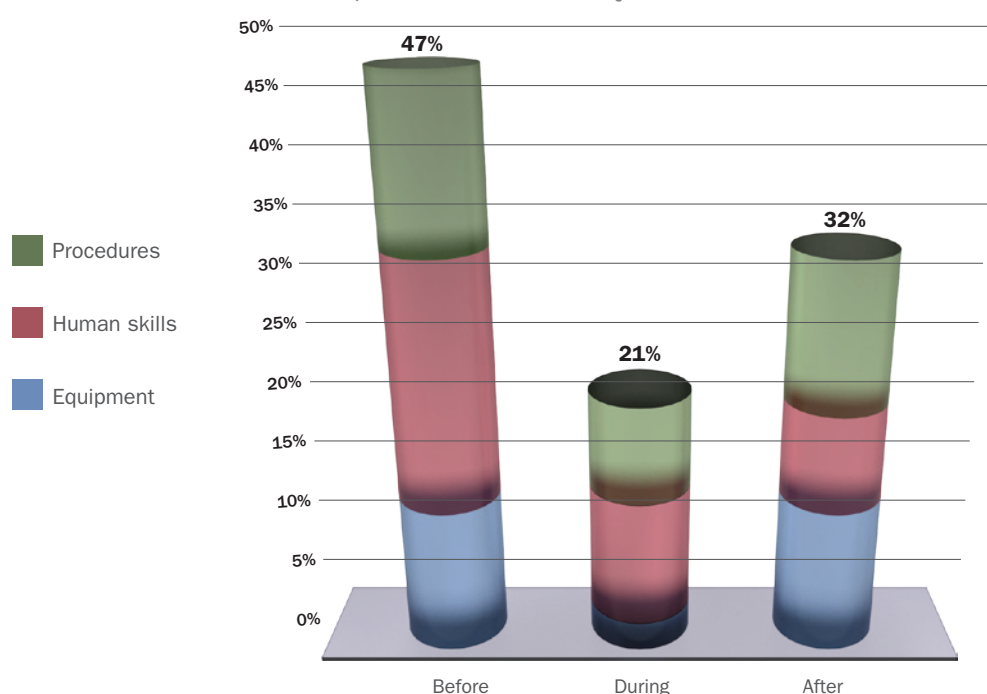


Figure 1: Only 21% of company efforts are invested during the attack itself, while 79% is spent during the pre-attack and post-attack phase.

This behavior is also reflected in the results of the industry security survey, pointing out that companies spend 79% of their time in the pre-attack and post attack phases. Only 21% of the efforts are spent during the attack itself for activities such as operating security real time management systems or putting together a security team to respond and dynamically implement attack mitigation.

This behavior paradigm implicitly assumes that security attacks are short lived, and that pre-attack preparations can suffice to withstand them. Indeed, this was the case for many years, but not anymore. More and more attacks are prolonged and may last for days or even weeks. It is not feasible to win such a battle if you are not prepared to invest sufficient resources during the fight. This assertion applies to all network security domains, though in this report we will focus our argument on the DoS/DDoS domain.

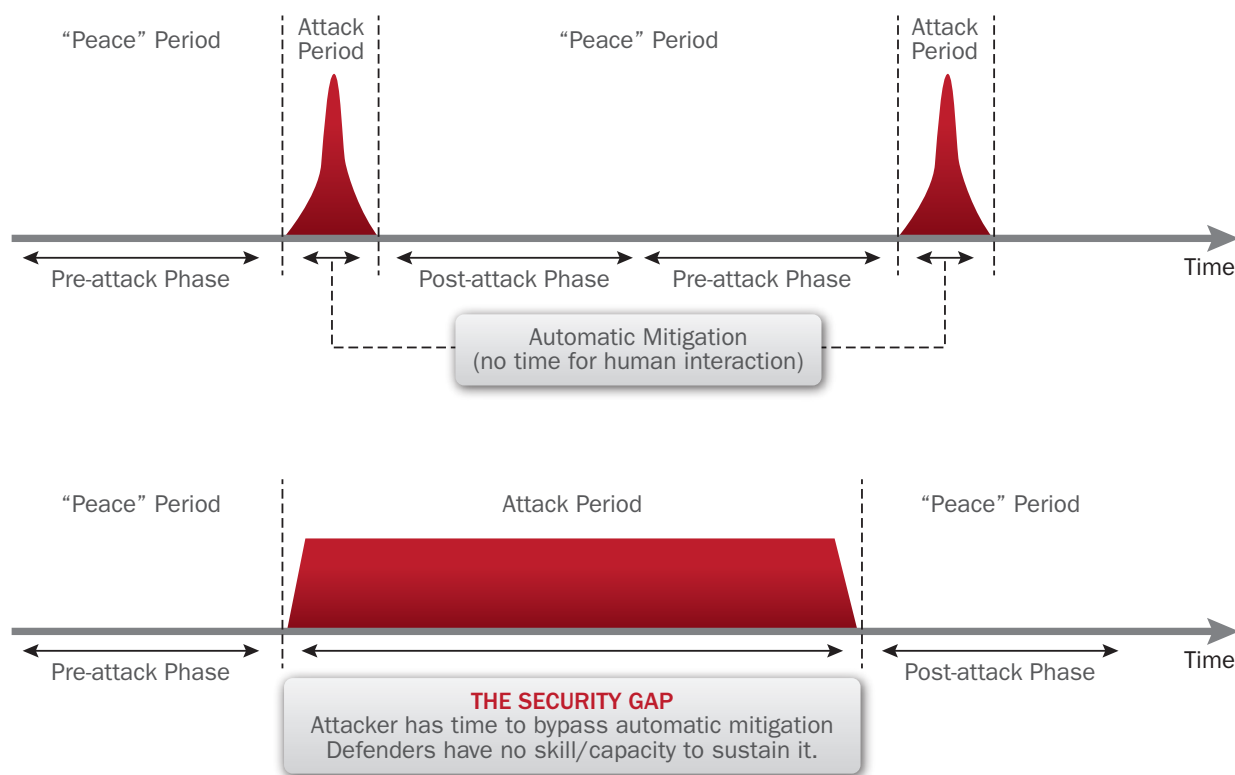


Figure 2: More attacks are prolonged and may last for days or weeks.

Another aspect of attacks, beyond duration, is the use of multiple attack vectors and the ability to dynamically switch between them. Consider an attack that is initially launched using a UDP flood. The attack is identified by the defending organization and blocked; but then the attacker switches to an HTTP flood vector, for which the defender is unprepared and cannot handle in a timely fashion. In practice, attackers use more than two attack vectors, making attack mitigation much more challenging.

## A New World with Different Attack Scale and Magnitude

The Radware ERT sees hundreds of DoS/DDoS attacks each year. We characterized these attacks and asked “what was the top change in attack profiles in 2012”? The response was unequivocal – attack complexity has increased. Attacks became much more forceful, sophisticated and persistent. In other words, attackers are fighting better, stronger, and faster.

## More Severe Attacks with Higher APT Score

To quantify this observation, we developed the Advanced Persistent Threat (APT) Score. The term APT is commonly used in the internet espionage and cyber warfare domains. We defined a scoring system that enables ranking APT attacks methodically by their severity. Each attack is assigned an APT score between 1 and 10 (10 being the most powerful), based on three factors:

- **Attack duration** – the longer the attack lasts, the higher its APT score.
- **Number of attack vectors** – a higher number of detected attack vectors increases the APT score. Attack vectors include the different attack methods used, such as HTTP attack, DNS flood, SSL garbage flood, etc.

- **Attack complexity** – the more complicated the attack vectors, the higher the APT score. For example, a SYN Flood gets a relatively low score; a slow rate attack gets a higher score; and an exotic attack that is rarely seen gets the highest score.

Figure 3 demonstrates the increase in severe DoS/DDoS attacks, as tracked by Radware's ERT cases. In order to avoid trivial attacks and focus on the more severe ones, we discarded the basic attacks that had an APT score below 3.

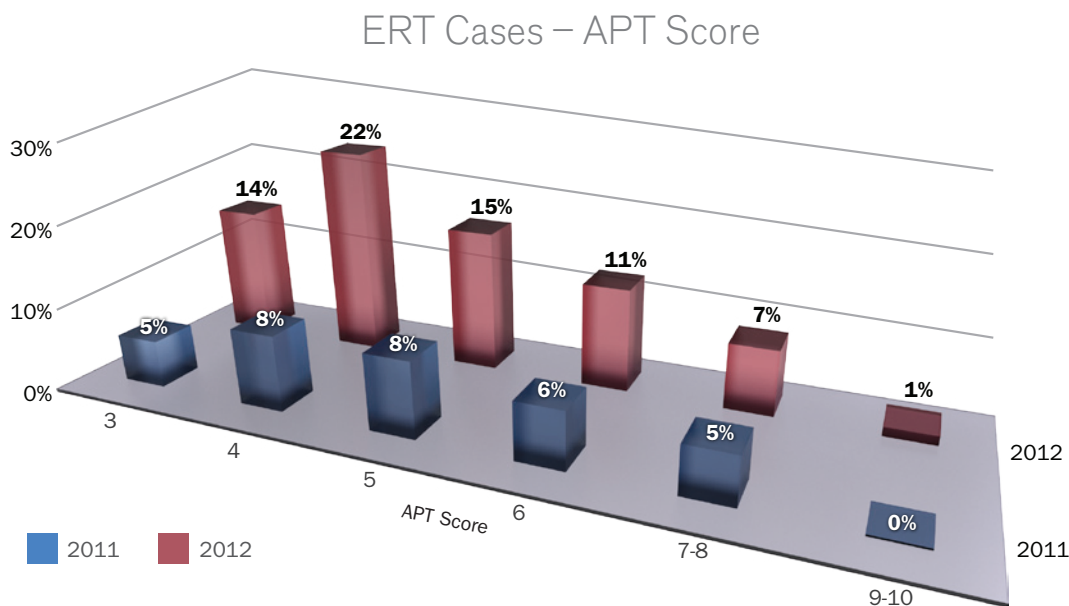


Figure 3: Severe attacks are increasing – The number of severe DoS/DDoS attacks, categorized by a high Advanced Persistent Threat (APT) score has increased in 2012.

It is important to note that powerful attacks also existed in 2011, particularly due to the attacks carried out by the Anonymous group. Consequently, the profile of the APT scores during 2011 is quite similar to 2012, yet the number of high scoring APT attacks has increased. We also see an increase in 2012 when isolating the parameters building the APT score (attack duration, number of attack vectors, and attack complexity).

### ERT Cases – Attack Duration Trend

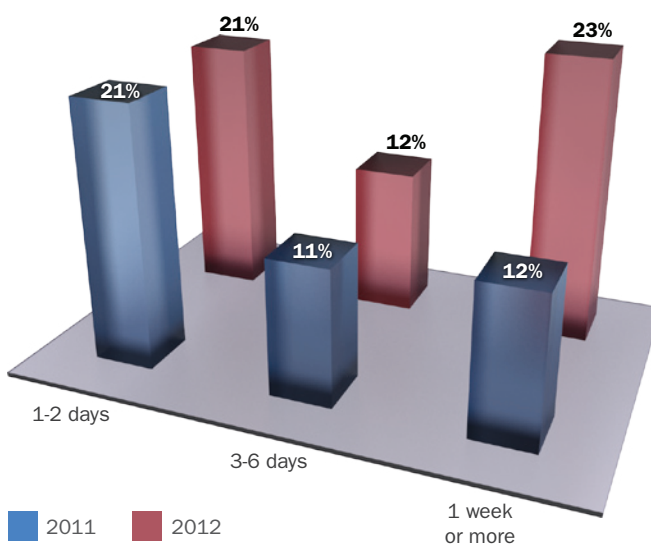


Figure 4: **Attacks last longer** – The number of DoS/DDoS attacks lasting over a week doubled in 2012.

## Expertise

Attackers plan and run attacks on a regular basis, essentially turning DoS/DDoS into their ‘profession.’ In this context, attackers have developed a DDoS supply chain that incorporates DDoS toolkits, distribution mechanisms, and DoS for hire services. Using the readily available DDoS tools and knowledge, novice attackers can leverage the expertise gained by the skilled hackers to launch sophisticated attacks. For more details about this trend, read the [DDoS - Do it Yourself](#) chapter.

Contrarily, defending organizations are way behind as they typically experience only a few DDoS attacks each year. While they may draw some conclusions from one attack towards the next, the experience is too limited to be able to build the required know how.



Figure 6: Defending organizations are behind in expertise, as they experience only a few DoS/DDoS attacks per year.

## ERT Cases – Attack Vectors

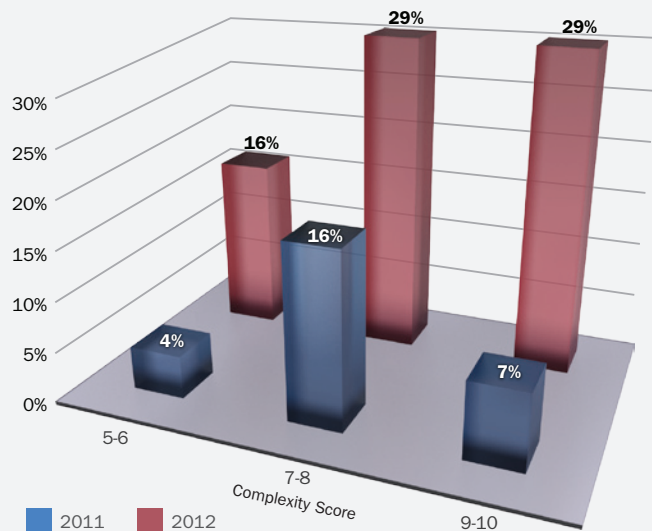


Figure 5: **Attacks are more complex:** 2012 DoS/DDoS attacks have become more sophisticated, using more complex attack vectors. Note the number of attacks using a complexity level of 7-10.

Industry Security Survey  
How likely is it that your  
organization will be attacked  
by cyber warfare?

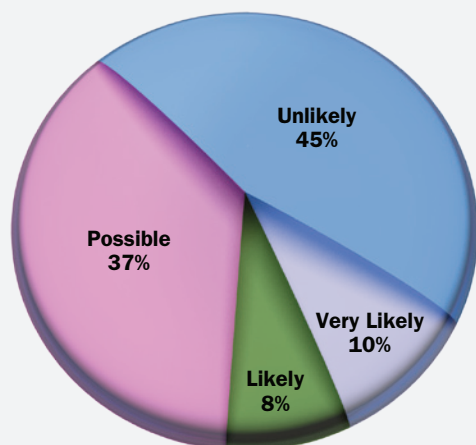


Figure 7: Over half of the organizations believe their organization is likely to be attacked by cyber warfare.

Industry Security Survey  
How well do you think you will  
survive a cyber warfare?

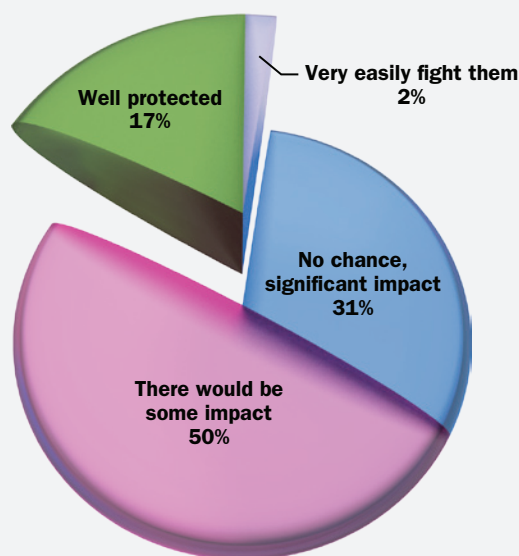


Figure 8: 81% of organizations feel inadequately about protect themselves against cyber-warfare.

## Cyber Warfare is Already Here

Cyber warfare has several definitions, but it generally refers to a politically motivated attack. Cyber warfare attacks are advanced and persistent and extremely difficult to mitigate. The perception of cyber warfare used to be that it only targeted countries and governmental bodies, such as power stations, nuclear plants, etc. This is not the case anymore. Our ERT handled numerous powerful attacks in 2012, which targeted financial institutions, e-commerce sites, cellular networks and other business entities. While it is difficult to be certain that all of these were cyber-warfare attacks (sponsored by governments), they featured all the attributes of cyber warfare in terms of potency, complexity and persistency.

Organizations are acknowledging the cyber warfare threat as well. As can be seen in the industry security survey, 55% of the surveyed organizations believe they may be a target of a cyber warfare attack. Paradoxically, the majority of companies surveyed (81%) believe they are not prepared to handle such an attack. This is the best comprehensive demonstration of our opening argument about organizations bringing a knife to a gunfight.

## Summary

Organizations fail to defend themselves primarily because they prepare for yesterdays' security attacks. But today's attacks are different – carefully planned, powerful and last days or weeks, while switching between attack vectors. Organizational security solutions are prepared to absorb the first strike, yet when attacks are prolonged, they have very limited resources and knowledge to handle. By the time they succeed in blocking the first two attack vectors, attackers switch to a third, more powerful one. This requires a different approach.

## The Solution

How can organizations step up their defense and ensure they are equally as powerful and resourceful as the attackers? The gap between attackers and defenders cannot be easily closed. Even large organizations will find it difficult to justify a security team that is fully dedicated 24/7 to handle attacks. Furthermore, it would be impossible for such a team to attain the experience and expertise by only handling several attacks per year.

Using an analogy from the healthcare world – organizations cannot succeed handling a critical health issue in a local health clinic. Instead, what is required, are the availability, immediacy and experience of an emergency hospital with highly trained, specialized surgeons.

The solution lies in searching for such expertise and setup externally – through security expert teams. Such a security management war room would include: to the following

- A team of security experts who are well trained in dynamically responding and handling persistent security attacks that last several days.
- The most up-to-date methodologies and tools that facilitates the analysis of traffic and quickly form new protections in real-time, during the attack.
- An accumulated experience gained by handling serious security attacks on a weekly or even daily basis.
- 24/7/365 availability to respond to attacks.
- Ability to deploy counterattack techniques to cripple an attack.

We also believe that since security threats are global in nature and extend beyond the private sector, governments and states would become more involved in providing and sharing defense expertise.



## Setting the Expectations

The following provides an illustration of a response to an attack. The table compares the typical attack insight and activities taken with limited resources vs. the more knowledgeable, in-depth handling alternative.

CEO/CTO Question	Answers Given Today	Answers You'd like to Give
How are we stopping this?	Our DoS/DDoS mitigation is blocking some traffic, reducing the bandwidth by 60%, but the 40% still comes and impacts the firewall. We are working to increase the firewall session table; this however will require a reboot.	<ul style="list-style-type: none"> <li>• The SYN flood was blocked perfectly well by the DoS solution.</li> <li>• The HTTP page flood was more sophisticated and passed the challenge based technology. We have enabled the behavior based technology instead and it has been good so far.</li> <li>• The R.U.D.Y. that attacked is a new version and was not mitigated well by the existing protection. We've composed an ad-hoc signature to block it.</li> </ul>
Who is doing this?	There is no way to know. We noticed however that traffic comes from all over the world. We don't want to use geo-protection so as to not lose our European customers.	The attacking IPs belongs to a known botnet control by an Eastern European cyber organization. They are running ddos-for-hire service; This attack probably cost around \$1,000 USD. The motivation of their customers is usually business competition.
Are we doing anything to stop them?	No, what can we do?	Yes, we are using counterattack techniques to shut down the attack. We were able to slow down one of their tools using craft TCP RST packets, and to completely paralyze the other tool using a crafted window-size-zero packet.
Are there any other risks?	None that we are aware of.	We know that this group has hacker teams that may try to penetrate into our organization, so we are monitoring all security logs, not just the DoS ones. It is very important to keep the firewall, IPS and WAF safe and running the entire time.
Has the attack been completely mitigated?	Yes, the attack is not as high as it was in the morning, and we blocked 70% of it. The site is still very slow but at least alive.	Yes. Site is running very well with normal latency. No known false positives.

## The Year of DNS Attacks

2012 was the year of DNS attacks. While DNS attacks have been around for a while, they were much more frequent in the past year, and more importantly - were carried out with increased sophistication and amplified effect.

Why have DNS attacks become so popular? The answer can be found in the recent history of DoS/DDoS attacks. While DoS/DDoS attacks have been around as long as the Internet, they really became mainstream and popular in late 2010, particularly with the Anonymous group selecting them as their attack method of choice. At first, organizations were completely unprepared, and whatever attackers did was very effective.

Towards the end of 2011 things changed when organizations started implementing attack mitigation systems to fight DoS/DDoS attacks, which pushed attackers to find new ways to bypass mitigation solutions with more sophisticated attack vectors. In this context, DNS was an excellent choice.

Looking closely at the 2012 attack data, the Industry Security Survey identified an increase of 170% in DNS attacks compared to 2011. About half of these were sophisticated recursive or reflective attacks, which did not even require that the victim have a DNS server in order to be attacked.

DNS attacks illustrate the dynamics of the overall DoS/DDoS arena. While the naïve and still common perception of DoS/DDoS attacks is that to be destructive use brute force to generate massive traffic, DNS attacks have proven otherwise. Sophisticated DNS attacks can leverage their asymmetric nature, and with relatively lower attack rates can be just as damaging and powerful. This growing sophistication is not limited to DNS attacks, but is part of the overall DoS/DDoS landscape.

## Related Links

- [Cyber War Rooms: Why IT Needs New Expertise To Combat Today's Cyberattacks](#)  
- Avi Chesla
- [Counterattack – Radware Global Network and Application Security Report 2011](#)  
(see chapter 10)

## High Profile 2012 DNS Attacks

2012 included some major DNS attacks on high-profile organizations:

### AT&T

In August 2012, AT&T experienced a DDoS attack that flooded its Domain Name System servers in two locations. During the attack, which lasted at least 8 hours, AT&T's own site was down. More critical however, was the fact that business web sites on AT&T's network were also unavailable.

"Due to a distributed denial of service attack attempting to flood our Domain Name System servers in two locations, some AT&T business customers are experiencing intermittent disruptions in service. Restoration efforts are underway and we apologize for any inconvenience to our customers. Our highest level of technical support personnel have been engaged and are working to mitigate the issue."

- AT&T spokesman message during the attack

Figure 9: Source: [Martyn Williams](#), IDG News Service.



Figure 10: GoDaddy Twitter updates during the DNS attack.

### GoDaddy

On November 10 GoDaddy, the Web's largest hosting and domain registration provider suffered a DNS flood attack that affected millions of internet domains. Not only was the [www.godaddy.com](#) domain unreachable, but all domains registered with GoDaddy that used its server name and DNS records were also down.

### Anonymous Attack on Root Servers

On March 31st, the Anonymous hacktivist group threatened to shut down the entire Internet by attacking the world's 13 DNS root servers. The group planned to use a DNS reflective amplification attack and released an attack utility called 'Ramp,' which was designed to harness the resources of multiple Internet Service Providers (ISPs) and other corporate DNS services to shut down the DNS core. Eventually the attack was never carried out, but its sophisticated method (see the '[Reflective DNS Attack](#)' section further down) had destructive potential.

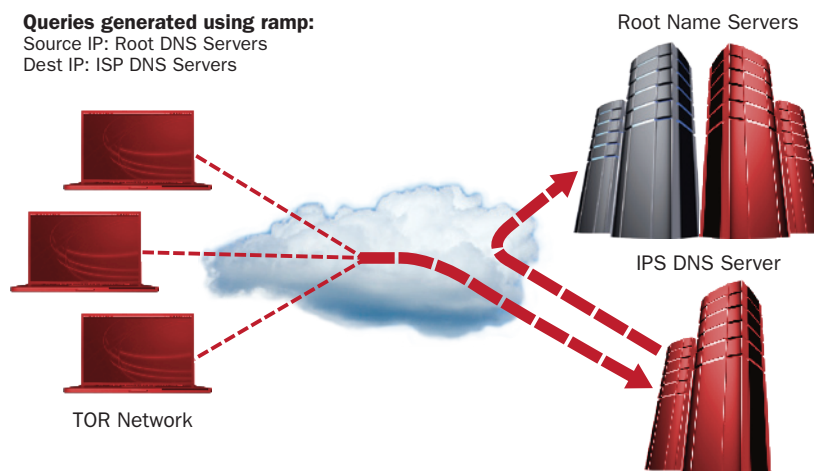


Figure 11: DNS reflective amplification attack.

## Four Types of DNS Attacks

DNS DoS attacks can be categorized into four methods, which differ in their approach, process, and amplification.

### Basic DNS Flood

Using the most basic DNS flood, the attacker sends multiple DNS requests to a DNS server, flooding the server with requests and consuming its resources. The attack method is attractive, as it is both relatively simple to execute and allows hackers to hide their identity.

**How does it work?** An attacker generates DNS packets, which are sent over, **User Datagram Protocol (UDP)**, to the DNS server. A standard PC can generate 1,000 DNS requests per second, whereas a normal DNS server can only process 10,000 DNS requests per second. In other words, only 10 PCs are needed to take down a DNS server. Because DNS servers

primarily use UDP, attackers do not need to establish a connection and therefore can spoof the source IP and hide their identity. This property also plays a role in the ability to mitigate the flood – an attack coming from numerous spoofed sources IPs is much more difficult to mitigate than one arriving from a confined list of IPs.



Figure 12: In a **Basic DNS flood**, an attacker sends numerous DNS requests to the target DNS Server, flooding the server with requests and bringing it down.

### Reflective DNS Attack

Being asymmetric in nature, a reflective DNS attack enables generating a massive flood effect with limited resources.

**How does it work?** The attacker sends a DNS request to one or more third party DNS servers, which are not the real target of the attack. The attackers spoof the source IP of the DNS request to be that of the target server (the victim), so that when the third party servers reply, their reply is sent to the target of the attack.



Figure 13: In a **Reflective DNS attack** an attacker sends DNS requests to third-party servers, while spoofing the source IP of the request to be that of the target server (the victim). The reply sent by third-party servers is sent to the target DNS server, amplified 3-10x times.

The attack makes use of an amplification effect, whereby a DNS reply is 3-10 times larger than a DNS request. In other words, the attacked server receives a massive flood of traffic compared to the small number of requests originally generated by the attacker. The reflective attack also demonstrates that the victim does not need to own a DNS server to become the target of a DNS attack, as the objective is to bring down the internet pipe or the firewall.

Reflective DNS attacks can employ several levels of amplifications:

- **Native** – In DNS, response packets are natively much larger than request packets. Therefore, even the most basic attack can achieve 3-4x amplification.
- **Selective** – DNS replies do not have a uniform size: some DNS requests will be answered with a short answer, others with a much longer one. A more sophisticated attacker can first identify the domain names that have response packets larger than others. By sending queries only for those domain names, an attacker can reach 10x amplification.
- **Crafted** – at the top level, attackers can design specific domains that send extremely large response packets. By sending queries for these self-built domains, attackers can reach 100 x amplification.

The level of anonymity in reflective DNS attacks is increased by an order of magnitude. Beyond spoofing the SRC IP (as in class DNS floods), the attack itself is completely indirect – as it is the third party server that sends requests to the target of attack.

### Recursive DNS Attack

The recursive attack is the most sophisticated and asymmetric DNS attack method in that it requires minimal computing resources from the attacker, and results in extensive resources invested by the victim's DNS server.

**How does it work?** A recursive attack exploits the way recursive DNS queries operate. Under recursive DNS, when a DNS client makes a request with a query name that is not in the DNS server cache, the server sends repetitive queries to other DNS servers, until an answer can be returned to the client. Taking advantage of this process, the attacker makes recursive requests using phony query names that it knows do not exist in the server cache (see the screen capture example). To resolve these queries, the DNS server then needs to process each record, temporarily store it, send a request to another DNS server, and wait for a response. In other words, it needs to allocate extensive computing resources (CPU, memory, and bandwidth), to the point where it becomes unavailable.

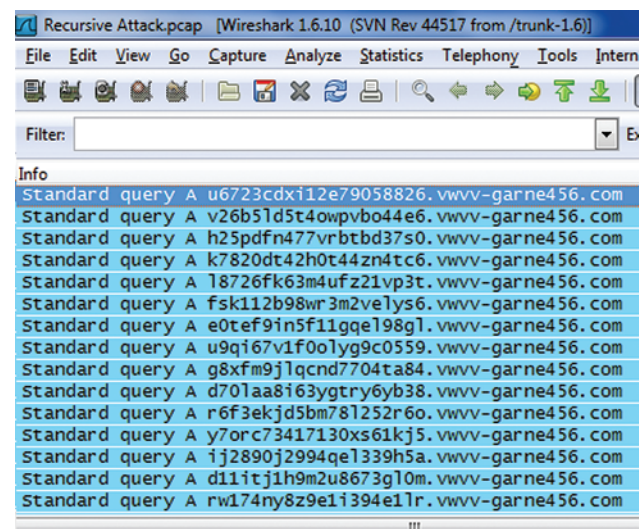


Figure 14: A recursive DNS attack sends requests with query names that do not exist in the DNS server cache. This enforces the server to send iterative requests to other DNS servers while allocating extensive computing resources.

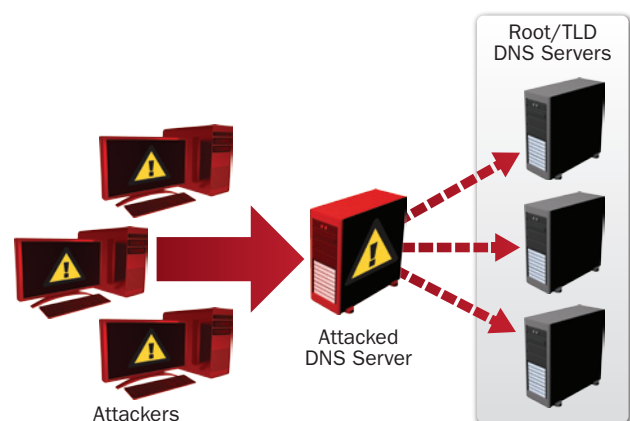


Figure 15: In a **Recursive DNS flood**, an attacker makes DNS requests with phony names that are not in the DNS server cache. The attacked server needs to allocate extensive computing resources, sending iterative queries to other DNS servers, to the point where it becomes unavailable.



The asymmetric nature of the recursive attack and its low traffic rate, make it difficult to mitigate. A recursive attack may pass undetected beneath the radar of both protection gear and humans, who are more focused on identifying high-volume attacks.

### Garbage DNS Attack

As implied by its name, a garbage attack, floods a DNS server by sending large data packets (1500 bytes or more) to its UDP Port 53. The concept behind this attack is to overwhelm the network pipe using large data packets. Attackers can generate garbage floods using other protocols too ( UDP port 80 is also popular); just like in other protocols the target can stop the attack by blocking the port at the ISP level, with no repercussions. The one protocol where such a defense option is not possible is DNS, as most organizations will never close this port.



Figure 16: In a **Garbage DNS flood**, the attacker floods the DNS server with large data packets sent to its UDP port 53. This attack exploits the fact that organizations will always leave the DNS port open and will not block traffic at the router level.

### Summary

DNS attacks have gained popularity because they offer attackers multiple benefits:

- **Critical Infrastructure** – DNS is a critical infrastructure, meaning that if the DNS service of an organization is disrupted, its entire Internet traffic goes down. Or at a higher scale, if you take down the DNS root servers – the entire Internet goes down (as Anonymous tried to do in ‘Operation Blackout’).
- **Asymmetry** – with their asymmetric amplification, DNS attacks can cause a denial of service using limited traffic and resources.
- **Anonymity** – the stateless DNS protocol allows attackers to spoof their SRC IP and easily conceal their identity. Using a reflective flood, the attacker does not even send the traffic directly to the target. Presently, after many arrests of hackers and Anonymous group members, anonymity is an important consideration.



	Anonymity	Asymmetric	Low Detection Signature <sup>2</sup>	Impact		
				Internet Pipe	Firewall / Stateful Devices	DNS Server
<b>Basic</b>	Yes	No	No		✓	✓
<b>Reflective</b>	Yes <sup>1</sup>	Yes (Bandwidth)	No	✓	✓	
<b>Recursive</b>	Yes	Yes (Server Resources)	Yes			✓
<b>Garbage</b>	Yes	No	No	✓		

## The HTTPS Challenge

There are two assumptions in DoS/DDoS mitigation. The first is that you need to clean the attack as early as possible before it reaches deep into your network. The second, and more obvious assumption, is that you need to inspect traffic. With HTTPS-based attacks, achieving these objectives is quite challenging. The ERT has experienced an increase in requests for assistance in handling HTTPS attacks. It was surprising that these attacks were not used even more frequently and we expect to see a sharp rise in their popularity.

## Understanding SSL and HTTP Vulnerabilities

Why is an HTTPS attack so ominous? Although it uses the exact same protocol as HTTP, it is a world apart in its threat potential. Here's why: typically, attacks carried over HTTP can be detected and mitigated using a DDoS mitigation solution - whether it is based on customer premises equipment (CPE), a cloud-based solution, or ideally both. Such solutions can handle HTTP attacks whether they are network flood attacks or application-level attacks.

## Related Links

- [Operation Blackout – Get Yourself Prepared](#)  
- Ronen Kenig
- [DNS Amplification Attack \(YouTube\)](#)



Figure 17: HTTP attacks are mitigated by DDoS protection solutions.

However, when the same attacks are carried over HTTPS, things are different. Network floods can still be mitigated just the same; the data is not yet encrypted, and a SYN flood, for example looks exactly the same on HTTPS as the one on HTTP. However, application attacks are problematic for detection.



Figure 18: HTTPS-based attacks are not detected by cloud or CPE device mitigation solutions. An application-level HTTPS attack is encrypted and cannot be analyzed by the mitigation gear. In addition, HTTPS is vulnerable to unique SSL Attacks.

As seen in the diagram, HTTPS encrypted traffic is typically decrypted only by the web-server, load balancer or dedicated SSL terminator. These entities are usually placed 'deeper' within the network, after traffic has already passed through DoS mitigation solutions (cloud or CPE):

- Since organizations are reluctant to move their SSL certificate keys to a Cloud MSSP as it puts them in risk, the Cloud DoS mitigation solution cannot analyze encrypted traffic and therefore does not detect an attack.
- The CPE device also sees encrypted data, which it is unable to examine.

Consequently, the attack is detected too late, when it has already reached its destination.

## SSL Attacks

In addition to HTTPS attacks, there are native SSL-layer attacks which directly target the SSL-handshake mechanism. SSL attacks, carried via the THC-SSL-DOS tool, were discussed in length in our 2011 report, but here is a brief summary.

Normally the SSL handshake is carried out only once to establish a secure connection. The attack makes use of a 'renegotiation' option of the protocol, used to establish a new secret key. By sending repeated requests for SSL renegotiation, the attacker creates a heavy load on the

## Related Links

- [THC-SSL-DOS Attack Tool](#)  
- YouTube
- [THC-SSL-DOS - Radware](#)  
[2011 Global Application and Network Security Report](#)  
(see chapter 8)

target server CPU to the point of exhaustion. In cases where the server does not support the 'Renegotiation' option, the attacker can alternatively open fresh SSL connections, causing the same affect. The SSL attack is asymmetric by nature - the resources required by the server to handle the handshake are 15X larger than those required from the initiator (the attacker).

### Summary & Recommendations

HTTPS is supported by practically all web sites and is an essential component in financial sites, where it protects monetary transactions. In light of the difficulty to detect HTTPS attacks, we expect to see a sharp rise in their popularity and recommend organizations, particularly in the financial sector, to acquire a solution that addresses this problem.

### Hackers Can See Through Your CDN

With their ability to dramatically improve performance, Content Delivery Networks (CDNs) have been quickly gaining popularity in recent years, controlling more and more of the Internet backbone traffic. CDNs work by caching static content on their own servers and placing it closer to users around the world to accelerate user access to web content. Perhaps because most of their site data is stored on CDN servers, CDN customers have started to believe that CDNs also provides protection against DoS/DDoS attacks. According to our Radware Security Survey, 70% of CDN users believe that their CDN provides a solution for DoS/DDoS attacks.

Do you consider Content Delivery Networks (CDNs) a solution for a DoS/DDoS attack?

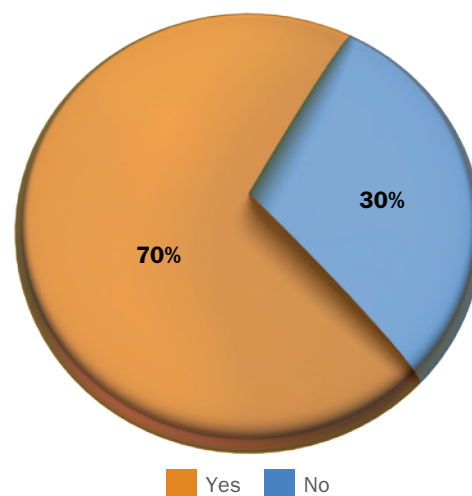


Figure 19: 70% of the companies who use CDN believe the CDN is a solution for DoS/DDoS attacks.

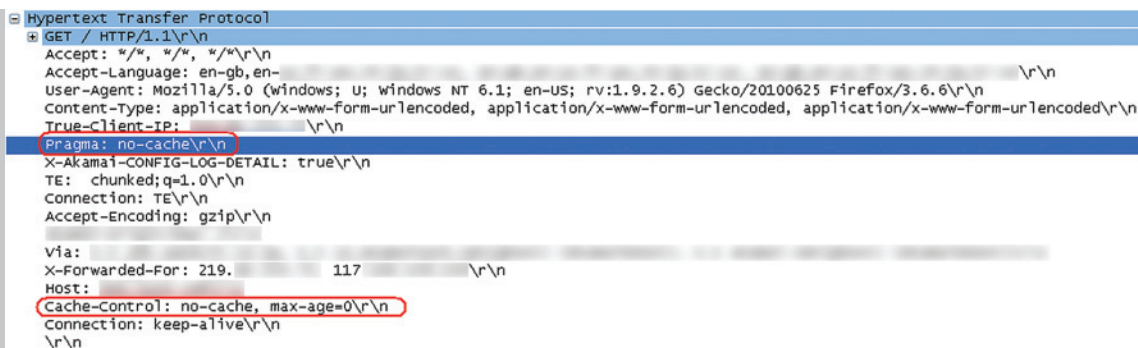
Indeed, a CDN can absorb high-volume attacks and make it difficult to saturate the CDN data center. It has full control over both the data it stores and the users accessing it, and can protect the data using [Captcha](#) challenge-response tests or other user authentication methods.

Unfortunately, these security measures provide a false sense of security. A CDN is not equipped or designed to provide complete DoS/DDoS protection and can only protect the data it stores; the data stored at the customer's data center is still exposed. Sophisticated DDoS attacks use multiple attack vectors to bypass the CDN and directly attack the vulnerabilities of the customer's data center. Here are a few examples of how this may work.

## CDN Denial-of-Service Security Loopholes

**Dynamic data** – CDNs only store static data. All dynamic data such as market quotes, current weather conditions, running news headlines, etc. remains on the customer's data center. In practice, requests for dynamic content easily bypass the CDN and go directly to the customer's datacenter. DoS attacks exploit this vulnerability, neutralizing the CDN's ability to absorb and activate its protection. An attacker can also access dynamic content by altering parameters on recursive requests, thus forcing the CDN to “lift the curtain” and directly query the data center.

**Bypassing the CDN with cache system directives** – Cache system directive are specific parameters in the HTTP header that instruct the CDN to pass the request to the backend server rather than provide the response from its cache. Radware's ERT identified many cases where attackers used a cache system directive such as “cache-control: no-cache” or similar “Pragma:” instructions. Using these directives attackers bypass the CDN's protection layer even for static data.



The image shows a screenshot of an HTTP request in a network analyzer. The request is a GET / HTTP/1.1. The headers include: Accept: \*/\*, Accept-Language: en-gb,en-... User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.6) Gecko/20100625 Firefox/3.6.6 Content-Type: application/x-www-form-urlencoded, application/x-www-form-urlencoded True-Client-IP: ... Pragma: no-cache X-Akamai-CONFIG-LOG-DETAIL: true TE: chunked;q=1.0 Connection: TE Accept-Encoding: gzip Via: ... X-Forwarded-For: 219. ... 117 Host: ... Cache-Control: no-cache, max-age=0 Connection: keep-alive. The 'Pragma: no-cache' and 'Cache-Control: no-cache, max-age=0' lines are highlighted with red boxes.

Figure 20: Attackers use cache system directive, such as “Pragma: no cache” and “cache-control: no-cache” to bypass the CDN.

**Highly-distributed attacks** – Attacks that are highly distributed do not generate enough volume at any network node of a CDN network, and therefore will arrive with high volume only at the attacked data center, bypassing the CDN and resulting in a denial of service. It is not feasible for a large CDN to synchronize in real time the data and statistics between all CDN network points in order to effectively detect a distributed attack – whether high or low volume.

These loophole examples clearly point out that while CDNs can protect against many attack vectors, they cannot provide complete DoS/DDoS protection. The 80-20 rule does not apply in the security world, as hackers will always exploit the open holes or weak links, and take advantage of the few attack vectors that are not covered.

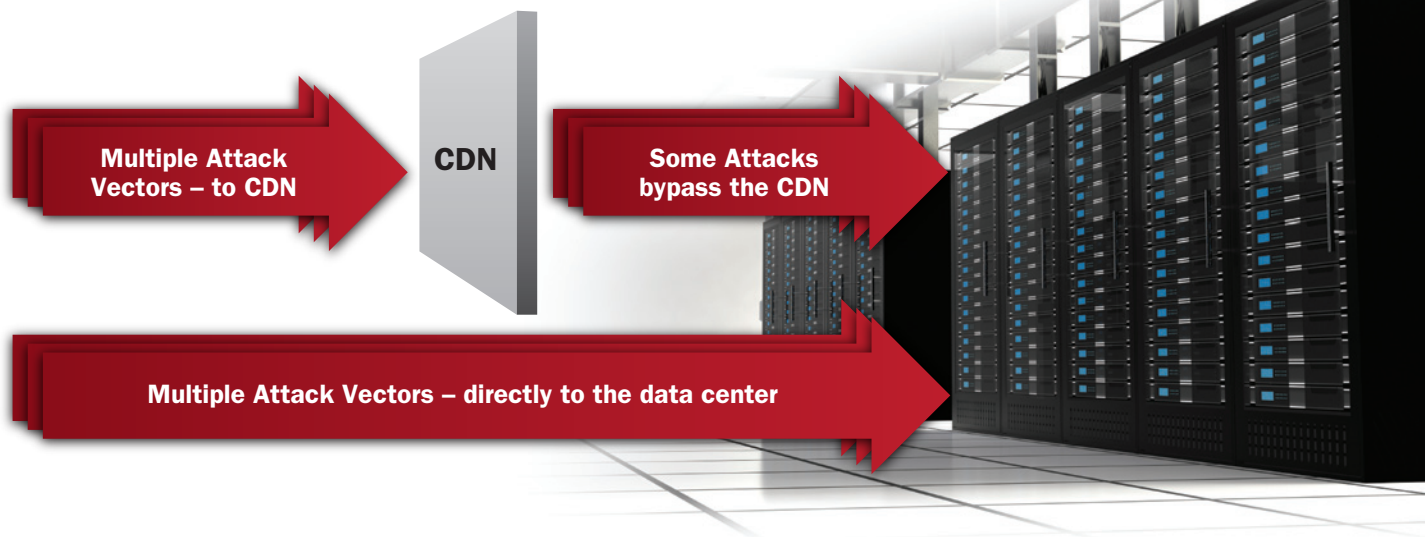


Figure 21: Despite the CDN ability to block some attack vectors, there are still many ways to bypass its protection and generate a denial of service attack directly on the data center.

### A CDN DDoS Attack Case Study

This case study outlines an attack carried out on a large corporation (which we'll call BCDN). BCDN hosted some of its content on the servers of a large CDN provider, but kept the dynamic data stored in its data center. In the DDoS attack launched on BCDN, hackers used three different attack vectors.

The first attack vector was carried out by sending malformed TCP packets to BCDN's public IP, while the second attack vector sent garbage UDP packets to port 53 (DNS port). BCDN had a proper attack mitigation system on -premises and therefore succeeded in mitigating the first two attack vectors.

The hackers were aware that BCDN was storing data on a CDN, and used a third attack vector. This vector - a simple HTTP flood - would have been easily stopped by the attack mitigation system if it were not behind the CDN. However, this third attack vector used a CDN bypass technique – querying the data-center dynamic data. This caused the CDN to bypass the attack to the data center.

Since this attack vector was launched through the CDN, the source IP of all requests was the CDN IP and it was considered legitimate. The CDN servers, as well as any legit user behind the CDN, easily passed any challenge-response sent by the attack mitigation system. In the defense world, once an IP passes all challenges, it is marked as a “safe IP” (temporary white-listed) and is allowed access to servers. Once the CDN IP was marked as safe, all requests, both the legitimate ones and those sent by the attackers, were able to reach the data center, causing a denial of service.

An attempt was made to limit the traffic based on threshold. However, it was impossible to block certain clients, and the limit applied to all CDN connections. Since most connections were attacks, legitimate users behind the CDN were not able to access BCDN servers. In short, this mitigation technique failed to stop the DoS attack because both the attack and the legitimate traffic were all coming from the same source IP.

The only place where the actual user IP can be seen is in the X-Forwarded-For (XFF) header in the HTTP. To block the attack, an offline analysis was carried out by the attacker IPs, based on XFF data. Once IPs were identified, they were blocked using a XFF inspection with the known attackers IPs. As evidence from this scenario, blocking an attack that bypasses the CDN is challenging and involves time-consuming manual intervention.

## 2012 vs. 2011 – Quick Trends

Each year we look back and compare past year's network security attacks to the previous year. We look at some key parameters such as attack distribution, bottlenecks, investment in DoS, motivation and probability to be hit by a DoS attack. In this section, we present the results of our findings with an analysis of the data.

### Attack Distribution – No Significant Changes

When looking at the distribution of attacks based on their type, we see no major changes in protocols. Also the ratio of application vs. network attacks remained about 50:50, as it did during 2011.

The diversity of attack types is powered by the attackers' usage of multiple attack vectors. An effective attack will typically consist of two network attacks and two application attacks. Therefore, even if a particular attack gains popularity, in the overall distribution it will not have a noticeable effect, since it is only one attack vector in the overall campaign. This is reflected in the statistics, which show a wide diversification in attack types.

## Industry Security Survey – Attack Count by Type

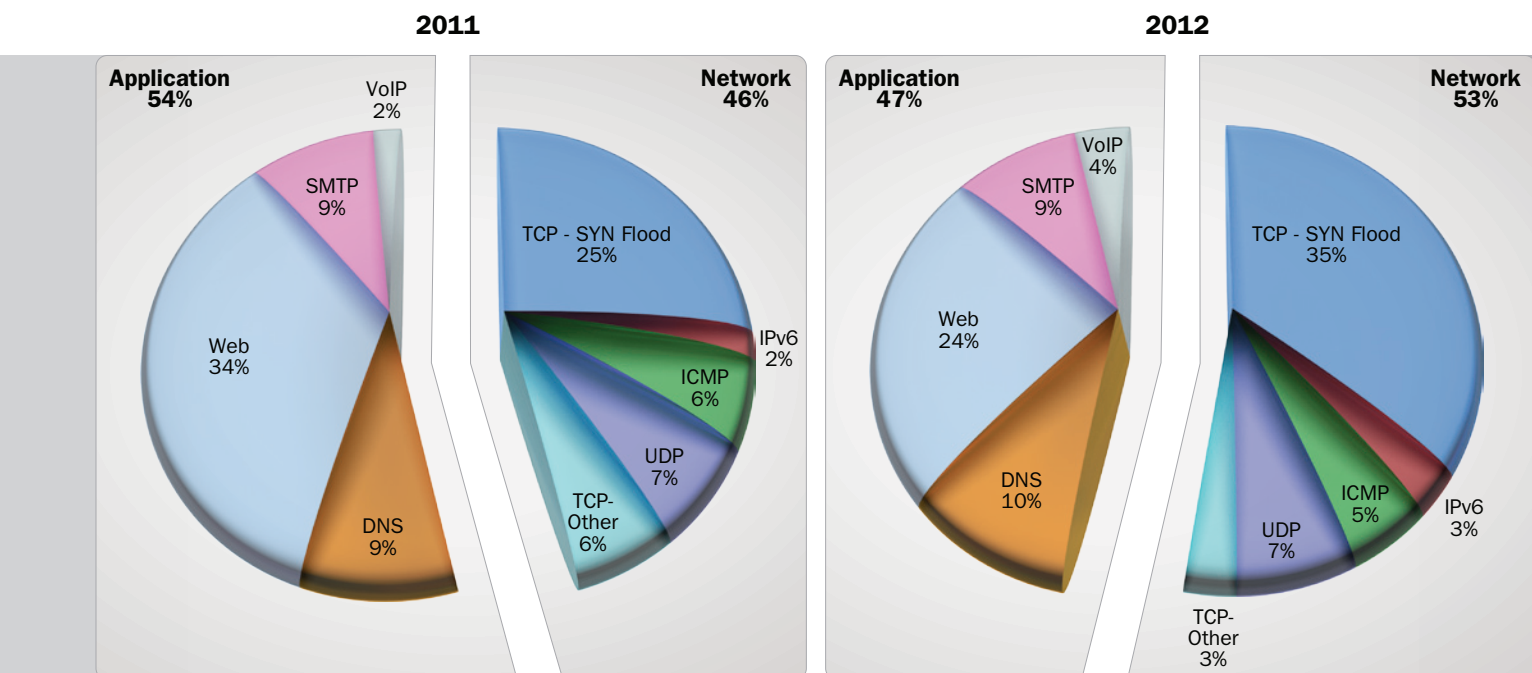


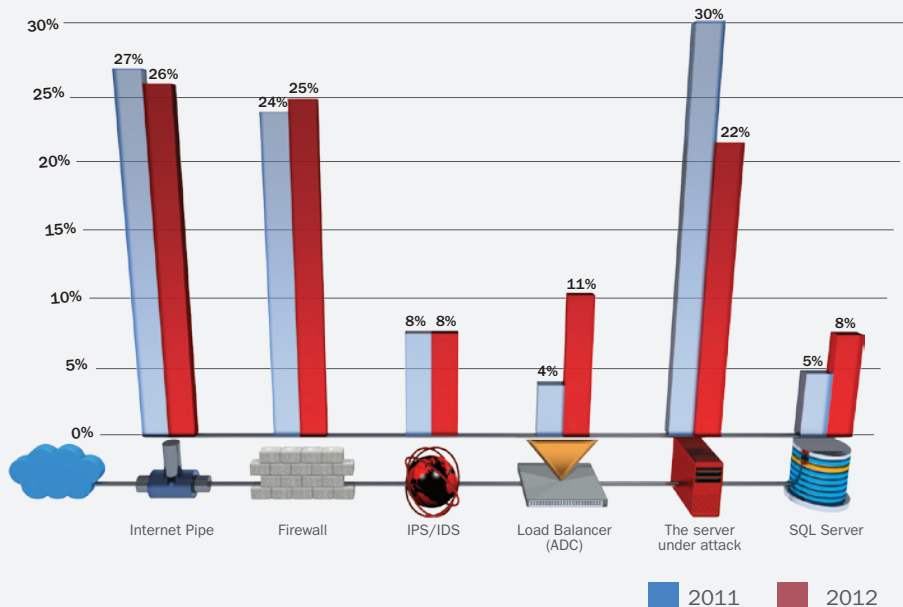
Figure 22: Attack remained diversified between different attack types. This reflects attackers using multi-vector attacks.



## Industry Security Survey

Which services or network elements are (or have been the bottleneck) of DoS?

Figure 23: The three entities that are consistently the bottlenecks in DoS/DDoS attacks are the server under attack, the firewall and the Internet pipe.



### Server, Firewall and Internet Pipe Remain Bottlenecks

Similarly to last year, the three weakest links that are targeted by DoS/DDoS attacks are the server under attack, the firewall and the Internet pipe.

- **Servers** become the bottleneck simply because attackers consume more resources than the servers can provide.
- The **Internet pipe** becomes the bottleneck under attacks using high bandwidth, also called volumetric floods. These can include UDP floods with a large payload, or high-bandwidth TCP floods.
- Even though a **firewall**, as a security product, is not expected to go down under a DoS/DDoS attack, attacks that generate multiple states like a SYN Flood, Connection Flood and UDP flood exhaust the firewall state until it becomes the bottleneck.

### Organizations Invest More in DoS/DDoS Mitigation

Because DoS/DDoS became mainstream as of 2011, organizations had the time to react. By 2012, companies developed a better understanding of the need for dedicated DoS/DDoS solutions, as opposed to relying on limited features provided as part of broader solutions. Specifically:

- The usage of 'general' DoS/DDoS solutions, such as firewall and IPS, was reduced by 13% in 2012. This is also because prominent firewall vendor do not present their firewall as a DoS solution anymore.
- Organizations have increased their reliance on dedicated DoS solutions, using Managed Security Service Providers (MSSPs).
- Usage of 'DoS/DDoS expert services' is still low. As discussed in the opening trend chapter, [Organization Brings a Knife to a Gunfight](#), we expect this figure to increase.

## Industry Security Survey

### Which solutions do you use against DoS attacks?

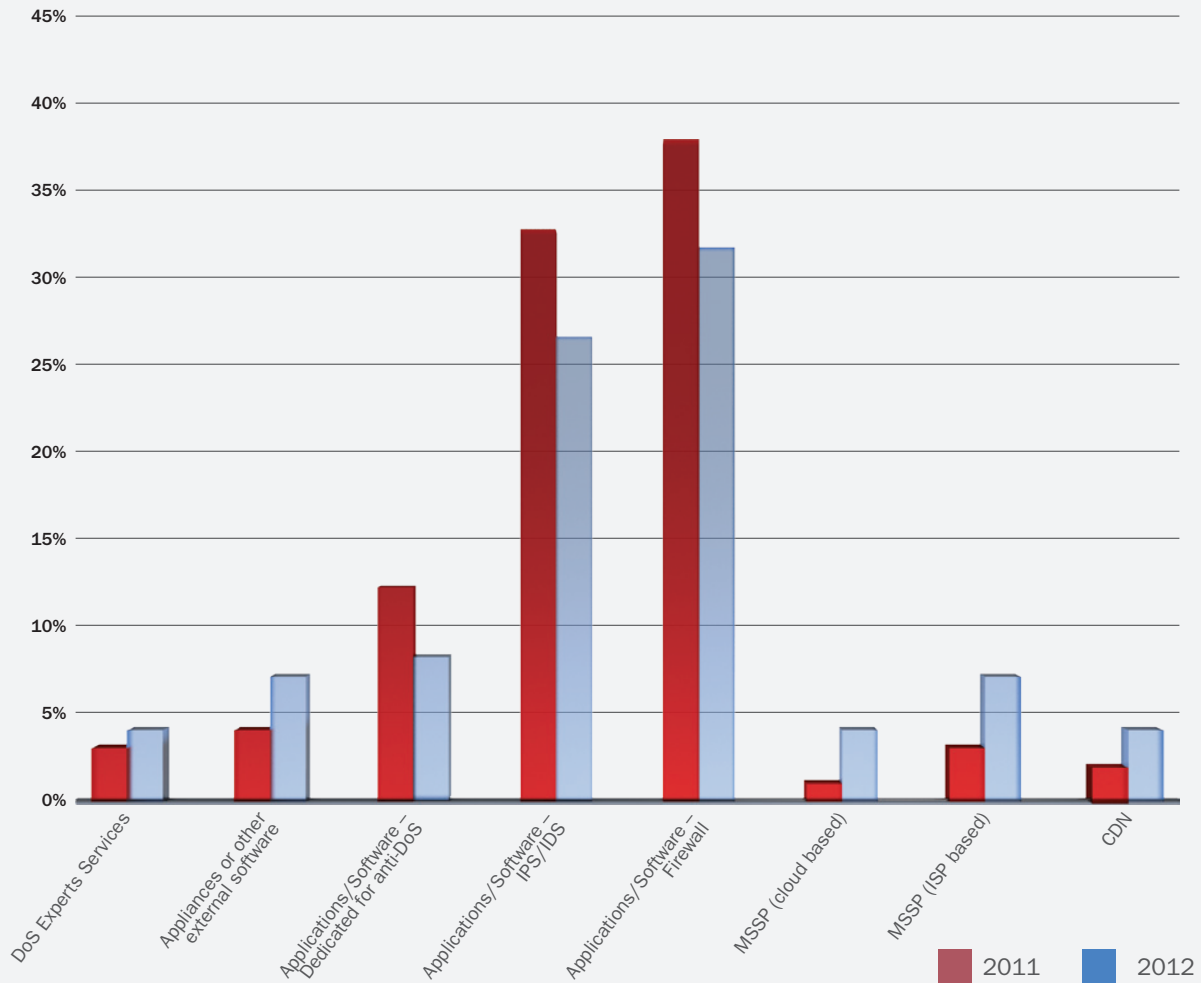
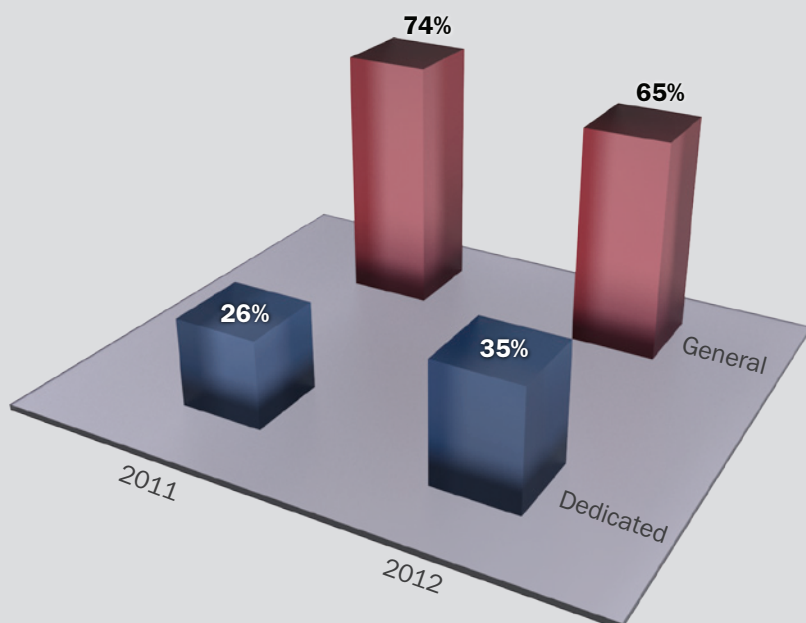


Figure 24: Which solutions do you use against DoS attacks?



## Industry Security Survey

### Dedicated Versus General Solutions

Figure 25: In 2012, organizations are starting to shift towards using dedicated DoS solutions, as opposed to general security solutions.

## No Change in DoS Motivation

Unlike in 2011, when there was a dramatic increase in ‘hacktivism’ and politically-oriented attacks, we have noticed no changes in 2012.

The motivation for most attacks is still unknown. Yet, in those cases where the motivation is known, political/hacktivism compromise 50% of the attacks. We have reasons to believe that during 2012 the proportions have shifted towards political reasons compared to hacktivist groups. More political and governmental supported attacks were noticeable.

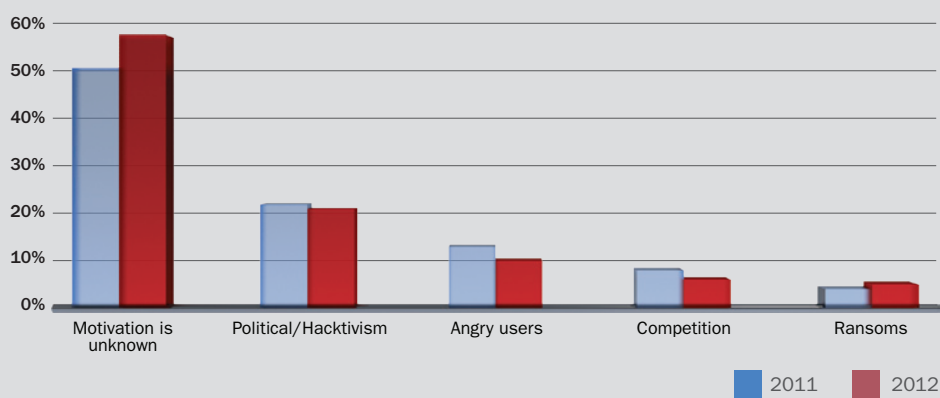
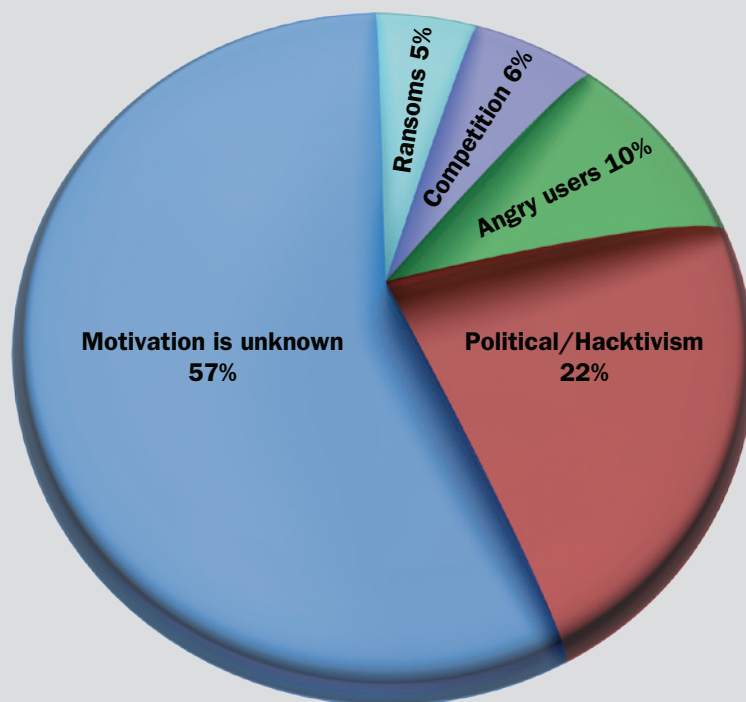


Figure 26: DoS motivation did not change in 2012 compared to last year.

Industry Security Survey  
Which of the following  
motivation(s) are behind  
the DoS/DDoS attacks  
that you experienced?

Figure 27: The motivation for the majority of DoS attacks is still unknown. Within the attacks with a known motivation, over half are political/hacktivist attacks.



## Financial Sector Moves Closer to the Ring of Fire

In 2012, government sites were still the focal of DoS/DDoS attacks, just like a year earlier. One change that occurred in 2012 is that the financial sector moved one step further towards becoming a focal target for attacks.

One of the major attacks that took place during September 2012 was “Operation Ababil”, in which a large number of U.S. banks and financial organizations were attacked. Allegedly, the attack was tied to the release of a trailer for the movie “Innocence of Muslims,” which was uploaded to YouTube. The film, which contained what some viewed as offending content, triggered demonstrations, violent protests and attacks on U.S embassies in Muslim countries. On September 18th, 2012 a group called “Cyber Fighters of Izz ad-din Al Qassam” announced an upcoming cyber attack campaign on what they claimed ‘American and Zionist’ targets.

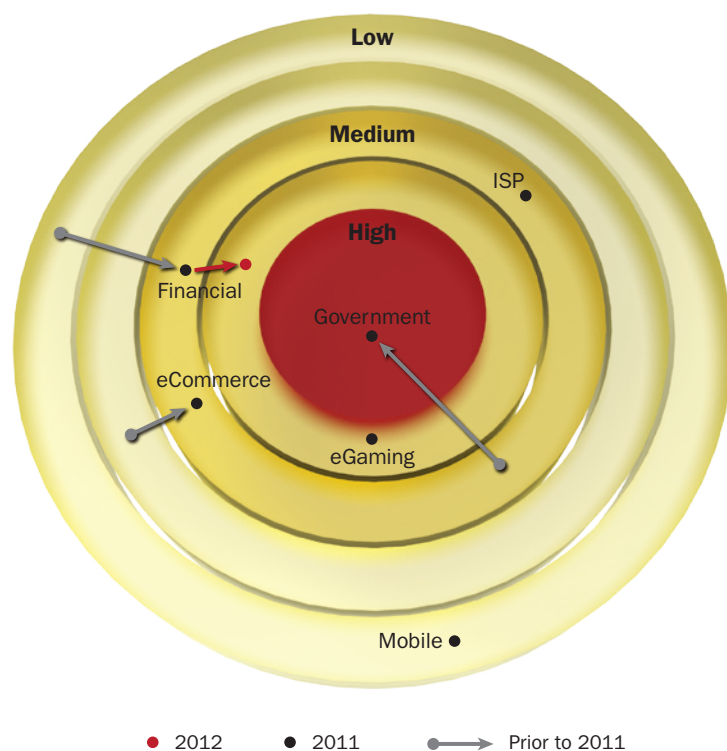


Figure 28



## Attack Tool Trends

### DDoS - Do it Yourself

DDoS has turned into a commodity. Granted, it may not yet be found on ecommerce sites, but in underground online sites you will discover a wealth of options – DDoS kits, price lists, and even DDoS for hire services. The availability of these DDoS kits has lowered the barrier for both network and application attacks. Anyone, from private users through cybercriminal organizations, can easily set up a Botnet and launch an attack.

### DDoS Kits

Requiring no coding or advanced hacking skills, DDoS kits let novice attackers easily set up a [Botnet](#). A DDoS kit is a software package containing two components - a Bot builder and a command and control server.

- **Bot Builder** - a GUI-based, step by step Bot generation tool that allows the attacker to create an executable file (Bot) to be distributed to potential targets. The newly generated Bot is armed with the address of the Command and Control server with which it can communicate.
- **Command and Control (C&C)** - the admin page used by the attacker to track its bots and send them commands for execution.

#### Current prices on the Russian underground market:



Hacking corporate mailbox: \$500  
 Winlocker ransomware: \$10-\$20  
 Unintelligent exploit bundle: \$25  
 Intelligent exploit bundle: \$10-\$3,000  
 Basic crypter (for inserting rogue code into a benign file): \$10-\$30  
 SOCKS bot (to get around firewalls): \$100  
 Hiring a DDoS attack: \$30-\$70/day, \$1,200/month   
 Botnet: \$200 for 2,000 bots  
 DDoS Botnet: \$700   
 Zeus source code: \$200-250  
 Windows rootkit (for installing malicious drivers): \$292  
 Hacking Facebook or Twitter account: \$130  
 Hacking Gmail account: \$162  
 Email spam: \$10 per one million emails  
 Email scam (using customer database) \$50-\$500 per one million emails

Figure 29: DDoS products and services offered in the Russian underground market.



Once the C&C is installed and the Bot executable is ready, the attacker can distribute the Bot to as many victims as possible, using common methods like social engineering and ‘drive-by’ attacks, which is a vector of attack where your web browser, whether its Internet Explorer or Chrome, is used to trick you into downloading and running a malware. Once the army of Bots is large enough, the attack is ready for launch.

Like professional software developers, DDoS kit developers advance their products and keep producing new versions, which are published and sold. In this underground world, most kits are variants of other Bots, whose binaries and/or source code have leaked and were customized and rebranded. A group of kits sharing the same origin is commonly referred to as a ‘family’.

## DDoS for Hire

The prevalence of DDoS kits has also facilitated the emergence of DDoS for hire services. Cybercrime organizations take advantage of the simplicity of kits to quickly offer attack services in various underground forums (DDoS-for-Hire/Rent a Bot).

A typical ‘business scenario’ of a DDoS for hire may involve offering a customer to ‘take down the competition web site’ or conversely, involve an extortion in the form of ‘pay-us-for-not-taking-down-your-site’.

**TOP- DDOS Service (Support)**  
Order a ddos attack! Removable poster competition!

**MENU**

- Home
- Reviews
- Rates
- Methods of payment
- Contacts

**Top-ddos**

It seems that all is well and business have long gained its momentum, but has recently appeared a number of competitors with whom you just can not cope? Our company offers a **ddos attack order** , by which time your competitors go out of control due to *off and hang on their sites* .

**Ddos-attack** - this is one of the varieties of attacks on computers. Their goal is to prevent getting users to a particular site, resulting in attendance will be limited resources and competition with those of firms weakened. It should be noted that not all providers are able to protect against **attacks Doss** , and it follows that all the cards in your hand and you can earn more money while your competitors are trying to find a way out. **Order ddos attack** on our site is easy and very easily, and besides, our prices will pleasantly surprise you. Our *ddos* service will help you. Web sites of your competitors will be based on how much you need.

**Type of attack**

- ✓ HTTP (GET, POST)
- ✓ DOWNLOAD
- ✓ ICMP
- ✓ UDP
- ✓ SYN

Figure 30: A DDoS-for-hire web page offering ‘on demand’ DDoS attack services with various attack types. The copy reads, “Order DDoS attack on our site is easy, and besides, our prices will pleasantly surprise you.”



## Summary

The availability of DDoS kits has turned DDoS attacks into a commodity that is readily available to anyone. It is safe to assume that DDoS kits will continue to evolve and offer new capabilities, forcing the defending side, or victim organizations, to adjust their defense strategies.

With the barriers for entry lowered, organizations should not be surprised if the number of attacks continues to grow each year. Not any less concerning is the expansion and improvement of the 'DDoS attacker supply chain.' For organizations, which are the target of this supply chain, this means only one thing: more sophisticated and challenging attacks.

## Dirt Jumper

Dirt Jumper is a well-known DDoS 'family', which has spawned other known Bot variants like Pandora, Di-BotNet and DIY. DirtJumper is sold for about \$800 as a DIY kit. It is also implemented in many DDoS for hire services and can be hired (rent-a-Bot) for \$30-\$70 a day in underground/black markets. The last Dirt Jumper 5 version had many promises (published in underground forums) about features such as HTTP 2.0 support, anti-debug and anti-virtualization, yet none proved to be true.

## Bot Builder

The Dirt Jumper Bot builder generates a build.exe file, which then is used to infect victims' machines. Advanced users may even use packers in order to evade AV detection.

## Command & Control

The Dirt Jumper Command and Control (C&C) component lets the attacker keep track of new and active Bots and enables sending Bots the target and attack vector details. Bots send HTTP POST requests on fixed intervals in order to communicate with the C&C server.

## Attack Modes

Dirt Jumper offers several attack modes. All attacks use a dynamic referrer, combined with randomized user agents. This creates a layer of randomization that makes it difficult for IPS and anti-DDoS solutions, which rely on static signatures, to detect the source attacker.

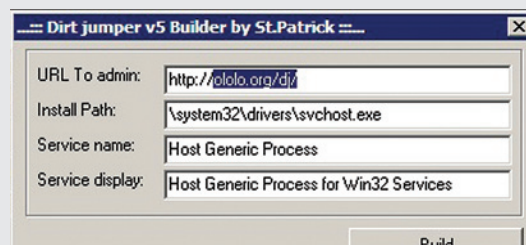


Figure 31

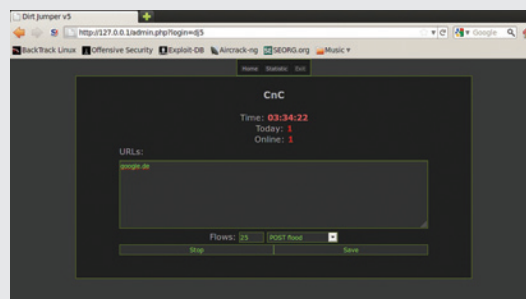


Figure 32

**POST flood** attack uses a POST request containing the target URL as a payload with the content-length header calculated accordingly.

**HTTP flood** attack uses GET requests with no special attributes, looping over URLs in the list.

**Synchronous flood** is the same as the HTTP Flood, yet it appears like the attack is using more connections to be more aggressive.

**Downloading Flood** uses simple HTTP GET requests, although the name implies an intensive resource download attack.

**Anti-DDoS flood** supposedly circumvents standard DDoS mitigation solutions. However, this method does not seem to work out of the box.

## Servers Enlisted to the Botnets Army

In the early day of Denial-of-Service (DoS), primitive server infrastructure was the main infrastructure for launching attacks. However throughout the last decade, servers have disappeared from the DoS scene and Distributed-Denial-of-Service (DDoS) attacks have completely taken over, relying on botnets with hundreds and thousands of personal computers.

In recent months Radware's ERT has witnessed what may be a new dramatic change in the DDoS landscape - the appearance of server-based botnets. Unlike the early days of single-server attacks, the new DDoS attacks employ multiple server machines, spread out geographically and organized in a powerful botnet. This new type of server-based DDoS architecture can be much more threatening than the common botnet attacks for several reasons:

- **Firepower** – servers have a much larger upload bandwidth, which enables fewer machines to produce the same impact as many client Botnets. Consider that the average US home computer has 600 Kbps upload speed, whereas a typical hosted server has an upload speed of 1Mbps-100Mbps – up to X150 times the bandwidth speed.
- **Reliability** – servers provide a far more reliable environment compared to home PCs. Home PCs are frequently shut down or taken offline, so that attackers must enlist a much larger number of computers than those that will actually be used in the attack. Servers, on the other hand, are always online and available for an attack.
- **Command and Control** – controlling a small number of highly available servers eliminates many of the challenges related to orchestrating thousands of unreliable botnet computers.

Although a server based botnet infrastructure is extremely effective, it does present some challenges to attackers compared to using home PCs:

### 1. Traceability

It is much easier to track and identify a group or individual behind a server based attack than a home computer individual, since servers contain better and more easily accessible audit trails. Also, it is easier for Attack Mitigation Systems (AMS) to block DoS coming from a small traceable list of attackers compared to a large distributed botnet.

### 2. Performance monitoring

Because server performance is constantly being monitored and owners are typically charged based on the traffic they generate, a server is much more likely to be detected when it begins uploading heavy traffic as part of an attack.

### 3. Protected environments

Servers are typically located in controlled and protected IT environments, such as server farms. Such environments are more likely to include software protections (such as anti-virus) and network defense systems (such as firewalls or IPS) that are much more likely to detect and block an attack.

### 4. High-entry barrier

Enlisting a server bot army requires more advanced attack skills. For example, home computer botnets may be easily purchased in the black market or can be hacked and abused using well-known attack vectors. Servers, on the other hand, will require more advanced, tailor-made attacks. In general, attacks coming from a server based botnet can indicate a stronger adversary.

Some questions still remain open in regards to the usage of server based botnets. For example, are attackers paying online hosting services to use their servers, or are they using clever attacks to hack and abuse servers? If servers are indeed being hacked, which attack vectors are used? Which methods are used to coordinate attacks? And finally, the most interesting question - is there a specific attacker profile that uses these new **server-based botnets**? Are they Hacktivists attacking for political agendas? Crime organizations with financial motives? Or perhaps even governments initiating cyber warfare?

## Case Study: 5 servers = 100 bot clients

In September 2012, some of the largest U.S. financial institutions experienced massive DDoS attacks. Known as '**Operation Ababil**', the attack was directed at institutions such as NYSE, Bank of America, Chase Bank and others. It flooded web sites with traffic, rendering them unavailable to customers and disrupting transactions for hours.

Data samples taken from this attack reveal that there were only tens of attacking resources used, which were located in a handful of countries such as Turkey, United States, Russian Federation, Bolivia, China.

The average server upload bandwidth in this attack was 10Mbps. In other words; five attacking servers had the same impact as 100 client machines in typical botnet attacks.

## DoS/DDoS Infrastructure Changes Over the Years

<b>1998-2002</b> <b>Individual Servers</b> Malicious software installed on hosts and servers (mostly located at Russian and east European universities), controlled by a single entity by direct communication.  Examples: Trin00, TFN, Trinity	<b>1998-Present</b> <b>Botnets</b> Stealthy malicious software installed mostly on personal computers without the owner's consent; controlled by a single entity through indirect channels (IRC, HTTP)  Examples: Agobot, DirtJumper, Zemra	<b>2010-Present</b> <b>Voluntary Botnets</b> Many users, at times as part of a Hacktivist group, willingly share their personal computers. Using predetermined and publicly available attack tools and methods, with an optional remote control channel.  Examples: LOIC, HOIC	<b>2012</b> <b>New Server-based Botnets</b> Powerful, well-orchestrated attacks, using a geographically-spread server infrastructure. Few attacking servers generate the same impact as hundreds of clients.
--	--	---	--



# Mitigation Trends

## Mitigating Attacks that Pass the CDN

The [Hackers Can See Through Your CDN](#) chapter clearly demonstrates that CDNs do not provide a viable protection against DoS/DDoS attacks. Attackers make use of multiple attack vectors to easily attack data centers –completely bypassing the CDN, and creating a masked attack that is difficult to detect and mitigate.

So how do you resolve the challenge - serve content via CDNs, but at the same time ensure an adequate DoS mitigation strategy? This chapter offers a solution in the form of a two-layered approach. Combining the defense mechanisms of both the CDN and the CPE device, this approach leverages the strengths of both entities to enable the effective detection and mitigation of attacks hiding behind a CDN.

## Why an ‘Independent’, CPE-only Approach Will Fail

One approach that may seem logical initially, is placing a CPE Customer Premises Equipment (CPE)) security device at your data center, while ignoring the CDN’s security role altogether. Theoretically, such a device should be able to identify and handle all traffic, regardless of its origin. However, with a DoS attack hiding behind a CDN, a CPE device will fail to provide protection on its own.

When using a CDN it is important to realize that it acts as a full proxy; any traffic arriving from the CDN to the data center will carry the CDN’s source IP, rather than the original user’s IP. Hence, in case of a DoS attack on the data center, it will appear as if the CDN is the attacking entity. Blocking CDN IPs will block all traffic to the data center, essentially creating a ‘self-inflicted’ DoS attack, while CDN IPs provide access to harmful traffic, thus failing to block the DoS attack.



Another challenge is handling the CDN multiplexing technique used by the CDN, in which –one session aggregates many customer requests. This approach saves resources as a TCP handshake is not done per request. However, even if the CPE device finds a problematic request, it cannot block the entire session as the session contains many other legitimate requests. Cutting only some of the session will make the CPE device in-line and visible, while draining its resources by making it a proxy that has to change any seq\ack of the session packets.

### The Winning Approach - Combining CPE and CDN Protection

A two-layered approach combines the defense of both the CDN and the CPE device, leveraging the strengths of both entities to maximize protection.

- **Attack identification** – Placed at the data center, the CPE device can scrutinize all data, regardless of the attack vector used, and decide about the attack type and mitigation approach.
- **Attack mitigation** – the CPE and CDN can communicate and work together to mitigate attacks, with the CDN protecting cached data and the CPE protecting all non-cached data. This takes advantage of the strengths of the two components, while eliminating their weaknesses.
- **Multi-vector attack protection** – the CPE can mitigate multi-vector attacks, which include direct attacks on the data center and others that bypass the CDN.
- **Attack management** – with the mitigation engine placed in the CPE, you have a single point of control with full visibility over all attacks and mitigation.

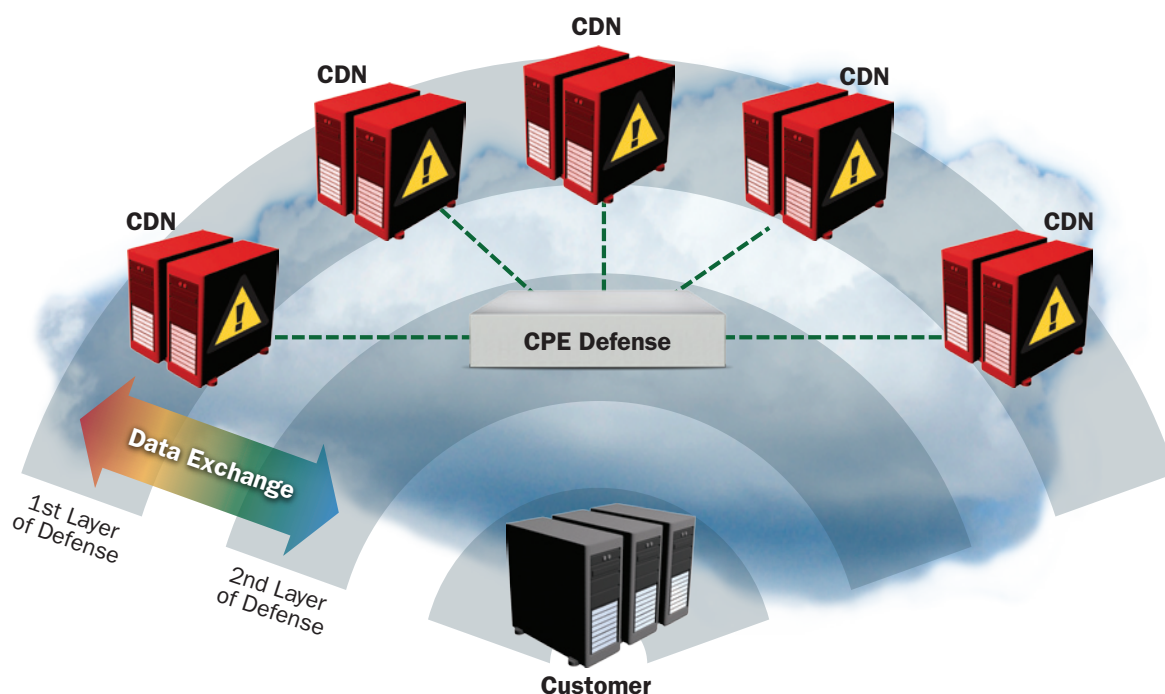
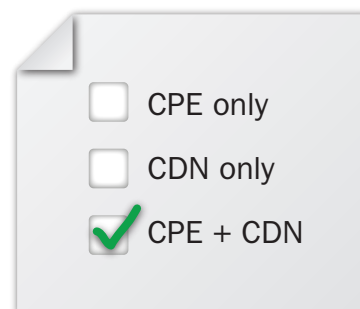


Figure 33: Two layers of defense – a CPE device and the CDN - effectively protect the customer against DoS attacks carried out behind a CDN. Each layer protects against certain attacks, with both layers communicate with each other.



# Summary

## Recommendations for the Network and Security Community

This report describes and explains findings based on the two surveys conducted by Radware's ERT. In this summary section, we provide opinions and make recommendations based on the content of this report.

### General Recommendations

#### ***Acquire Capabilities to Sustain a Long Sophisticated Cyber Attack***

Our findings clearly demonstrate how attackers perform meticulous pre-attack preparations, allowing them to launch effective and long lasting attacks. Organizations must balance this with similar efforts.

Our analysis shows that the gap between attackers and defenders is primarily in the real-time response abilities, rather than in technology or forensic skills. More specifically, organizations lack experts that can dynamically respond during the attack to shifting attack vectors. (For more details on this issue, see [Organization Bring a Knife to a Gunfight](#)).

Organizations should therefore examine their ability to withstand prolonged, sophisticated attacks and estimate the human resource required. For example, assuming that three skilled engineers are required per shift and that a DoS attack can run continuously for 3 shifts then at least 9 engineers are needed.

In most cases, it will be impractical for organizations to internally resolve the gap between the resources needed for routine operations vs. those required for the 'under attack' phase. Organizations should therefore search for additional competencies externally – from security experts, vertical alliances, or governmental services.



## Industry Security Survey

### How often have you experienced DDoS attacks in the past 12 months?

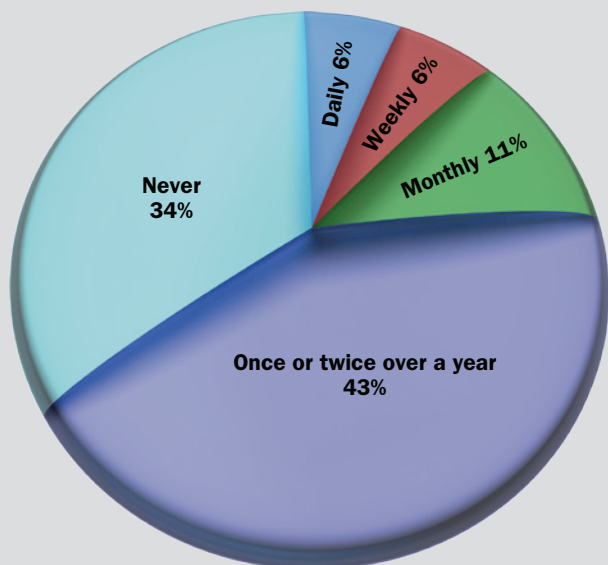


Figure 34: Frequency of DoS/DDoS Attacks.

### The DDoS Mitigation Checklist

- ☐ Volumetric Attacks (also in the cloud)
- ☐ Application Attacks
- ☐ Low-and-Slow
- ☐ Vulnerability Based DoS Attacks
- ☐ Response Team
- ☐ HTTPS Floods (encrypted traffic)

### DoS/DDoS Recommendation

#### ***DoS/DDoS Attacks Expected to Continue in 2013 as a Mainstream Attack***

DoS/DDoS attacks became mainstream in 2001, a trend which continued in 2012. This becomes apparent through multiple indicators – from media coverage about high-profile DoS attacks, through the Radware Security Survey that points out that 2 out of 3 organizations were attacked last year, and finally, the rapid increase in attacks as seen by our ERT.

In 2013 we expect DoS/DDoS to remain a mainstream attack. Inherently, DoS/DDoS characteristics make it extremely attractive. Unlike some security vulnerabilities that can be patched, there is no simple solution against DoS. Moreover, as DoS toolkits spread and barriers are lowered, virtually anyone can launch an attack.

#### ***Examine Your Lines of Defense against DoS/DDoS Attacks***

During 2012 we noticed a beginning of a shift in the investment in DoS/DDoS solutions. Mitigation may have improved, but this has also pushed attackers to come up with more sophisticated attack vectors and invest in finding the weak links in lines of defense. For more details of the DoS/DDoS investment trend, see [2012 Versus 2011 – Quick Trends](#).

Organizations should ensure that their line of defense is comprehensive and can withstand scaled up attacks. As part of this, a mitigation checklist must be completed, with any missing elements in to be addressed.

Many organizations react to the DoS/DDoS trend by relying on one of their existing security or network products: firewall, IPS or UTM and even load balancer. These products may block an attack or two, but the only realistic approach for an all-rounded protection is through all of the following components:

- A dedicated customer on-premise DoS/DDoS solution used to protect against all types of attacks
- A cloud-based solution that protects the pipe against volumetric attacks
- A 24x7 expert team capable of withstanding and responding to long sophisticated cyber attacks

### ***Do Not Consider Complimentary Features as a DoS/DDoS Mitigation Solution***

As suggested above, having a system with a few DoS/DDoS mitigation features is not the same as a full, dedicated DoS/DDoS solution. Here is a brief Radware ERT case study that demonstrates this issue.

In a previous attack, the target organization was surprised by DoS/DDoS attack. The attacker was persistent and kept changing the attack vectors to prolong the attack. The situation was critical and the organization summoned its security contractors, including the firewall and IPS providers. It challenged them with the question “which one of you can stop the attack?” The organization was not aware that firewalls are not a DoS/DDoS mitigation solution nor is IPS per se, and had unrealistic expectations from these systems. This false sense of security was based on the security tools having some DoS/DDoS mitigation features. For example, many firewalls have a SYN flood protection technology, but these same firewalls cannot handle an HTTP flood. Radware’s ERT is quite often called upon to protect a security product that was the first to fail when attacked by DoS/DDoS.

### ***Carefully Plan the Position of DoS/DDoS Mitigation Within Network Architecture***

To be effective, a DoS/DDoS mitigation solution must be placed before most of the network elements in the path. A typical installation would place it before the firewall so it could protect the router, firewall, load balancers, Internet service, and other internal servers. In addition, a solution deployed within the organization’s perimeter cannot protect the Internet pipe from a volumetric attack. Such a protection can only be achieved via a cloud based solution that can ensure the pipe is clean from volumetric attacks.

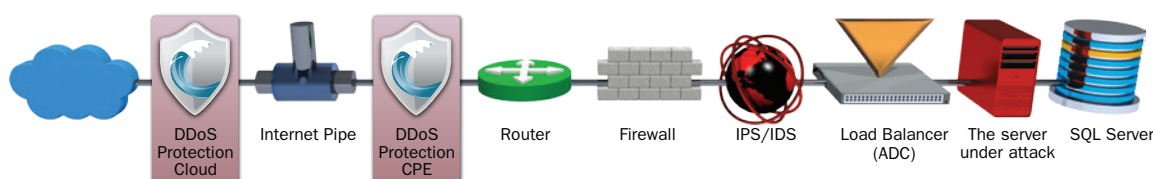


Figure 35

### **Using an APT Score**

As this research report shows, there is a new trend in the cyber security landscape—the introduction of attack campaigns. Organizations are now being targeted by multi-vector attacks, with more complicated attack vectors and lengthier strikes. Due to this change, Radware established the Advanced Persistent Threat (APT) score which takes into account the length of the campaign, how many attack vectors there were and how complicated each attack vector was.

As this trend continues to increase and the campaigns become more advanced and organized, attackers are focusing on ensuring the loss of service availability and impact on their targets site. Radware’s APT score was developed to show the increase in the complexity of APT attacks and assist in the mitigation of these campaigns. By using the APT score, organizations can avoid bringing a knife to a gun fight – that is they can better understand these new attack vectors, what components are involved and analyze them in real time, ultimately shortening the duration of these campaigns before any damage is caused to a company’s network.

## Methods

Data from the Industry Security Survey was collected from a random sampling frame of 15,766 IT and IT security practitioners located in all regions of the Americas were selected as participants to this survey.

This year, 179 unique companies responded to the survey, the majority of which are not Radware customers. As seen in Figure 36, 95% of the survey participants are not using Radware DoS/DDoS mitigation solutions. Figure 39 shows the distribution of organizations based on their annual revenue. The majority includes large and medium organizations, with some small organizations as well. Figure 37 illustrates that the majority of organizations conduct business worldwide, rather than in a specific country or region.

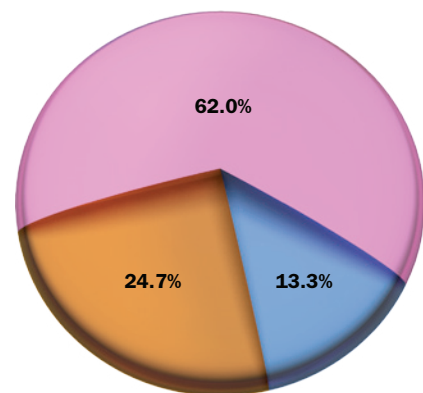
Is your organization currently using Radware's Attack Mitigation System (AMS)?



■ No - 95.5% (170) ■ Yes - 4.5% (8)

Figure 36: Majority of Industry Security Survey responders are not Radware customers.

What is the scope of your organization's business?



■ Country-wide (e.g. US only)  
■ Region-wide (e.g. North America only)  
■ World-wide

Figure 37: Geographic scope of business.

What is your organization type?

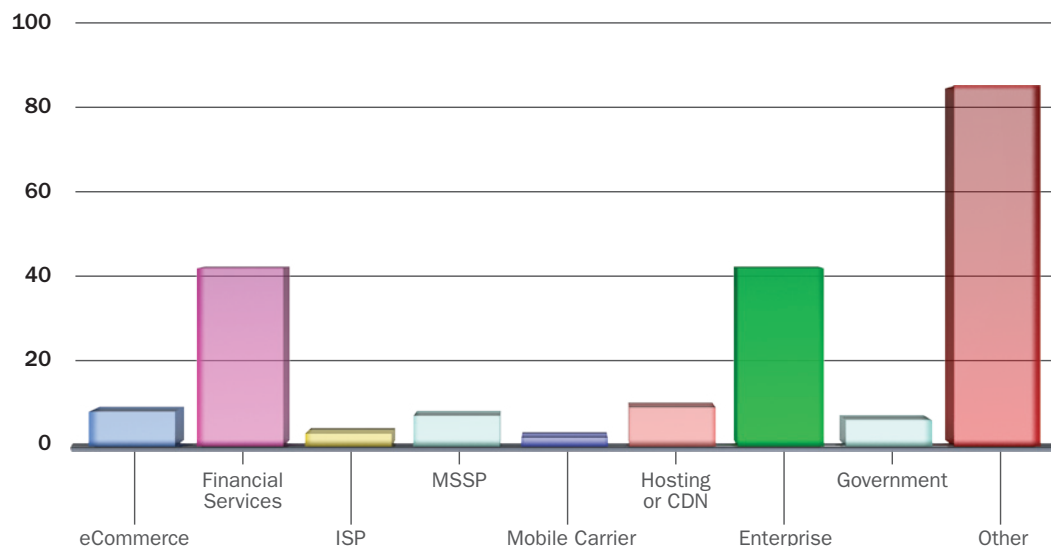


Figure 38: Organizations by type.

## What is the annual revenue of your organization?

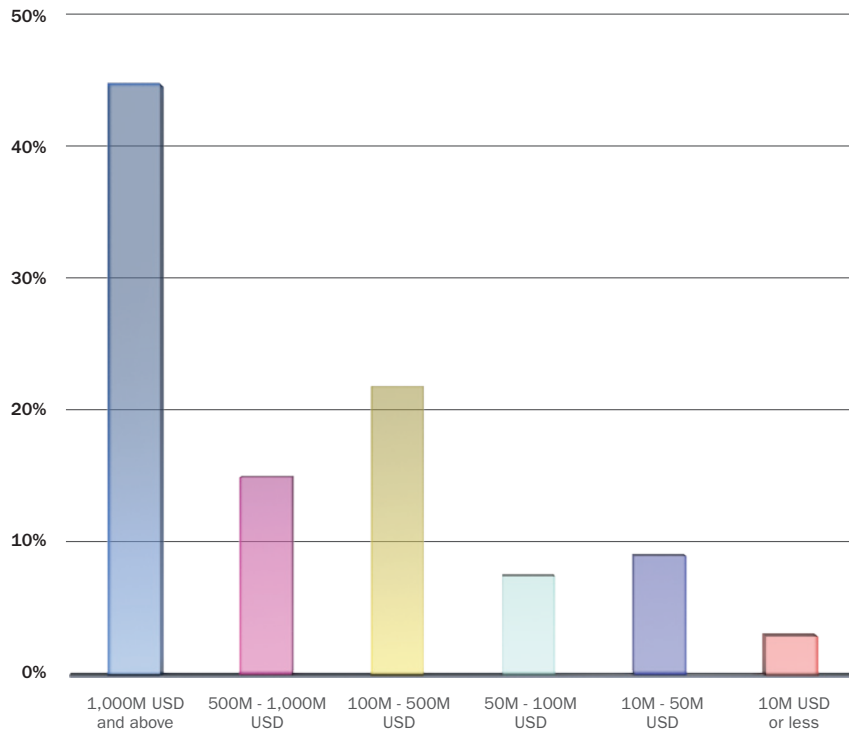


Figure 39: Annual revenue.

## How many employees are currently working in your organizations?

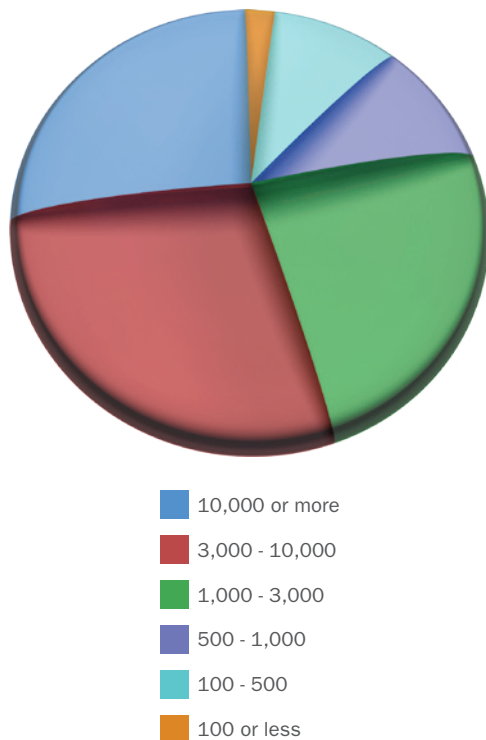


Figure 40: Number of employees in the organization.

## What is your role within your organization?

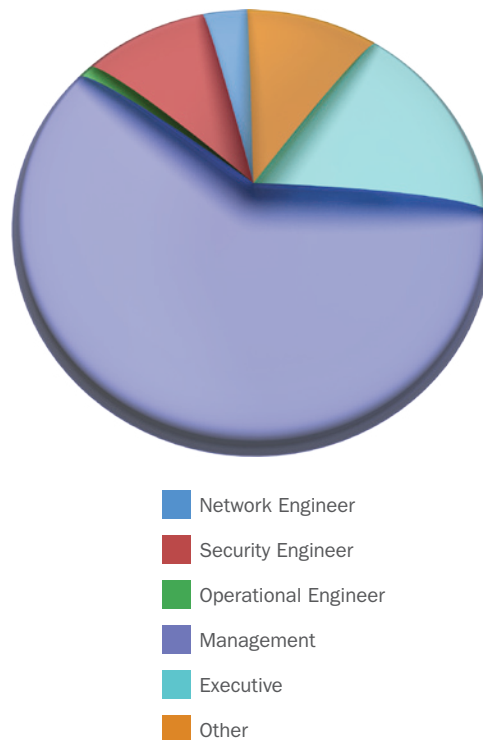


Figure 41: Employees' role within organization.

# Credits

## Authors

Ziv Gadot  
*SOC/ERT Team Leader,*  
Radware

Eyal Benishti  
*Security Researcher,*  
Radware

Lior Rozen,  
*Director of DefensePro R&D,*  
Radware

Yaniv Balmas  
*Security Researcher,*  
Radware

Matan Atad  
*Security Researcher,*  
Radware

## Advisory Board

Avi Chesla  
*CTO,*  
Radware

Carl Herberger  
*VP Security Solutions,*  
Radware

Ronen Kenig  
*Director, Security Product Marketing,*  
Radware

## Special Thanks

Carolyn Muzyka  
*Sr. Marketing Communications Manager,*  
Radware

## About the Authors

Radware (NASDAQ: RDWR), is a global leader of application delivery and application security solutions for virtual and cloud data centers. Its award-winning solutions portfolio delivers full resilience for business-critical applications, maximum IT efficiency, and complete business agility. Radware's solutions empower more than 10,000 enterprise and carrier customers worldwide to adapt to market challenges quickly, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit [www.radware.com](http://www.radware.com).

Radware' Emergency Response Team (ERT) is an emergency service with dedicated specialists that can respond in real time offering proactive, "hands-on" participation by security and product experts to mitigate active threat. Our longstanding relationships and reputation as a trusted advisor and solution partner make this guide possible. Our ERT has extensive experience handling attacks 'in the wild' as they occur.

Radware's ERT gives real-time assistance to customers under DoS/DDoS attacks. They do this by directly accessing the customer's network equipment, capturing the files, analyzing the situation and discussing the situation with the customer. Although the main intention of the service is to stop the attack and help the customer recover, the team also gets a unique view of the attack.

Due to their hands-on involvement, they get real-time information regarding what the attack actually looks like. They are able to actually measure the impact caused by the attack. In other words, ERT has an in-depth perspective of what really happens when a website is attacked. Generally, the ERT is only called upon to respond when it is a medium to high grade attack campaign.

## For More Information

Please visit: [www.radware.com](http://www.radware.com) and <http://www.ddoswarriors.com> for additional expert resources and information.



© 2013 Radware, Ltd.  
All Rights Reserved.  
Radware and all other  
Radware product and  
service names are  
registered trademarks of  
Radware in the U.S. and  
other countries. All other  
trademarks and names  
are the property of their  
respective owners.

## About Radware

Radware (NASDAQ: RDWR), is a global leader of application delivery and application security solutions for virtual and cloud data centers. Its award-winning solutions portfolio delivers full resilience for business-critical applications, maximum IT efficiency, and complete business agility. Radware's solutions empower more than 10,000 enterprise and carrier customers worldwide to adapt to market challenges quickly, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit [www.radware.com](http://www.radware.com).

Radware encourages you to join our community and follow us on [LinkedIn](#), [Radware Blog](#), [Twitter](#), [YouTube](#) and the [Radware Connect](#) app for iPhone® .