radware

2011

Global Application & Network Security Report

2011 Global Application & Network Security Report

radware

Smart Network. **Smart** Business.

Table of Contents

Smart Network. **Smart** Business.

01

Executive Summary

2011 was the year in which DoS / DDoS attacks turned from its niche corner and became a mainstream security threat. The single most important reason for this is the Anonymous phenomena. This loosely organized group brought virtual social protests to the forefront with attacks on large and well-known organizations. Their major campaign, Operation Payback, during the WikiLeaks saga in December 2010 against those supporting the US government was the turning point that shaped the security scene in 2011. After it, similar attacks become ubiquitous worldwide. Anonymous popularized DoS / DDoS attacks and made them well known not only among the security community, but also to the public.

As a result, the traditional targets for DoS / DDoS attacks were not the same. The financial sector, which had not really considered itself as a prime target, was hit and urgently forced to confront threatening situations. Government sites had been targeted before, but 2011 saw a dramatic increase in frequency, and neutral governments that felt themselves exempt, like New Zealand, were attacked. By the end of 2011, it was generally concluded that no organization, large or small, could say it was immune from DoS / DDoS attacks.

Denial of Service attacks became much more organized and professional in 2011. The attacks became more complex with attackers using as many as five different attack vectors in a single “attack campaign”. Hackers had become quite sophisticated blending both network and application attacks in a single offensive. In addition, those in control of these attacks learned to plan their campaigns strategically. Groups like Anonymous vote on a target, select the most appropriate attack tools, advertise the campaign and invite anyone capable of downloading the tools to participate in the attack.

In addition, they take time prior to the attack to test their tools effectiveness against the target site. While the attack is in progress, they do not rely just on volunteer participants, but the inner circle of more knowledgeable computer hackers compliment the attack with other effective tools. To summarize, the nature of DoS / DDoS attacks has become more of an Advanced Persistent Threat (APT) and, therefore, much more serious.

For the security community, mitigation became an important topic. Many organizations either had no protection at all or had inadequate protections in place, and found themselves unprepared for these attacks. On the bright side, the very public attacks last year raised awareness of DoS / DDoS and made organizations acquire better and more capable mitigation solutions. It also made security experts aware that there are new horizons to expand mitigation and that they needed to find new counterattack technologies enabling them to move from defense to offense.

02

Introduction

Scope of the Report

The Radware Security Report is an annual report prepared by Radware that focuses on denial-of-service and distributed denial-of-service (DoS/DDoS) attacks and their mitigation. This document is intended for the entire security community and is designed to be an authoritative report about DoS / DDoS attacks and network security in 2011. It is based on two sources. The first source was a Radware Security Survey sent to a wide variety of organizations to get responses that are vendor neutral and as objective as possible. The second survey analyzed 40 selected cases that were handled by the Radware's Emergency Response Team (ERT). It was conducted by Radware's internal DoS / DDoS security experts in order to provide a deeper forensic analysis that could not be expected from the former survey population.

The goal of this report is to produce an informative and educational document that analyzes the status of DoS / DDoS attacks during 2011. This document covers the types of attacks experienced, their victims, and presents an overview of the mitigation technologies. It is not designed to promote any specific solution, but only to capture the current state of DoS / DDoS.

Radware Security Survey

The Radware Security Survey was designed to collect factual and concrete information regarding the issues facing network operators combating DOS attacks during 2011. The survey consisted of twenty three questions divided into four sections addressing the following topics:

- General – queries about general information
- DoS / DDoS Experience – queries about the nature of the attacks
- DoS / DDoS Impact and Mitigation – queries about the impact and mitigation techniques
- Real World Attacks – queries to get additional in-depth information about the three most severe attacks experienced

In order to be objective, the survey was sent primarily to organizations that are not using the Radware Anti-DoS solution (DefensePro). Radware received 135 responses to this survey most of whom are not currently customers of Radware.

The graphs below identify the survey population. As seen in Figure 1, 80% of the survey participant confirmed that they are not Radware DoS / DDoS mitigation customers. Figure 2 shows the revenue generated by the various organizations participating in the survey. The survey represented large, medium and small organizations. Figure 3 indicates the role and responsibility of the individual completing the survey. The majority of the surveys were completed by security engineers and network engineers. The managers and executives who participated in the survey were the organization's security and network managers such as CISO, CIO and IT directors.

Radware Security Survey:

Is your organization currently using the Radware Anti-DoS product (DefensePro)?

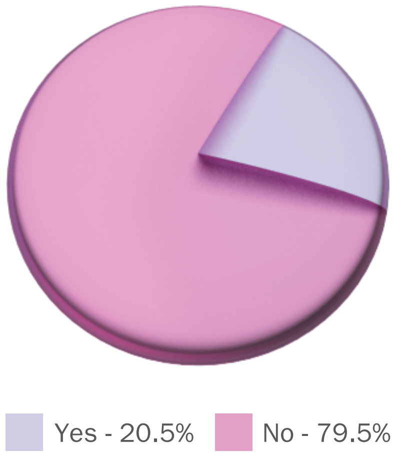


Figure 1: In order to be objective, the survey was sent primarily to organizations that are not using the Radware Anti-DoS equipment

Radware Security Survey:
What is the annual revenue of your organization?

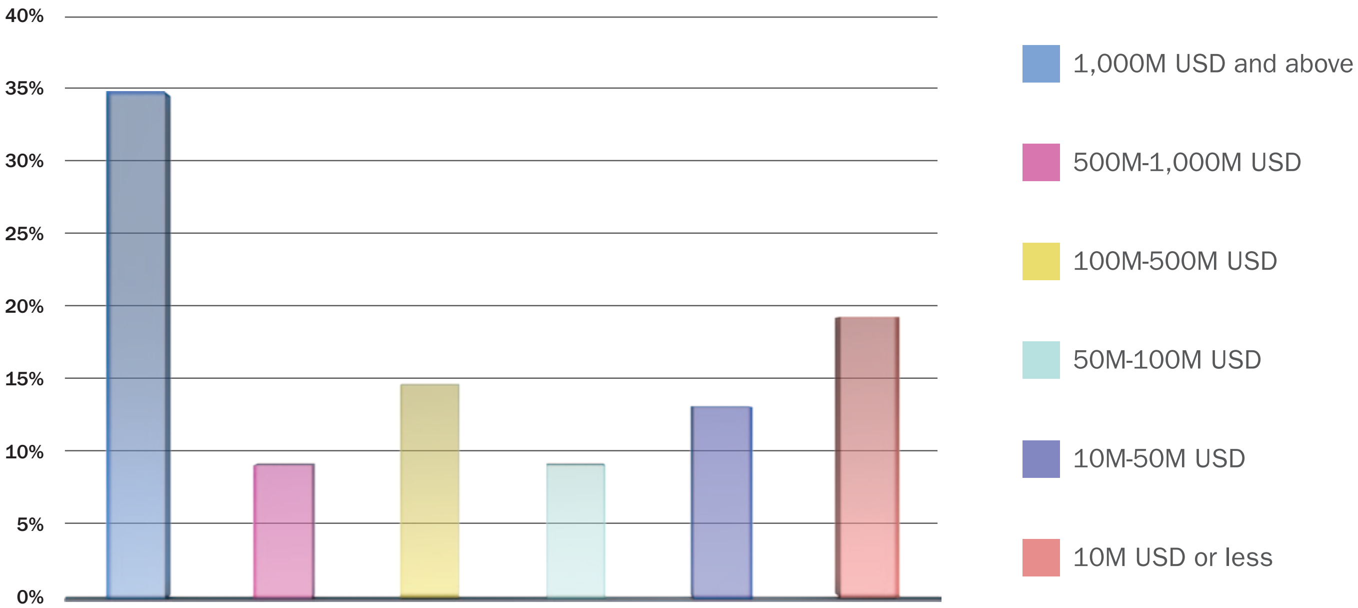


Figure 2: Radware surveyed a wide range of organizations from small to large as the shown in the graph defining the revenue of the organizations evaluated.

Radware Security Survey:

What is your role within your organization?

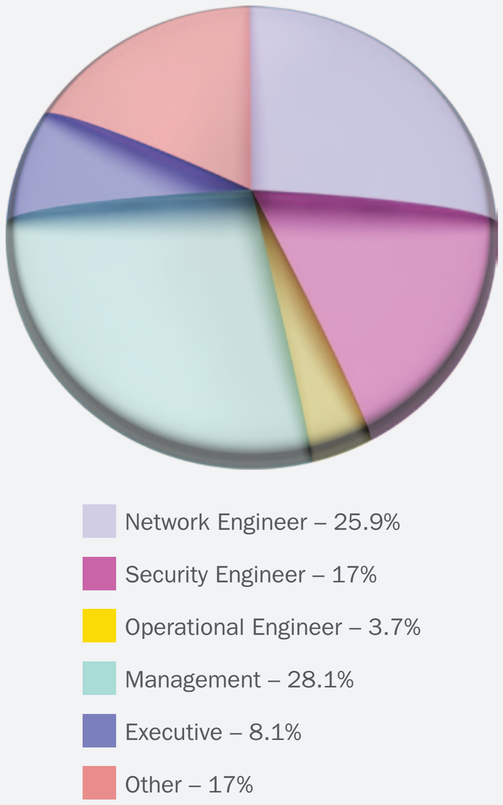


Figure 3: The executives and managers who completed the survey were CISO, CIO, and IT directors.

The ERT Survey

In order to understand the nature of the ERT contribution to the report, it is necessary to explain the function of this team. The 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. Radware's ERT gives real-time assistance to customers under DoS / DDoS attack. 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.

To provide a more in-depth analysis for this report, Radware analyzed 40 selected ERT cases as a separate survey. The additional analyses provided by this ERT survey added deeper, forensic information to the external survey.

03

Hacktivism and the Rise of Anonymous

Since the inception of the Internet, hackers have created DoS / DDoS attacks mostly by generating floods that prevent legitimate users from accessing a site. Hacktivist vigilantes used a variety of Internet tools to organize and perpetrate attacks mainly for political reasons. These groups are able to muster additional power from masses of lay users who may not even be fully aware of what the tools they downloaded are capable of doing. In 2011, there was a definite trend toward more sophisticated political attacks.

Hacktivism

Hacktivism is a controversial term that can be defined as using digital tools as a form of political and social protest. Hacktivists use a number of different tools to promote their messages including web site defacements, denial-of-service attacks, information theft and other types of virtual interference. This type of "civil disobedience" covers a broad range of activities hacktivists use to promote their political agenda and publicize their messages. They reinforce the message by showing that the Internet is not really safe. The most notorious hacktivist group today is Anonymous.

DoS
Denial of Service (DoS) is when an Internet site is unable to provide service. The DoS attack causes the site to not function either temporarily or permanently. The most common method used by attackers is to send massive numbers of requests to a designated Internet service. This forces the target to use their resources on these false requests until the target's resources are exhausted, thereby denying service to legitimate users. Other methods include using software vulnerabilities or design weaknesses.

DDoS
A Distributed Denial of Service (DDoS) attack is a DoS attack carried out by multiple systems. It requires the cooperation and coordination of all participants to generate an effective attack. This cooperation can be achieved, for example, with a botnet. Most flood attacks are DDoS since they require more than one computer to generate sufficient malicious traffic that would cause impact on the target.

Floods
Flood attack is a synonym for a DoS / DDoS attack that is based on sending large amounts of traffic. In this technique the DoS is caused by flooding the target's network with too much data, or servers with too many requests, until they can process no more.

Radware Security Survey: Which of the following motivations are behind the DoS / DDoS attacks you experienced?

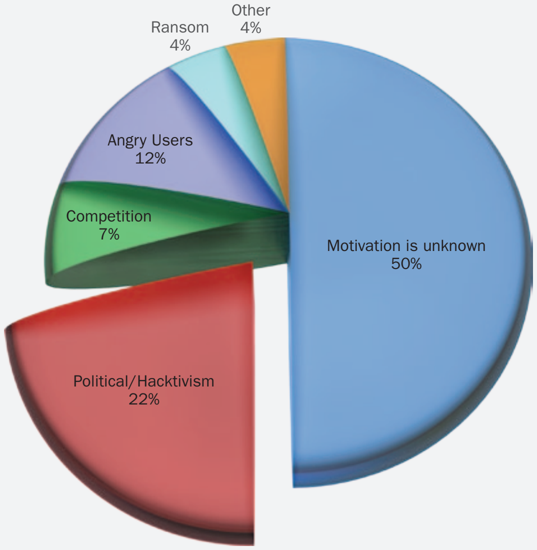


Figure 4: While the "unknown motivation" is still prominent, the most prominent motivation is by far Political/Hacktivism

ERT Survey: Motivation Behind Attacks

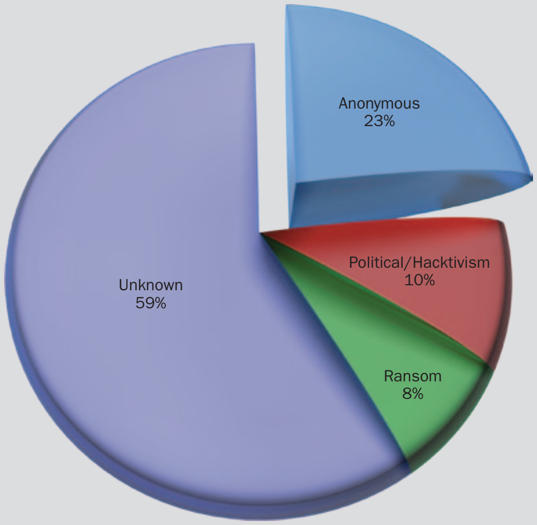


Figure 5: ERT cases due to Anonymous attacks increased from nearly 0% to 23% in 2011

Anonymous is a term used to describe a loose collection of Internet savvy hacktivists who use their abilities to initiate acts that they consider civil disobedience. This group is geographically diverse, but it has developed into a virtual community that attempts to maintain the anonymity of its members. Anonymous finds its members from IRC channels and a variety of chat rooms all over the world. In the beginning, Anonymous rallied this digitally connected community mainly for attacks to support what they perceived to be infringements on the rights of the entertainment industry. But its hacktivism agenda has become more diverse, and has expanded to protest those who would curb the freedom of the Internet and freedom of speech.

Anonymous has created a brand for itself by using the Guy Fawkes mask from the comic book series and movie, *Vendetta*, which made this face popular. Everyone looks alike, and can't be identified.

Anonymous Projects

Last year saw a significant shift in motivation of DoS / DDoS attacks that was mainly due to the political agenda of the Anonymous group. Their chosen targets really put DoS / DDoS attacks on the front pages of the media in 2011. No organization is immune. Anonymous not only attacked government organizations, but financial and commercial sites as well. Their motivation is usually political or to pursue a cause. Anonymous draws most of its power from average computer users. The inner circle or administrators of Anonymous depend on easy to download tools that can be downloaded by anyone with a computer.

Figure 6: Anonymous

Anonymous Power

The brute force of Anonymous attacks comes from massive numbers of these non-technical users who are able to join in the fight even though they may not be aware of how these tools work or exactly what they are doing. The fact that so many users join the attack enables Anonymous to gather the strength needed to flood a website and deny service to legitimate users.

Anonymous Opens Fire

A prime example of how Anonymous made news is when it launched Operation Avenge Assange, which was part of Operation Payback, following the controversy over leaks of United States diplomatic cables. In December 2010, Anonymous chose to support Wikileaks founder Julian Assange, and called for DoS / DDoS attacks against the banks and credit card companies that had succumbed to political pressures to stop transferring payment to Wikileaks. The group then escalated to diverse attacks on major pro-copyright and anti-piracy organizations, law firms, and even individuals. These attacks were diligently reported in the media, and Anonymous gained notoriety. They also gathered a reputation as a powerful group of sophisticated hackers; but Anonymous remains a loose organization with informal leadership and most of their attacks are done on-the-fly. Anyone can act in the name of Anonymous, it is not necessary to be a skilled hacker or real computer geek. However, there are real experts in the mix as well.

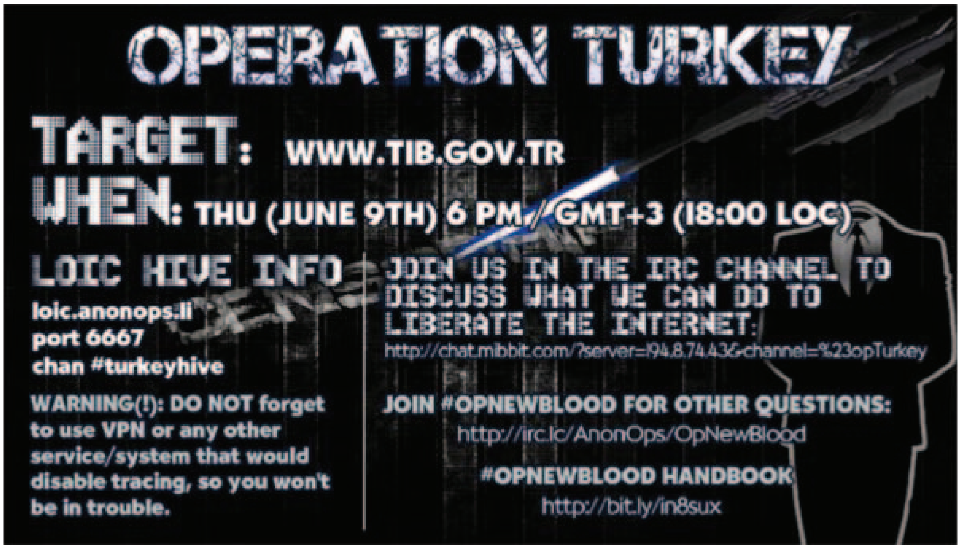
As stated before, Anonymous encourages the global public to add their voice to their causes by propagating the Low Orbit Ion Canon (LOIC) tool that can be downloaded and used by even the most non-technical person. There is a simple to follow short video tutorial. Once the tool is downloaded, all the user needs to do is fill in the parameters as shown on the web postings. With this power behind the attacks, Anonymous was able to impact even very respected web sites.

Section Highlights

- 2011 - Anonymous mainstreamed the DoS / DDoS attack – increasing its threat level dramatically
- Open salvo in December 2010 - Operation Avenge Assange (part of Operation Payback) attacks financial institutions that stopped supporting WikiLeak's owner, triggering numerous attacks during 2011
- Anonymous advertises an easy-to-download application (LOIC) that enables anyone with a computer or laptop to participate in their DoS / DDoS attacks
- Anonymous insiders, the "inner ring", conduct more sophisticated attacks in parallel to attacks by the general public
- Anonymous attacks threaten organizations, cause havoc and are taken seriously by potential victims

Case Study: Attack on Turkish Government

The Turkish government planned to implement an additional filter on Internet browsing under the pretense of protecting the youth from “harmful elements on the web”. Critics argued that the proposed filters would lead to wide-spread censorship. Anonymous saw this as a denial of free speech and decided to protest what they felt was government censorship. The administrators of Anonymous put out an Internet message to the general public asking them to join the protest.



OPERATION TURKEY

TARGET: WWW.TIB.GOV.TR

WHEN: THU (JUNE 9TH) 6 PM / GMT+3 (18:00 LOC)

LOIC HIVE INFO

loic.anonops.li
port 6667
chan #turkeyhive

WARNING(!): DO NOT forget to use VPN or any other service/system that would disable tracing, so you won't be in trouble.

JOIN US IN THE IRC CHANNEL TO DISCUSS WHAT WE CAN DO TO LIBERATE THE INTERNET:

http://chat.mibbit.com/?server=194.8.74.43&channel=%23opTurkey

JOIN #OPNEWBLOOD FOR OTHER QUESTIONS:

http://irc.lc/AnonOps/OpNewBlood

#OPNEWBLOOD HANDBOOK

http://bit.ly/in8sux

Figure 7 - Poster directing Anonymous group supporters how to attack

The message clearly stated the target site (www.tib.gov.tr), the time and place of the attack (Thu June 9th at 6PM or GMT + 3 if you were not local) and the website to download the tool needed to participate in the attack. With this advance notice, the Anonymous group launched attacks against several main government sites with the help of all the volunteers who downloaded the LOIC attack tool, which is described in the section on attack tools. In this way, Anonymous was able to launch simultaneous attack campaigns against several government sites, to protest government censorship.

The attack campaign coordinated thousands of non-technical computer users who downloaded the LOIC tool in order to create a botnet of computers to create the floods. The message board posters sent by Anonymous gave explicit instructions so that the general public could easily join the attack. The attack campaign called for a multi-vector attack, which means that several different types of messages were sent to the sites. This attack sent the following vectors:

- HTTP Get flood attack – targeting the web application resources and further modifying the target URL during the attack
- TCP connection flood on port 80 – targeting the web application resources
- SYN flood attack – targeting the server TCP/IP stack
- UDP flood attack – targeting network bandwidth resources

Other attacks were evident, such as fragmented packets flood and Reset flood sessions. Attack bandwidth reached over 1Gbps of traffic and above 3,000,000 concurrent sessions. While some of the attacks were generated by lay people who downloaded the tools, other vectors were clearly perpetrated by the inner ring Anonymous hackers.

Anonymous Modify Attack Vectors to Avoid Personal Prosecution

There is one small problem with the LOIC tool - it does not protect the identity of the user. It leaves a footprint that makes it easy to track the user's real IP address and there have already been several arrests. In the United States, the Federal Bureau of Investigation (FBI) launched an investigation and arrested eleven people after an attack on a federal website. There have been arrests in other countries as well. The tool does not really make users anonymous and many connected with the group want to put this tool out to pasture because it leaves users open to being identified and arrested.

In order to continue their attacks, Anonymous is developing new intrusion-based tools, such as the #RefRef, which is designed to exploit software vulnerabilities. The tool is platform neutral, leveraging JavaScript and vulnerabilities within SQL to create an overwhelming impact on the targeted website. The tool is said to use the target site's own processing power causing resource exhaustion. Resource exhaustion is an attack vector that has existed for some time, but is often ignored by attackers who favor the brute force of a DoS / DDoS attack. However, this tool in theory is very effective; a 17-second attack from a single machine resulted in a 42-minute outage on a test site.

The effectiveness of #RefRef is because it exploits a widespread vulnerability. The flaw is apparently known but not widely patched yet. The tool's developers know that they can probably hit a high profile site only once before the tool is identified, but that is enough for them. This means that there are a lot of possible targets that are vulnerable and can be hit at least once before the tool is blocked. While the #RefRef tools' effectiveness is questionable, it points to the direction Anonymous is currently going.

Section Highlights

- In the post-LOIC period Anonymous is not depending on mass user participation for their attacks. This is to protect their supporters from legal actions that several countries are already enforcing
- To compensate for the LOIC, Anonymous is focusing on their inner-circle hacking activities, which include the development of tools such as #RefRef that rely on exploiting software vulnerabilities rather than brute force attacks
- Despite the chaotic and headless nature of Anonymous, they are a persistent threat modifying the means in order to accomplish their goals. When they realized their first LOIC strategy didn't work, they developed a different tool that is vulnerability and intrusion-based

A Post-LOIC Attack – Case Study

In one of its latest attacks, Anonymous publicized its protest via a video message on YouTube. In addition, links were posted to the Anonymous Twitter feed that invited users to download the LOIC tools and participate in the campaign. However, there were other communications that warned users proclaiming "Save Yourself", noting that others who had joined Anonymous attacks via the LOIC tool had been identified and arrested. Nevertheless, the attacks continued and according to ERT analysis the success of these Anonymous DoS / DDoS attacks cannot be attributed to the mass use of the LOIC tool alone. Instead, there is an inner circle of Anonymous that has access to more sophisticated methods and tools so that they do not need to rely only on the volunteers who are able to generate a brute force for this attack using LOIC.

This was a much more sophisticated attack using a multi-vulnerability cyber-attack vectors that included:

- Oversized UDP Frame Flood (over 1Gbps)
- Multiple LOIC DoS Tool TCP attacks
- Multiple LOIC DoS Tool UDP attacks
- Multiple Mobile DoS LOIC (HTTP flood)
- Multiple UDP Floods on port 80, on port 53 and random ports (300 Mbps+)
- #RefRef DoS Tool attacks (home grown by Anonymous – first time witnessed!)
- TCP Fragment Floods

04

Attack Sizes Varies Dramatically

DoS / DDoS attacks pose a serious threat and their rate of growth presents a distinct challenge to both businesses and governments. Since it is likely that DoS / DDoS attacks will continue to target organizations, it is important that the people who are responsible for Internet security describe and measure attacks accurately and precisely.

Most Internet sites are inherently vulnerable, making it a major challenge for the average organization to predict whether or not their site will be attacked and what the volume of that attack might be. This section describes three types of DoS / DDoS attacks and explains how these attacks should be measured and evaluated.

Major DoS / DDoS attacks are often reported using measurement terms like “A 50 Gbps UDP attack attacked site X” or “A 30M PPS DNS attack attacked site Y” because numbers like 50Gbps or 30M PPS are easy to understand and make a complex subject somewhat comprehensible to the average reader. But these size measurements do not really explain what is happening during a DoS / DDoS attack, and provide minimal insight.

When evaluating DoS / DDoS attacks, the belief that only the size of the attacks counts is a “myth” about what is happening when a site is attacked. It is important to understand both the size and type of attack. The belief that the bigger the attack, the more severe is incorrect. In reality the type of attack is also significant. A much smaller HTTP flood on the application level, for example, may do more damage than a larger UDP flood on the network.

The first myth debunked is that organizations need to prepare for enormous attacks. The actuality is that the average organization may never experience an intense attack. The participants of the Radware Security Survey were asked to specify the largest attacks by bandwidth that they experienced. Figure 8 shows that many attacks are not enormous. The results showed 32% of attacks were less than 10Mbps, while 76% were less than 1Gbps.

It is essential to take the type of attack as well as the size into account. It is not accurate to measure all attacks by the same standards. Smaller, less intensive attacks can still cause serious damage.

Radware Security Report:

Attacks by Bandwidth

Figure 8: Most attacks are not enormous, yet they can still be damaging

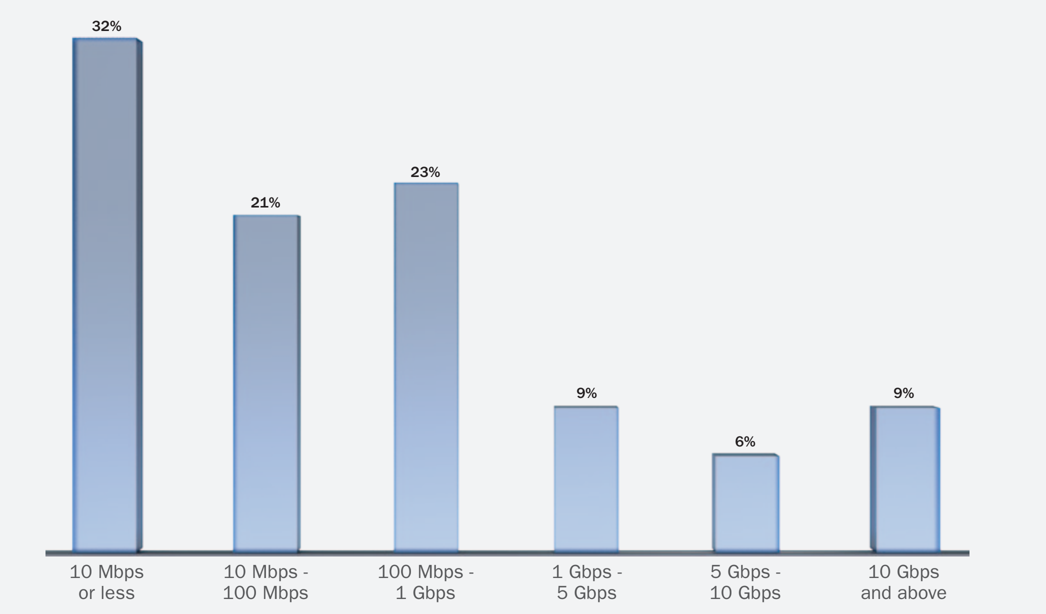
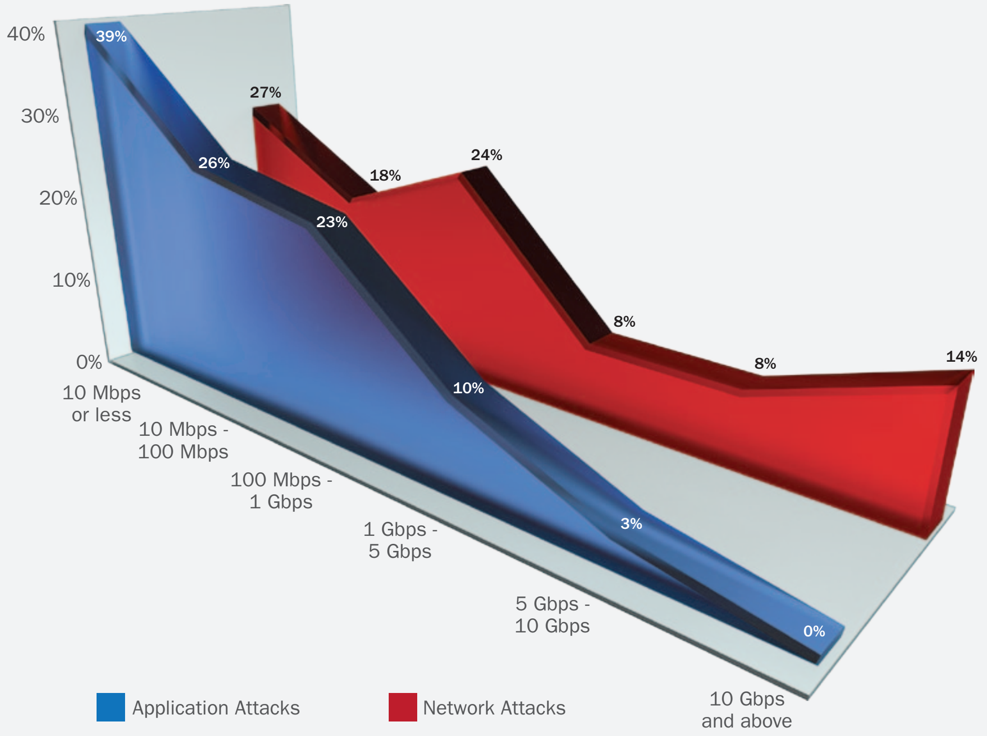


Figure 8 shows that many attacks are not enormous. The participants of the Radware Security Survey were asked to specify the largest attacks by bandwidth that they experienced. The results showed 32% of attacks were less than 10Mbps, while 76% were less than 1Gbps.

The media reports sensationalize large attacks which supposedly causes organizations to prepare defenses they feel are needed to protect themselves against these large attacks. However, it is essential to take the type of attack as well as the size into account. It is not accurate to measure all attacks by the same standards.

The second myth is that the proper way to measure attacks is by their bytes-per-second (BPS) and packets-per-second (PPS) properties. If the number of packet is high, the attack is more serious. Following this logic, a 10Mbps UDP flood would be more severe than a 5Mbps HTTP flood, which is not necessarily true.



Radware Security Report:

Network versus Application by Bandwidth

Figure 9: Generally application attacks are smaller in bandwidth than network attacks, but cause as much or more damage

The chart in Figure 9 shows the difference between network and application floods. Network attacks reported include UDP, ICMP and SYN floods. Application attacks include HTTP, HTTPS, and SMTP. It is evident that application floods are much smaller than network floods; however that does not indicate the severity of the attack or the problems it causes for victims.

When evaluating DoS / DDoS attacks the measurement scale should match the type of attack. There is no point in comparing a UDP flood to an HTTP flood. The proper measurement scale for UDP floods is in bandwidth and PPS while the measurement scale for HTTP floods is in transaction per second, concurrent connections and new connections-per-second. The significance is in how the attack affects the victim. The UDP flood may seem to be larger and more dangerous, but the HTTP connection-based attack can cause more damage with much less traffic than the UDP attack. In various cases, which were handled by the ERT, it was observed that attacks that are much less intensive can still cause serious damage.

Attack measurements can be divided per type of attack as follows:

Attack Types	Description	Measurements	Remarks
Brute Force Floods UDP floods, ICMP floods, SYN floods, and TCP out-of-state floods (RST flood, FIN+ACK floods, etc.)	Bombards the network with as much data and as many packets as possible without establishing a full network connection	Measured in Mbps (bandwidth) and PPS (packets per second)	Attackers do not need to invest resources in maintaining the connection
Connection Based Floods HTTP floods and SMTP floods	Designed to flood the application layer	Measure these attacks in HTTP transactions per second, concurrent connections, new connections-per-second	Requires the attacker to establish a legitimate connection
Slow Rate R.U.D.Y (Are You Dead Yet), Slowloris, and Sockstress	Targets specific vulnerabilities or design flaws	Measuring these attacks is difficult since each attack is unique. For example, R.U.D.Y. attack intensity can only be measured by the number of concurrent connections and the number of attackers	The attack measurements are uniquely tied to the attack, but sometimes there is no point in trying to measure the attack

The question still remains: What type and size should an organization expect and what are the options that can be taken by an organization to prepare for a DoS / DDoS attack? This is not an easy question to answer even if we narrow the parameters to a single industry. For example, what kind of attack should an e-commerce site expect? Unfortunately, we still don't have a ready answer. DoS / DDoS attacks are so diverse in both type and size that it is impossible to make any kind of accurate predictions.

In many cases handled by the ERT the customer was not prepared for the attack. It was not that the customer did not prepare for the right type of attack or the right size of the attack; it was that the customer did not have a DoS / DDoS mitigation solution ready. They may have had a firewall and anti-virus security solutions, but they were unequipped to mitigate a DoS / DDoS attack.

In conclusion, when reviewing and analyzing DoS / DDoS attacks, it is important to measure attacks with the appropriate matrices. The attacks seen by the ERT are so diverse in volume, that it is impossible to present a definitive picture on upcoming or expected attack volumes. That being said, many organizations don't prepare at all. They should be aware of the frequency and severity of DoS / DDoS attacks and take some precautions against attacks.

05

DoS / DDoS Attack Nature Becomes More APT Oriented

DoS / DDoS attacks have been around for a long time. They originally began with network floods, which were brute force attacks designed to stop traffic, like UDP floods that saturate the Internet pipe and SYN floods that overwhelm the firewall. Later, the attacks became more sophisticated as hackers “climbed” into the application level using HTTP, SMTP and other flood attacks. Today, it is still easy to create a massive flood since there are many sites that have not updated their protection and they cannot cope with newer traffic rates. These attacks hit the computer resources in its “soft belly” to overload memory and make computers so slow as to be unusable. However, one type of attack does not replace the other.

Radware Security Survey: Attack count by type and bandwidth

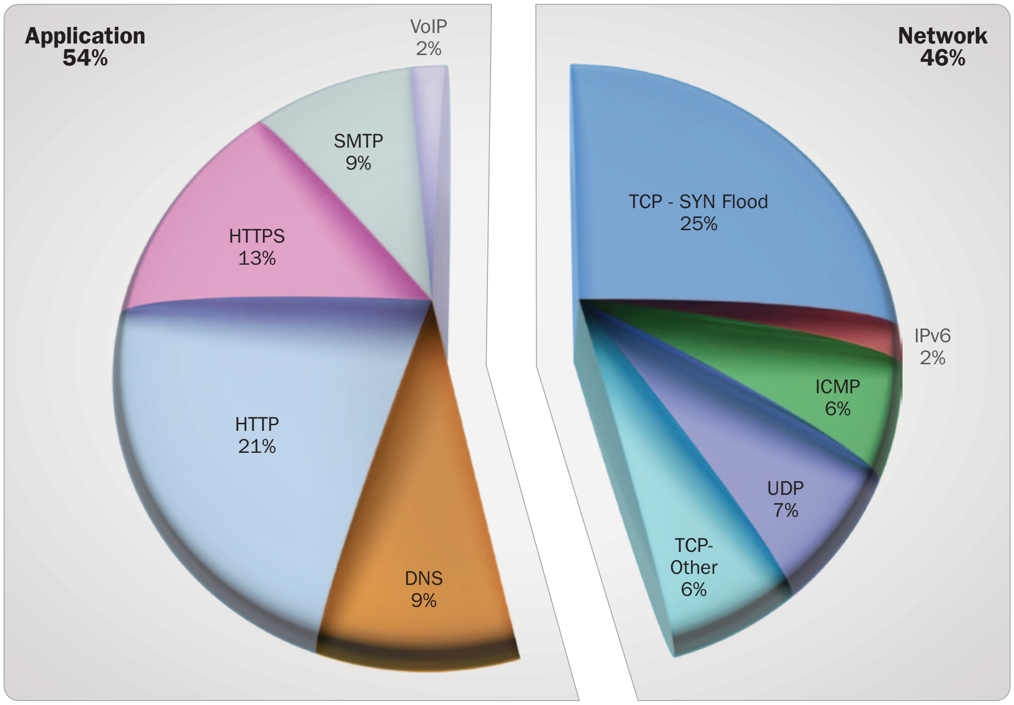


Figure 10: Network and application attacks co-exist

Application attacks are only slightly more popular than network attacks, but as the chart shows application level floods co-exist with network level floods. During the past year, the number of application versus network floods did not change appreciably.

However, the nature of DoS / DDoS attacks is changing. The most significant change seen during 2011 was the rise in attack campaigns, which is when the attacker blends several attack vectors combining network and application floods and even adding slow rate attacks into the mix. Last year saw a dramatic increase in these multi-vector attacks. The ERT has seen attack campaigns perpetrated by Anonymous as well as other attackers; they easily counted four to five attack vectors in a single campaign. The attacker moves from one attack vector to another until the best one is found or the attacker may combine two vectors since together they may have a greater impact than an even larger single vector. However, even if one vector is successful, the impact on the business web site can be severe.

Attack campaigns that blend various attack vectors are not the only thing that makes DoS / DDoS attack campaigns more APT oriented. In Anonymous attacks, for example, they select a target date and the time of the attack, and invest a great deal of effort inviting others to join the attack via web posts, chat rooms, Twitter, Facebook, etc. A day or two before the attack Anonymous will have conducted a short fireproofing, maybe a 10 minute test, to check in advance the effectiveness of their arsenal. In an attack on one financial organization, ERT noticed the attacker deliberately chose to attack at a time that was most critical and painful for the victim.

In general, they are also well-funded. One of the key features of APT is that it represents the very high level of professionalism reached by hackers today. A prime example is the Stuxnet worm, which is the first malware that has targeted industrial systems, such as power plants, factories and suspected uranium enrichment infrastructure in Iran.

Attack campaigns that blend various attack vectors are not the only thing that makes DoS / DDoS attack campaigns more APT oriented: in Anonymous attacks, for example, they select a target date and the time of the attack, and invest a great deal of effort inviting others to join the attack via web posts, chat rooms, Twitter, Facebook, etc. A day or two before the attack Anonymous will have conducted a short fireproofing, maybe a 10 minute test, to check in advance the effectiveness of their arsenal. In an attack on one financial organization, ERT noticed the attacker deliberately chose to attack at a time that was most critical and painful for the victim.

In addition to the brute force and application level floods, attackers have another tool. They are conducting slow rate attacks using tools like Slowloris, Sockstress and RUDY. (A more detail description of this tool is in the section on Attack Tool Trends.) These tools can disrupt service and cause outages with just a small amount of traffic by capitalizing on specific design flaws. However, these tools are still not that prominent, as can be seen in the Figure 11.

In conclusion, DoS / DDoS attacks are becoming more sophisticated and APT in nature. This can be seen by the persistent efforts invested by the attackers. Attack planning has improved, the attack timing is carefully selected, and during the attack period multiple attack vectors are launched (network, application and slow rate), until the most painful one is found. From a higher security perspective, DoS / DDoS attacks are not only becoming intrinsically more APT oriented, they have also become a bigger weapon or “building block” of the overall APT scene. The best example of this is the attack on Sony Pictures in which a massive DoS / DDoS attack was the first stage believed to have been only camouflage for later attacks that were actually used to steal critical information.

Radware Security Report:

Have you ever been hit with a slow rate attack?

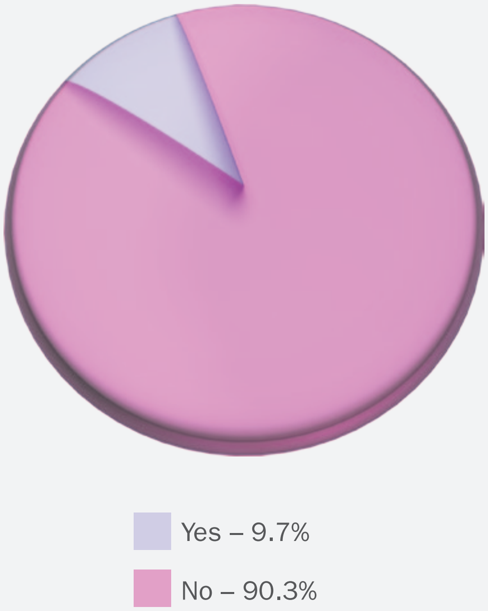


Figure 11: While slow rate attacks became more popular in past year, they are still not a major threat.

radware

06

The Internet Server is Not Necessarily the First to Fall

The Internet was designed with functionality, not security, in mind, which means that there are other network entities that can be vulnerable to DoS attacks. When a web server is under attack, it is not necessarily the first entity to fail. The Internet server capacity is only one reason why a DoS attack succeeds. It seems probable that when cnn.com is being attacked by an HTTP flood, it is expected that the web server will fail. However, it is already common knowledge that other network entities can be affected as well. The Internet pipe can get saturated and attacks may affect the router, firewall, IPS, load-balancers and SQL servers. Despite being designed to provide network security, firewalls and IPS, are impacted by DoS attacks. As a matter of fact, it is often the firewall that is the weakest link.

Radware Security Survey:
Which services or network elements are (or have been the bottleneck) of DoS?

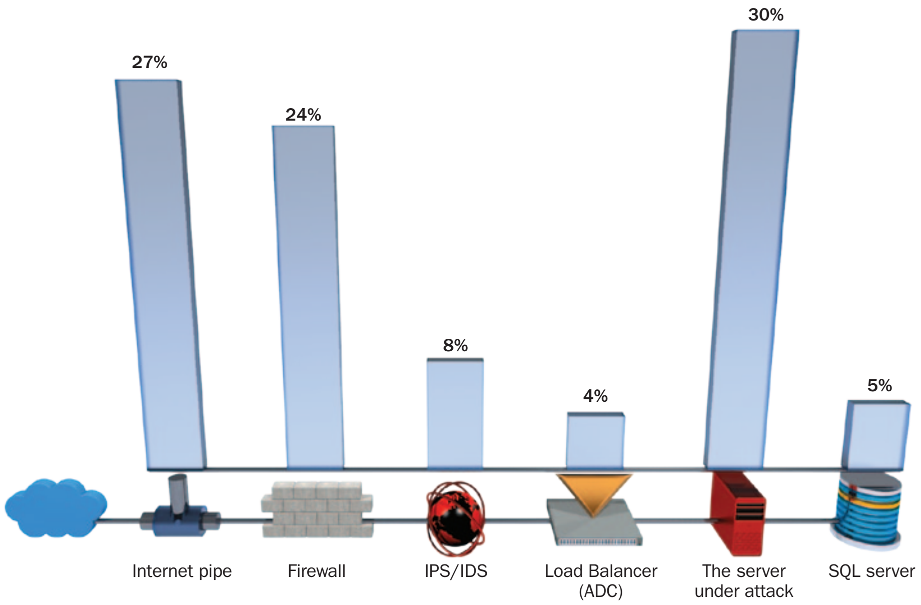


Figure 12: The Internet server under attack is not necessarily the one to suffer the effect of DoS, the Internet pipe and firewall are also likely victims

Those attacking the site seem to understand this as well. When they send a UDP flood of 1500 bytes per packet, the intention is to block the Internet pipe and not to attack the web server. However, the ERT's experience is that UDP floods and other network attacks are short-lived. They are highly visible and relatively easy to block. Attackers also seem to understand that a SYN flood and other connection based floods (TCP and UDP) are more likely to impact the firewall rather than the server.

Constantly updating these network elements to prevent attacks is not a solution. Network devices are simply not designed to deal with DoS / DDoS attacks, including even firewalls and IPS, which both have different security functions. The best solution is to deploy and properly position a DoS / DDoS solution capable of protecting all the relevant entities. If it is an in-house deployment, the organization should make sure that the ISP can clean the pipe from extremely high rate attacks or at least increase the pipe capacity quickly during such an attack.

What Happens When a Firewall is Not Protected - Case Study

Recently, a leading online travel agency was hit by a massive HTTP page flood. More than 4,000 attackers pounded this site for three days with the aim of overloading the site so that the servers would not be able to answer normal requests. Initially, the company set protections on their web servers to deny access to malicious clients, which were recognized by their user agent parameters. These requests were easily recognized by their Accept-Language HTTP Header, but even with this defense mechanism there was still a partial outage. The company then installed DoS / DDoS mitigation hardware. This same protection was copy-pasted to their hardware. Since the hardware has dedicated resources, the web servers did not need to handle the attack and their functionality was restored. However, the resource overload moved to a different point in the network.

The company's security personnel noticed that the firewall session table was getting dangerously close to its maximum size. The DoS / DDoS mitigation hardware was then relocated in front of the firewall, protecting the firewall from being overloaded. Once the defense mechanism was relocated in front of the firewall, it stopped the attacking IPs and the firewall received only legitimate traffic. Once a protection policy with HTTP Page flood mitigation was set, the attack was mitigated restoring the web servers and the firewall resources returned to their normal state.

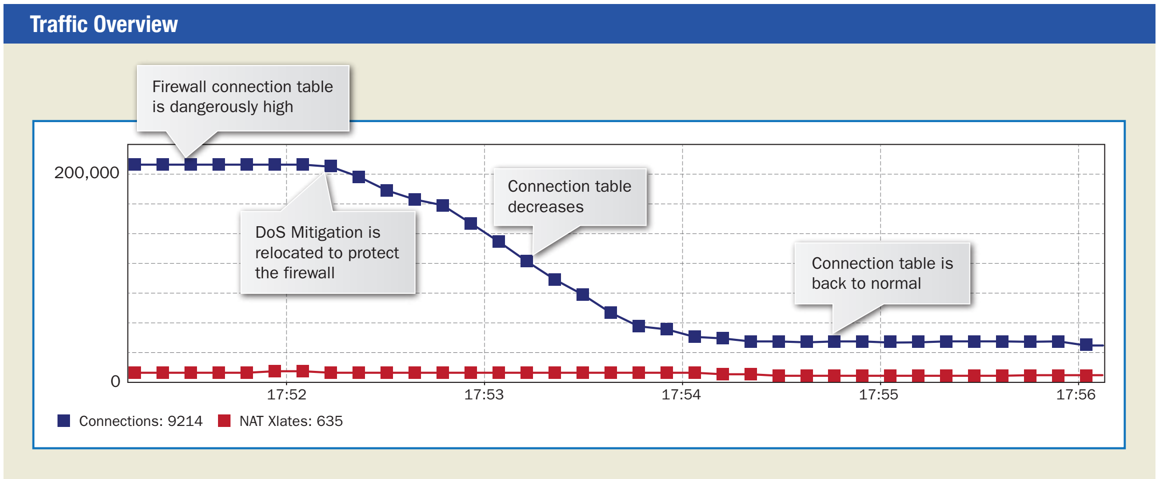


Figure 13: Firewall Snapshot
Snapshot of the firewall status taken the moment the DoS mitigation protected it. The moment the mitigation hardware protected the firewall, the number of connections returned to safe numbers.

radware

07

More Organizations are Now Under DoS / DDoS Threat

The Anonymous group has brought DoS / DDoS attacks into larger and more elaborate domains. Traditionally, hackers, like hacktivists, generally targeted government services and political sites. But Anonymous changed the playing field and added new victims that include financial institutions, the energy sector and even, to give an exotic example, drug cartels. Today, any type of site is more vulnerable to attack and should be aware of DoS / DDoS threats posed by groups like Anonymous. During 2011, Anonymous type hackers expanded their attacks to include financial institutions, the energy sector and many other types of sites that normally didn't consider themselves in the "ring of fire".

Since Anonymous is a basically a headless organization, virtually anyone with some computer skills can initiate an attack against a designated target with or without a reason. For this reason many organizations were caught totally unprepared to respond to a DoS / DDoS attack. They had no defense mechanism in place because they had never experienced the problem and never expected to be victims of a DoS / DDoS attack. In order to maintain service and stay on line, these organizations were forced to find and deploy a solution quickly.

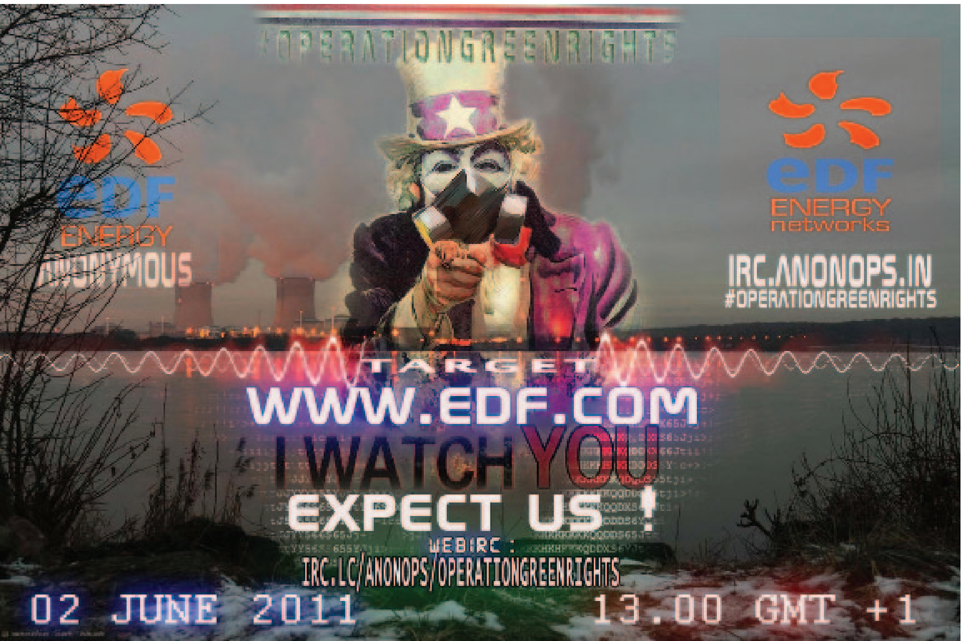
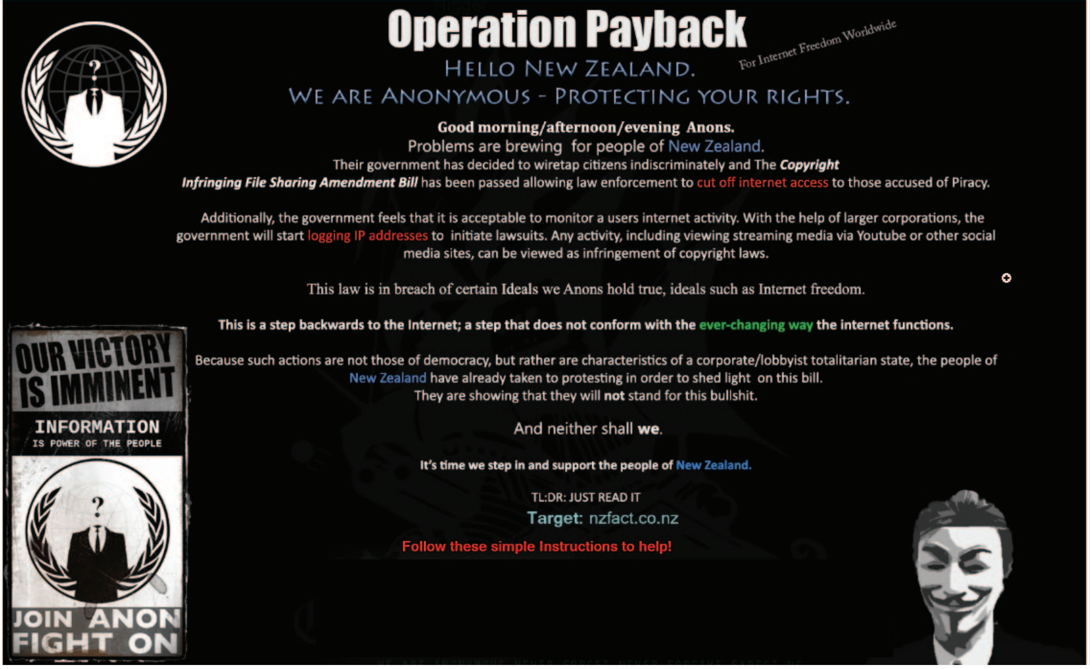


Figure 14: Anonymous Attack against www.edf.com
Anonymous use graphical banners to recruit supporters



Operation Payback

HELLO NEW ZEALAND.

WE ARE ANONYMOUS - PROTECTING YOUR RIGHTS.

Good morning/afternoon/evening Anons.

Problems are brewing for people of New Zealand.

Their government has decided to wiretap citizens indiscriminately and The ***Copyright Infringing File Sharing Amendment Bill*** has been passed allowing law enforcement to cut off internet access to those accused of Piracy.

Additionally, the government feels that it is acceptable to monitor a users internet activity. With the help of larger corporations, the government will start logging IP addresses to initiate lawsuits. Any activity, including viewing streaming media via Youtube or other social media sites, can be viewed as infringement of copyright laws.

This law is in breach of certain Ideals we Anons hold true, ideals such as Internet freedom.

This is a step backwards to the Internet; a step that does not conform with the ever-changing way the internet functions.

Because such actions are not those of democracy, but rather are characteristics of a corporate/lobbyist totalitarian state, the people of New Zealand have already taken to protesting in order to shed light on this bill.

They are showing that they will **not** stand for this bullshit.

And neither shall **we**.

It's time we step in and support the people of New Zealand.

TL:DR: JUST READ IT

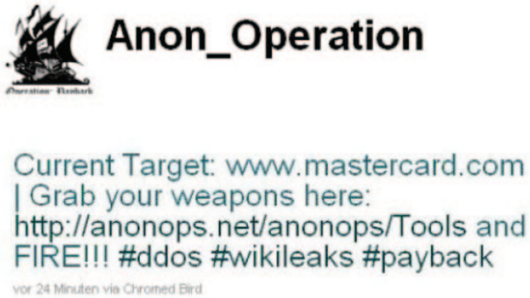
Target: nzfact.co.nz

Follow these simple Instructions to help!

Figure 15: Anonymous attack against New Zealand Parliament
Anonymous banner recruiting volunteers to participate in the attack on the NZ parliament.

Some of the more notable attacks that Anonymous perpetrated during the year included issues of free speech, preserving the openness of the net and righting perceived wrongs. For example, the group initiated attacks against the French nuclear giant, EDF to protest nuclear energy. And while Anonymous' historically perpetrated attacks for political reasons, the group targeted the usually non-controversial parliament of New Zealand when that government proposed laws restricting Internet freedoms.

The chart in Figure 17 shows an overview of DoS / DDoS attacks and cases handled by Radware's ERT in 2011 – due to DoS / DDoS attacks – segmented by customer type. As the chart shows, the Financial, e-Gaming and Government sectors take the lead. The large number of financial institutions requesting assistance from the ERT was not only due to a high number of DoS / DDoS attacks; it is also an indication that most institutions of this kind were totally unprepared. The financial sector had not experienced DoS / DDoS attacks prior to and during 2010, and therefore did not invest in DoS / DDoS mitigation solutions. In contrast, e-Gaming sites that were attacked prior to 2011 were generally more prepared. The e-Gaming industry has been the target of DoS / DDoS attacks for many years, so it has invested in solutions, and was generally more prepared than the financial sector.



Anon_Operation

Current Target: www.mastercard.com | Grab your weapons here: http://anonops.net/anonops/Tools and FIRE!!! #ddos #wikileaks #payback

vor 24 Minuten via Chromed Bird

Figure 16: Anonymous
Attack against www.mastercard.com during Operation Avenge Assange

In this Twitter account Anonymous provides real time instructions to its supporters on who to attack (MasterCard), and also supplies the attacking tool

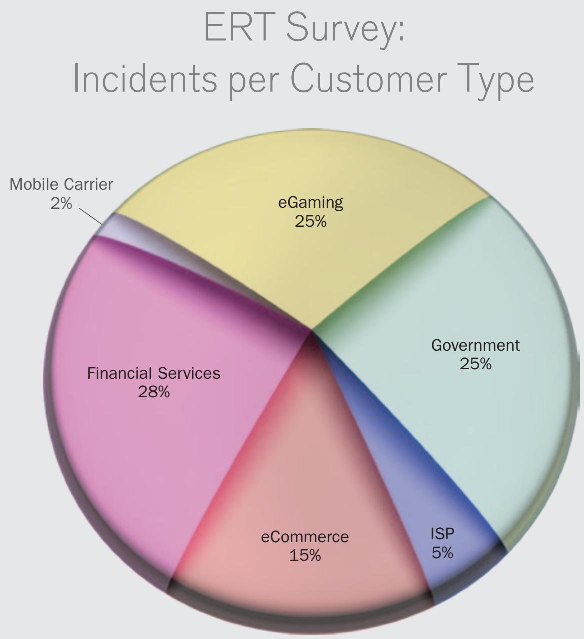


Figure 17: The cases that ERT handled last year were mostly in three areas, the financial sector, Government and e-Gaming. The financial sector was the most serious not just because of the number of attacks, but mostly because these financial sites were completely unprepared for DoS / DDoS attacks.

Victims Trends Illustration

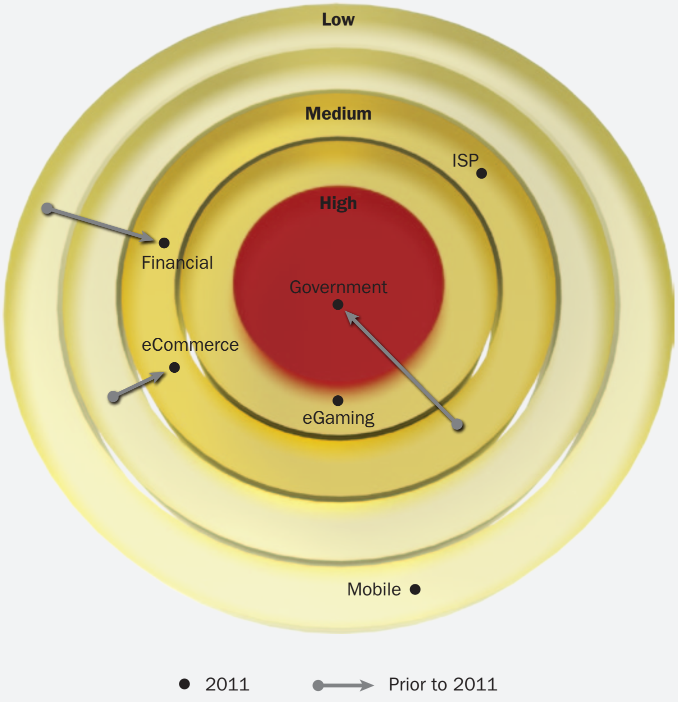


Figure 18: The government sector and the financial sector were the ones mostly affected, while the e-Gaming threat level did not change in 2011 remaining medium-high as always

Radware's ERT saw the same in the government sector; some governments were more familiar with, better prepared for and less surprised by 2011 DoS / DDoS attacks than others. For example, the United States and Israel Governments suffered from DoS / DDoS attacks prior to 2011 and were much more prepared for them than the New Zealand Government.

Figure 18, which is based on a combination of several sources, shows how the attacks against types of websites have changed over the course of the year. The arrows indicate the direction that the volume of attacks changed during 2011. The political sector is in the center - it became Anonymous' biggest target. The same trend happened to the financial sector. E-commerce showed a slight increase in hits while e-Gaming, mobile and ISP did not show significant changes.

In conclusion, 2011 saw many organizations threatened by DoS / DDoS attacks. Some were already at risk, but at a lower rate. For other types of organizations, there was a significant change. It is difficult to predict how this will change in 2012. On one hand, Anonymous made DoS / DDoS attacks very popular in 2011, but even Anonymous has exhausted the option of shutting down sites with the types of attacks that were most popular and they are currently looking for other means to pursue their agenda.

08

Attack Tool Trends

More DoS / DDoS Tools Are Becoming Available

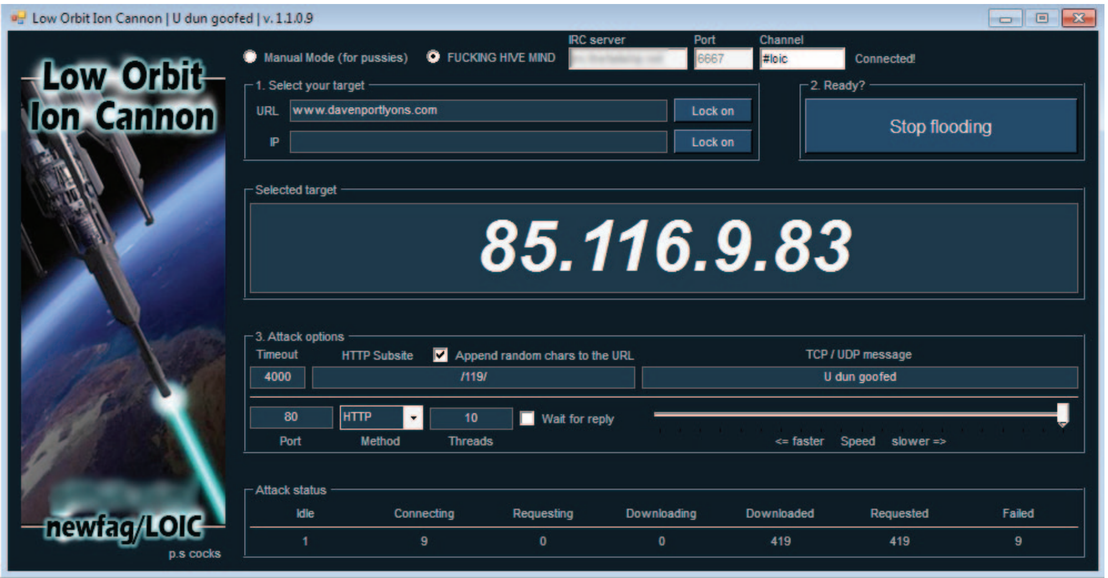
This section presents the four most prominent DoS / DDoS attack tools that were used in 2011. These tools are well known and have been well researched. This section is not intended to analyze them again. Instead, this section summarizes the main properties of each tool, examines the differences between them, and explains the concept of each tool.

The four tools described in this section are:

- LOIC
- Mobile LOIC
- R.U.D.Y.
- THC-SSL-DoS

LOIC

Low Orbit Ion Canon (LOIC) is an open source network stress testing and DoS attack application that was initially developed by Praetox Technologies and later released into the public domain.



Low Orbit Ion Cannon | U dun goofed | v. 1.1.0.9

○ Manual Mode (for pussies) ● FUCKING HIVE MIND

IRC server: [redacted] Port: 6667 Channel: #loic Connected!

1. Select your target

URL: www.davenportlyons.com

IP:

2. Ready?

Selected target: 85.116.9.83

3. Attack options

Timeout: 4000

HTTP Subsite: /119/

☑ Append random chars to the URL

TCP / UDP message: U dun goofed

Port: 80

Method: HTTP

Threads: 10

□ Wait for reply

Attack status

Idle	Connecting	Requesting	Downloading	Downloaded	Requested	Failed
1	9	0	0	419	419	9

Figure 19: LOIC GUI

LOIC is a flooding tool. A flooding tool generates a mass amount of traffic in order to utilize network or application resources, resulting in degradation and even loss of service to legitimate users. The tool runs on Microsoft Windows and Mac OS X generating massive amounts of TCP, UDP and HTTP packets. It performs denial-of-service attacks on the target site by flooding the server with non-legitimate packets in order to disrupt the service of a particular host.

On its own, one computer cannot generate enough TCP , UDP , or HTTP requests at once to overwhelm most web servers. It takes thousands of computers all pointed at a single site to make a real impact. Letting a central administrator control the process of attacking a selected target makes the process more effective. The LOIC tool gathers random computers and turns them into a network connection that sends an onslaught of fake requests towards a targeted web server.

The Internet Relay Chat (IRC) mode enables the LOIC tool to connect to an IRC channel and receive target and settings via the IRC topic message. This is referred to as the "Hive Mind" mode. The LOIC "Hive Mind" feature allows anyone with a computer to point their copy at an Internet Relay Chat server, allowing a third party like Anonymous to take control and aim every computer at a single victim. This effectively lets anyone with a computer participate in an Anonymous attack. They don't have to be especially computer literate or skilled.

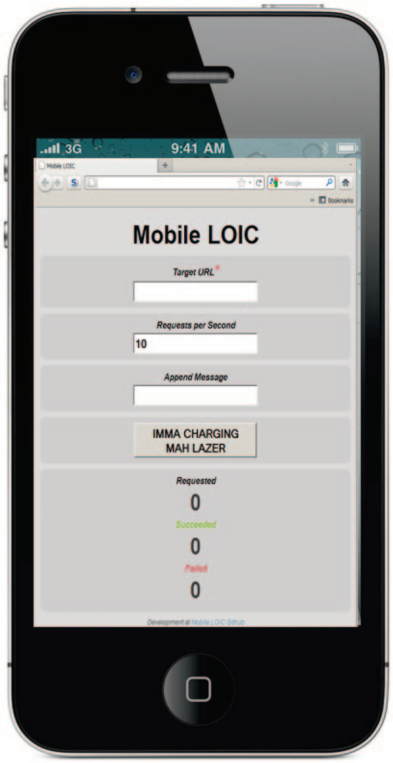
The LOIC tool has been used in several well-known attack cases against large organizations including attacks by the Anonymous group in Project Chanology, Operation Payback, and OpSony. More than 30,000 downloads of the tool were reported to have occurred between the 8th and 10th of December 2010 when Anonymous organized attacks on the websites of companies and organizations that opposed Wikileaks. LOIC was utilized by many attackers, and caused outage to many of them.

The tool does not spoof the IP but uses the real one, which can reveal the identities of the attackers. Overall, both the attack traffic and the hundreds of volunteers running the software on their PCs were not terribly sophisticated. Most volunteers clearly did not realize the tools do not anonymize their PC source or IP address. In actuality, a large part of the DoS / DDoS threat came more from the inner circle of Anonymous, who are increasingly skilled hackers than the volunteer activists.

If an attack is not routed through an anonymization network, such as Tor, traceable IP address records can be logged by its recipient. This information can be used to identify the individual user participating in DoS / DDoS attacks from logs kept by their ISPs.

Several countries including the United States have taken legal actions against attackers based on the IP information. On January 27, 2011, five people were arrested in the UK in connection with the Operation Payback attacks, while in June 2011 a further three LOIC users were arrested in Spain for their involvement in the web attacks. On June 14 2011, it was reported that Turkish police arrested 32 individuals who allegedly attacked government websites in protest against the introduction of state level web filtering. These individuals are thought to be members of Anonymous that used the LOIC tool in their protest. This eventually caused the tool's popularity to decrease towards the end of 2011.

Mobile LOIC


Mobile LOIC

Target URL*

Requests per Second: 10

Append Message

Requested: 0

Succeeded: 0

Failed: 0

Figure 20: Mobile LOIC

Mobile LOIC is the online web version of LOIC. It is a Java script-based HTTP DoS tool that is delivered within an HTML page, consisting of a simple 100 lines of code that executes-loop generating web requests. It has very few options and can only conduct HTTP floods. It is possible to append text with an appropriately revolutionary message. Unlike its PC counterpart LOIC, it does not support more complex options, including randomization of URLs and remote control by IRC botnets ("the Hive"). This tool is flexible because it can run on various browsers and accessed remotely. Normally attack organizers post a URL for the website hosting the page and invite others to use the tool to attack the specified target. The HTML page may be hosted on a website and as only a web browser is required, an attacker can even use a smart phone to generate an attack.

LOIC Highlights

- Anonymous primary attack tool during 2011
- Enables laymen to effectively participate in DoS / DDoS attacks
- Creates a "HiveMind" mode that enables a single entity to point all participants at a single target via an IRC channel
- Anonymous solicits participants via social networks, Facebook, Twitter, RSS, to use the tool
- Dangerous because the tool is not really anonymous as it can reveal the real IP of participants leaving them open to arrest and prosecution

Related Links

- LOIC - Wikipedia
- Low Orbit Ion Canon – Counter Measures - Yotam Ben-Ezra

Mobile LOIC Highlights

- The mobile version of LOIC only needs a web browser, requires no installation, and can run on smart phones and tablets
- Only supports HTTP floods, not UDP and TCP floods
- Makes the request identical to a legitimate request in many aspects by using the host browser
- Like LOIC, it also uses the host's true IP
- Passes basic web challenges, but has a constant part in the URL that can be used to detect it

Related Links

- Mobile LOIC – Counter Measures - Yotam Ben-Ezra

Mobile LOIC is very simple to operate since it needs only three configurable parameters, which are:

- **Target URL** - specifies the URL of the attacked target. Must start with http://
- **Requests per second** - specifies the number of desired requests to be sent per second
- **Append message** - specifies the content for the message parameter to be sent within the URL of HTTP requests

Detecting the Tool

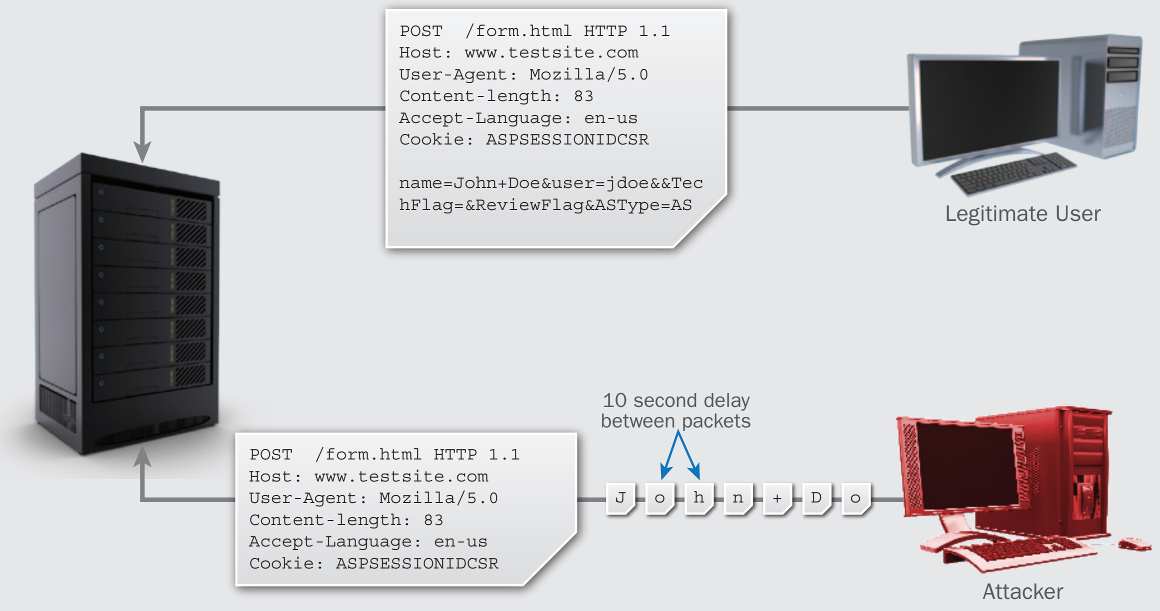
Like LOIC, this tool uses the real IP of the attacker exposing the user's identity so it is considered unsafe. Furthermore, each HTTP request sent contains the ID parameter. This parameter's value depends on time, but it is its first few bytes that will remain constant in the next few years. This value may be used to distinctly detect and mitigate the attacking traffic.

The tool however is better than most other tools, including LOIC, in passing HTTP web challenges such as redirect or cookies (Web challenges are further explained in the Mitigation section). Mobile LOIC however utilizes the HTTP implementation of the browser it is accessed from, for example, the HTTP headers in the requests are determined by the browser's configuration. Other attack tools implement their own HTTP layer and commonly fail to pass a challenge. This simple approach makes the Mobile LOIC difficult to distinguish from legitimate users because it arrives from a real browser.

R.U.D.Y. (R-U-Dead-Yet)

Over the last few years, slow rates attacks have gained attention. Tools such as Slowloris and SOCKSTRESS have been able to exploit design weakness, and with a surprisingly low rate flood can cause DoS. Unlike Slowloris attacks that can only target Apache and Apache based web servers, R.U.D.Y. can attack any website.

R.U.D.Y. was named after the Children of Bodom album - "Are You Dead Yet?" It implements a new technique to attack websites known as a slow HTTP POST request (published in Nov 2010). It runs with an interactive console menu, automatically detecting forms within



```
POST  /form.html HTTP 1.1
Host: www.testsite.com
User-Agent: Mozilla/5.0
Content-length: 83
Accept-Language: en-us
Cookie: ASPSESSIONIDCSR

name=John+Doe&user=jdoe&&Tec
hFlag=&ReviewFlag&ASType=AS
```

```
POST  /form.html HTTP 1.1
Host: www.testsite.com
User-Agent: Mozilla/5.0
Content-length: 83
Accept-Language: en-us
Cookie: ASPSESSIONIDCSR
```

Figure 21: R.U.D.Y. Diagram

a given URL, and allowing the user to choose which forms and form fields are desirable to use for the POST attack.

The tool sends the HTTP POST request, but instead of sending the entire request in single packet, it sends the data part byte-by-byte. Each byte is sent in its own packet at intervals of 10 seconds in order to exhaust the server's resources. Waiting for HTTP headers to complete sending is a basic and inherent behavior of web servers. Servers must "obey" the rules of the "content–length" field and wait for the complete message body to be sent. This behavior allows web servers to support users with slow or intermittent connections. The server keeps the connection open, which allows the attacker to open numerous connections in parallel until the connection limitation is reached on the web server and DoS happens. Any website that has forms, i.e. accepts HTTP POST requests, is susceptible to such attacks.

The tool is very efficient because it takes fewer connections to reach the server's resource limits making it highly lethal, and this is why it deserves the name of a slow rate attack. It can deny service regardless of the hardware capabilities of the host. However, since the attacks are accomplished by sending one one-byte-of-data packets, it can be detected as abnormal traffic.

R.U.D.Y. Highlights

- Exploits a design weakness that became public in Nov 2010
- A slow rate attack tool that can cause DoS with a relatively low amount of traffic generated
- Instead of sending the entire HTTP Post request at once, it sends one byte every 10 seconds making the connection last forever. It does it in parallel again and again over numerous connections until the server's resources are exhausted.

Related Links

- H.....t.....t....p....p....o....s....t - Wong Onn Chee & Tom Brennan

THC-SSL-DoS Highlights

- Attacks the SSL layer directly
- An asymmetric attack – attack makes the server invest 15 times more resources
- The attacker uses the 'SSL-Renegotiation' option to force the heavy recalculation again-and-again for the same connection

  Alternatively it is also possible merely to open brand new connections

Related Links

- THC-SSL-DOS official site
- The Hacker's Choice - Wikipedia

Asymmetric Attacks

A DoS / DDoS attack is considered to be an asymmetric attack if the attacker is able to invest a relatively small amount of resources, but forces the victim to expend a disproportionate amount of resources. The resources that the victim must use can be either memory, CPU labor or bandwidth. These attacks are also referred to as Amplification Attacks.

THC-SSL-DoS
This tool allows a single computer to knock web servers offline by targeting a well-known weakness in secure sockets layer implementations. All it takes is one computer with a simple Internet connection to use this tool to successfully attack. This is possible because the attack is asymmetric, i.e., the single client request can cause the server to invest up to 15 times more resources.

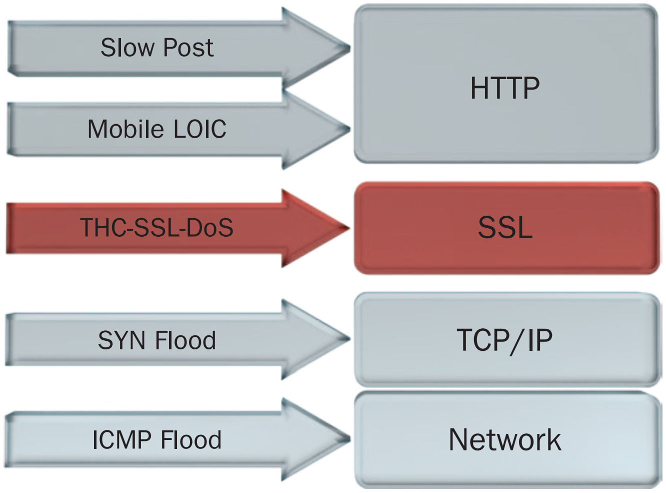


Figure 22: THC-SSL-DOS - This tool uniquely targets the SSL layer

SSL is generally used to prevent sensitive data from being monitored while the data travels between servers or between servers and end-users. This is done by establishing a secure channel in a process called the SSL handshake. This CPU consuming SSL-handshake is only done once, and servers are not prepared to handle large numbers of them. The protocol, however, has a 'Renegotiation' option that is used to establish a new secret key.

The THC-SSL-DoS tool attacks the server by creating a situation known as SSL exhaustion, in which it renegotiates the keys again and again. Here is where the attack is asymmetric – the renegotiation requires the server to invest 15 times more effort from the CPU than from the attacker. Even if the server does not support the 'Renegotiation' option, the attacker can alternatively open fresh SSL connections to cause the same affect.

The attack, however, can be detected when it is noticed that there are too many SSL handshakes in a short period of time.

Attack Types	Description	Abused Resource Type
DNS Amplification	A DNS Request is natively smaller than the DNS Reply. By carefully selecting the QName with a long answer, or even by controlling the DNS result, the attacker can reach up to a factor of 80.	Bandwidth
DNS Recursive Attack	DNS recursive request, which is simple to generate, causes the DNS server to query other DNS services, generate a new request, wait for the answer, and answer the client back.	Multiple
SNMP Amplification	SNMP Get-Bulk request that causes the server to send a large data reply. SNMP Attack is a known tool for that.	Bandwidth

09

Mitigation Techniques

Overview

There will always be Internet sites that can be compromised by DoS / DDoS attacks, therefore it is important to manage risks. Network security must identify, analyze and mitigate the attack as quickly as possible. The first step when an attack is detected is to identify, characterize and quantify the attack. The sooner an attack can be identified and mitigated, the better.

The standard protection devices for most Internet sites, which have been deployed for years, include routers, firewalls, and IPS and dedicated DoS / DDoS mitigation systems. These are familiar tools. In addition, the Multi-Router Traffic Grapher (MRTG) monitors and measures the traffic load on networks.

This section discusses the actual technologies used to mitigate DoS / DDoS attacks. It combines input from the Radware Security Survey, first-hand ERT experience and general discussions with organizations.

Mitigation Technologies

Enlarging Service/Network Capacity

When under a brute force attack, an organization can increase its traffic capacity proportionally by approaching a Content Distribution Network (CDN) to host its site during the attack. The CDN has the capacity to successfully overcome the attack by increasing access bandwidth and redundancy, which improves access to data and reduces access latency. This is a simple working solution. It is not sophisticated, but has a price, literally. Another problem is with dynamic pages – they are not stored by the CDN and if they are attacked, this solution does not help. This solution is being used more frequently due to the virtualization and cloud based services trend.

Another solution is to increase the capacity of a web server by adding more boxes in-house. While this does not scale for most organizations, it is recommended for sites that have a very weak web server as another layer of defense. Many government sites, for example, are running on very weak servers – for example servers that cannot handle 1000 HTTP requests per second – since their legitimate user rate is low. When such a site is attacked, even if the protection mechanism is doing its job, the percentage that is not mitigated can still cause outage or poor service.

Rate Limit and Bandwidth Management

This technology allows only a certain amount of traffic to reach its destination while other traffic is dropped. For example, an organization can allow only 10K request/second to reach the DNS server. This keeps the service alive and supports predictable behavior. More sophisticated rate limitations include actions such as per IP or per connection.

Rate limit is an important technique since it confines the impact of the attack and makes it predictable, but it can also drop legitimate traffic, actually causing a DoS condition. The more sophisticated rate limits continues to be an effective method since they confine the attack in a very predictable manner. Rate limit is often used for the “first reaction”; it quickly helps confine the attack and at least partially restore service. When this is achieved rate limit often makes room for other more surgical technologies.

Behavioral-Based Protection

This technology analyzes traffic during the attack. It blocks the attack by finding common patterns that can be used to create a real-time footprint. The idea is that nearly every attack has some kind of unique footprint pattern that can be used to block it.

However, attempting to identify a unique real-time footprint is not a predictable process. In some cases the footprint is accurate and blocks only the attack. In other cases the footprint is either too wide or too narrow, causing a false positive or false negative. Under a DoS / DDoS attack limited false positive or false negative is acceptable, but this causes customers to also favor challenge based technologies. Nevertheless, attackers can make an extra effort and pass the challenge, and then again the behavioral protection is the only active mitigation technology to rely upon, and for this reason plays an important role in the defender’s overall strategy. One way to benefit both worlds is to combine behavioral and challenged based technologies. The attack is first being characterized by the behavioral technology, a footprint is created to classify it, but now instead of blocking it, it is being mitigated by the challenge based technology. This way the intervention to network is kept minimal.

Challenges

This technology redirects the attack. During the attack, for example, the mitigation technique sends HTTP 302 REDIRECT to the same page. While legitimate users with normal browsers respond favorably to this challenge, the attacker script does not handle this challenge well. There are other types of challenges in HTTP, DNS and TCP. This technology is predictable and effective against the majority of the attacks. However, determined attackers can modify their attack tools to pass the challenge (false negative). In addition, it can also block legitimate clients, browsers and scripts, that don't pass the challenge (false positive). More solutions are now offering this type of challenge in their security portfolio as challenges are considered a very clean technology in the sense that even its inherent blockage of legitimate clients is well predicted and usually acceptable when under DoS / DDoS attack.

Stateful Inspection

This technology can block many flood attacks if they do not comply with the protocol state. For example, a FIN+ACK flood will be blocked since no SYN packet was sent before. This technology is predictable and very effective against certain types of attacks. Of course it will not block attacks that comply with the protocol states, and relative to other protections it is a resource consuming technology problematic for massive floods.

Geographical-Based Protection

This technique identifies the attacker's geographical locations (countries) and blocks these regions. In most cases this is done manually. It is predictable and effective in confining attacks, and is also one of the "first reaction" responses. However, it also blocks legitimate users from these regions and is not effective if the attack is too dispersed. It is much less effective for global organizations.

To give an example, in one particular ERT case, the customer under attack blocked users from all countries except their own. This successfully restored their services to a reasonable business level, but their management would not allow them to use this protection for more than two days. The customer needed to understand their next options.

ACL and RTBH

ACL also known simply as blacklisting relies on manual detection of the attack's SRC IP or network and blocks it. Remotely-Triggered Black Hole (RTBH) is a type of ACL conducted in routers. Manual detection means that a security expert or network engineer has to find the attacking IPs and then blacklist them. The procedure itself is simple, predictable and can be effective. However, it is not sufficient against distributed floods and attacks that blend well with legitimate traffic. It is always a per-attack solution. ERT's experience is that manual blacklisting is never sufficient by itself, but can be one of several layers of protection.

Signatures (Including Flowspec)

Once an attack is understood, it is possible to create signatures (aka footprints), that tell which traffic is malicious and should be dropped. Most signatures can be located natively in DoS / DDoS mitigation systems, IPS, FW and Routers (Flowspec). Signatures against DoS / DDoS attacks can be provided in advance as a service (most commonly in IPS products), or can be composed in real-time during the attack typically by security experts. For example, in the previous chapter it was shown how Mobile LOIC can be detected by a signature (a constant pattern in its HTTP request).

The main disadvantage is that during an attack campaign the attack vectors and patterns can constantly change and evade the signature. Nevertheless, they can play a role in blocking some of the attacks, making it easier to block the remaining ones with other technologies.

The Most Common DoS / DDoS Mitigation Technologies

Description	Advantages	Disadvantages
Enlarging Network Capacity	Simple	High Cost
Rate Limit	Predictable and service stays live	Drops legitimate traffic
Behavior-Based	Nearly every attack has some kind of footprint and therefore can be detected	Not predictable, footprint may be inaccurate especially when attack is similar to legitimate traffic
Challenges	Predictable and effective against the majority of challenges	Sophisticated attacks can overcome this challenge
Stateful Inspection	Blocks flood attacks	Consumes resources
ACL (Geographical-based Protection)	Predictable and effective in blocking from a specific area	Block legitimate users
ACL (Other) and RTBH	Predictable and simple	Not effective against massive floods
Flowspec	Blocks attacks by creating signatures or footprints	Need to identify the attack pattern
Bandwidth Management Technology	Predictable and can confine attacks	Drops legitimate traffic and not effective against more sophisticated attacks

Technology Efficiency

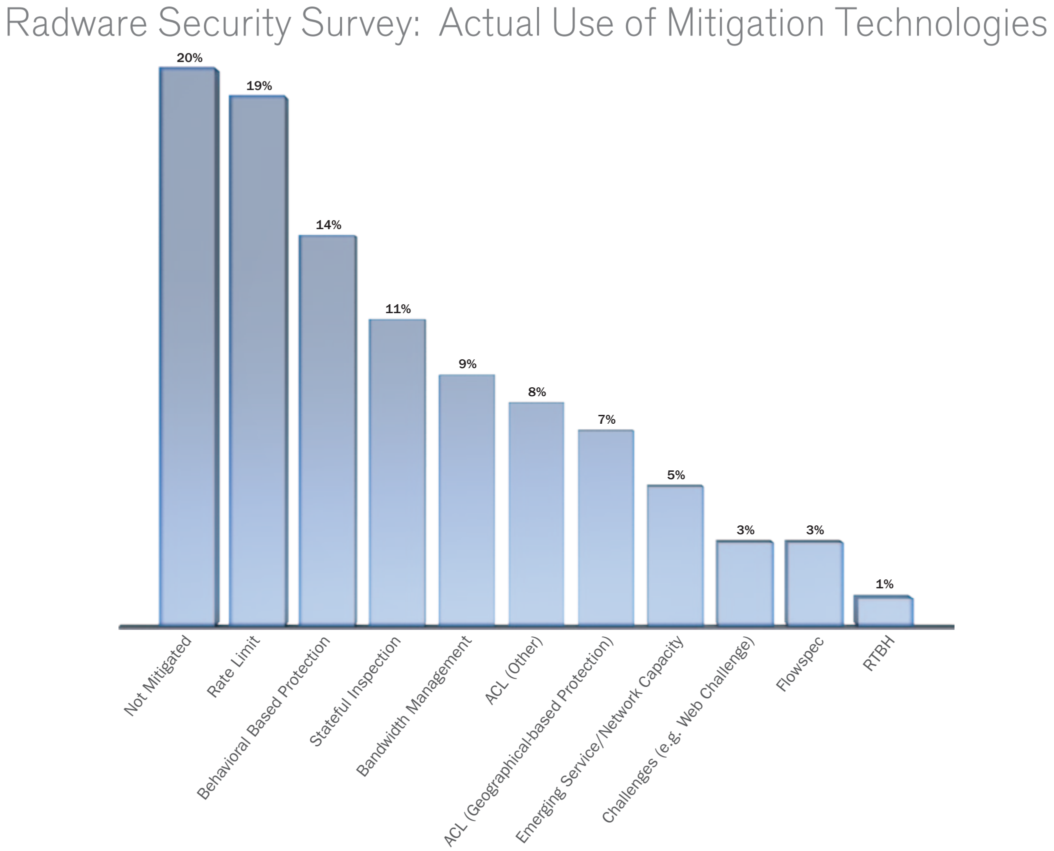


Figure 23: There is no one technology to block DoS / DDoS attacks. What is needed is a cocktail of techniques that together manage to be fully protected.

Figure 23 shows the actual usage of various technologies as reported in the Radware Security Survey. The respondents were requested to state up to three top attacks they experienced and then to state if they were blocked or not, and if so by which technology. The actual usage of protection is clearly the combination of the efficiency of the technology with its availability. This is the reason that the older Rate Limit, Behavioral, and Stateful Inspection technologies are more common than for example the more modern challenge technology.

There is, however, one thing that is evident. There is no “silver bullet”; the solution must be comprised of several different technologies to stop the DoS / DDoS attack, which is the main reason so many different mitigation technologies exist and are needed.

- **Different customers have different needs**
  For example, web challenges are a very effective solution against HTTP floods and currently stop most HTTP floods. While one customer might embrace and praise this solution, another customer would never use it since it also blocks legitimate scripts and other applications common in their environment.
- **Each technology has limited scope**
  Each technology is relevant only to a sub-set of the DoS / DDoS attack so each one represents only a partial solution. For example, SYN Cookies, a L4 challenge-based technique, is an excellent technology, but it is only relevant to SYN floods.
- **Asymmetric networks**
  Asymmetric networks may rule out some technologies as there is no guarantee the device will see all traffic. Challenged-based and state-based technologies require inspecting 2 types of packets, and if there is no such guarantee, the technology fails. However, for certain types of asymmetric networks, specifically Ingress, both technologies can be adopted.

10

DoS / DDoS is War

DoS / DDoS attacks are not much different than combat battles in a traditional war so security personnel tend to use the same language to describe both the attacks and the responses. We talk about attacks, counter attacks, defensive measures, intelligence gathering as if it were a ground battle and not a virtual one. War terminology may have bad connotations, but it is appropriate language to describe the situation.

The attacker has a target that is very visible. The attack is a bombardment that causes the victim serious damage and attacks can take an hour or several days. During this period, both sides are busy maneuvering and changing tactics. The more complicated the attacks become, as they did in 2011, the closer the virtual attacks resemble the real world. Just as battles cause damage in land, so do virtual battles to the Internet.

Counter Attacks

Traditionally, DoS / DDoS attacks have been mitigated by blocking the malicious packets. However, it may be possible that there are additional ways to stop DoS / DDoS attacks. Lately, it has become more obvious that defense alone is not the most feasible strategy as the attacker always has the edge. Some type of offensive action is required to protect the site. Offensive moves against the attackers are known as counter attacks. Often when talking about DoS / DDoS attacks, the terminology hints at warfare, making it logical to think in these terms. When being attacked it should be possible to launch a counter attack. However, this raises a number of issues. Since this is essentially an asymmetric war, which is to say that the defender is a law-abiding organization while the attacker is not, the very idea of a respectable organization conducting a possibly illegal operation even if it is aimed at an illegal entity naturally raises legal and ethical issues.

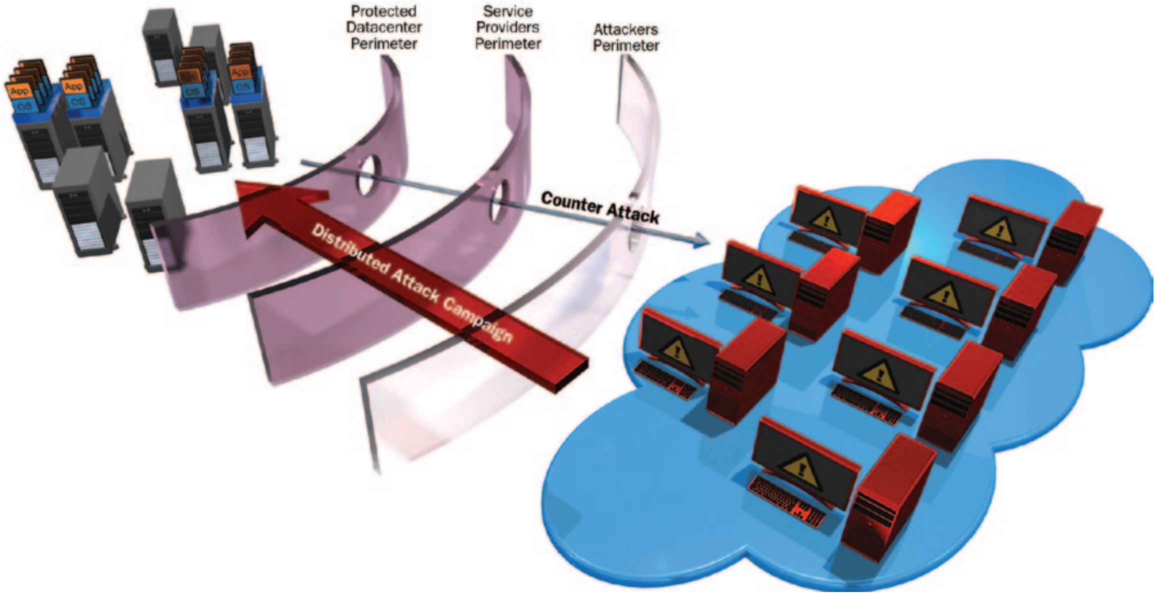

Protected Datacenter Perimeter
Service Providers Perimeter
Attackers Perimeter
Counter Attack
Distributed Attack Campaign
App
OS

Figure 24: Counter Attack

In order to be clear, the term counter attack should be well-defined. A counter-attack, in our definition, is any action that impacts the ability of the attacker to launch a successful attack. In the case of a DoS / DDoS attack, a counter-attack is anything that impacts the effectiveness of the attack volume, in percentage, and ideally totally (100%) cripples the attack volume.

There are many ways to counter attack with the primary one being turning the tables on the attacker and hacking into their computer network to stop their interference. The legality of this activity is questionable. Another method to take the offensive is to request the attacker's own ISP to block them. While this action is legal, it takes time and the war may already be over.

Security systems such as firewalls and IPSs can send different responses when a threat is detected. For example, detected DoS attack packets can be silently dropped for not generating more traffic than already generated by the attack. In other cases, the connection is reset when a TCP RST packet is sent to the attack, which closes the attacking connection. In either case the attacker's IP can be temporarily or permanently blacklisted.

What is really intriguing is that DoS attack tools respond differently when such basic actions are sent back to them. By carefully researching each attack tool, it is possible to find the most effective response to slow or stop it.

As can be seen in the graph below, even after the attack was detected, the attacker continued to send traffic. The silent drop mitigation only partially stopped it.

However, in the image 'Counter Attack - Drop and RST', it can be seen that the attacking traffic is reduced.

Security researchers investigating counter attacks can search for more exotic actions that the mitigation system can use on the attacker. One known TCP reply that can impact the other side is sending a packet and advertising a Window Size equals 0. This sends a message to the sending party that there is no more room for new information. Legitimate clients generally respect this and will suspend their communication for the time being. It seems that some attackers also honor this message and suspend the attack until a new, larger window size is advertised, which of course the site being attacked has no intention of doing. For certain attack tools, this mitigation strategy is even more effective than the others and far more effective than the silent drop. According to Figure 27, this strategy is even more effective than the others and by far more effective than the Silent Drop.

In conclusion, it may not be enough to defend and absorb a DoS / DDoS attack. The ability to fight back and launch counter attacks to stop malicious traffic or site degradation adds another dimension to the cat and mouse game, leveling the playing field. This ability is crucial as attacks become stronger and more sophisticated.

More information

- Security's Not Just About Defense - Avi Chesla
- Security? Defense, Offense, Both? - Carl Herberger
- Mobile LOIC – Counter Measures - Yotam Ben-Ezra
- Low Orbit Ion Canon – Counter Measures - Yotam Ben-Ezra

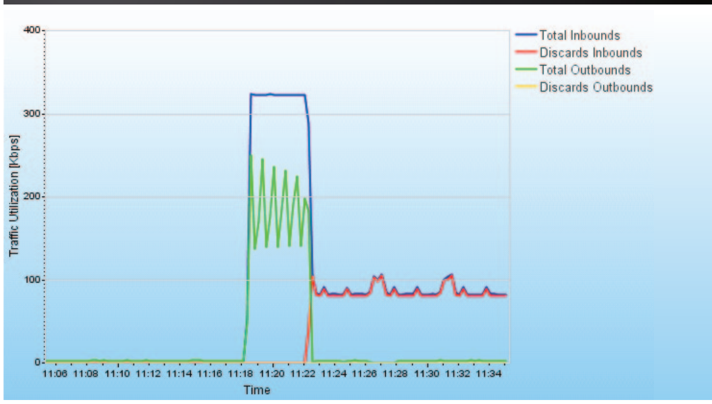


Figure 25: Counter Attack – Silent Drop against LOIC
The silent drop action only partially stops the LOIC tool

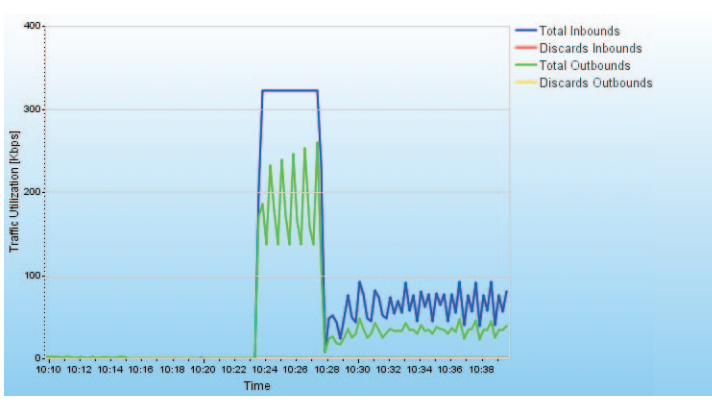


Figure 26: Drop and RST against LOIC
The RST action stops the LOIC tool better

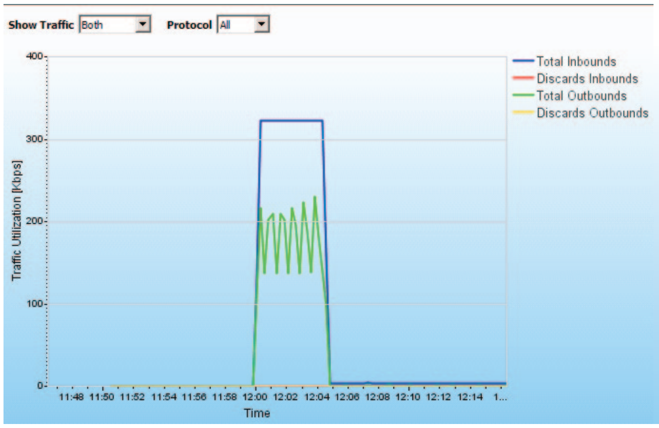

Show Traffic Both Protocol All

Figure 27: Counter Attack - Window Size Zero against LOIC
This action completely paralyzes LOIC

Counter Attack Significance

- Remove the inherent advantage that offensive forces usually have over defense forces
- Exhaust the attackers' resources, physically and mentally, wherever they are – to make him abandon the attack earlier than planned
- Clean the attack traffic end to end, breaching all network perimeters borders – virtually extending the network perimeter of defense up to the attacker origin

radware

11

Summary

Recommendations for the Network and Security Community

This report presents the security landscape of 2011. It describes and explains findings based on the two surveys conducted by Radware's ERT. In this summary section, Radware's ERT provides opinions and makes recommendations based on the content of this report.

DoS / DDoS Attacks Expected to Continue in 2012

In general, 2011 proved to be the year that attacks became more complicated with DoS / DDoS attacks becoming main stream. The unanswered question is whether this trend reached a plateau or will continue and grow in 2012. There was some decrease toward the end of 2011, but not enough to make Radware's ERT think that they are going to disappear. The increase in popularity of DoS / DDoS attacks during 2011 has taken them out of their niche and put them in the mainstream. DoS / DDoS attacks will not return to being a niche sector in security.

- For further details see Hacktivism and the Rise of Anonymous

APT is becoming more prominent and uses DoS / DDoS attacks as one of its tools. In politically oriented cybercrime attacks in Estonia, Georgia and South Korea, DoS / DDoS attacks took a major role in the attacks.

- For further information see DoS Attack Nature becomes APT Oriented

Be Prepared for DoS / DDoS Attacks

Although DoS / DDoS attacks are not necessarily massive; a mitigation solution is still critical. Many systems are not secure. Radware's ERT witnessed many organizations did not have any DoS / DDoS solution in place. In order to be protected against a DoS / DDoS attack, you must make a decision to do so.

- For further information see Attack Size Varies Dramatically

Do Not Consider a Complimentary DoS / DDoS Protection as a DoS / DDoS Mitigation Solution

It is not enough to have only a DoS / DDoS mitigation feature. This does not comprise a true DoS / DDoS mitigation solution. Here is a brief Radware ERT case study that demonstrates this. In 2011 the organization was caught off-guard and surprised by a DoS / DDoS attack. It was evident that the attacker was persistent and kept changing the attack vectors to prolong the attack. The situation was critical and the organization summoned all of its relevant security contractors, including the firewall and IPS providers, and challenged them "which one can stop the attack?" The organization was not even aware that firewalls are not a DoS / DDoS mitigation solution nor is IPS per se, and had the wrong expectations of the tools in place. This false sense of security was because the security tools they had in place had some kind of DoS / DDoS mitigation features, but they were far from comprising a DoS / DDoS solution. For example, many firewalls have a SYN flood protection technology, but the same firewall cannot handle an HTTP flood. Radware's ERT is very often called in to protect a security product that was the first to fail when attacked by DoS / DDoS.

- For further details see The Internet Server Is Not Necessarily the First to Fall

Well Position your DoS / DDoS Mitigation Solution

A full DoS / DDoS mitigation solution is necessary in order to protect all the different network entities that are vulnerable to DoS / DDoS attacks. The DoS / DDoS mitigation solution has to be located before most of the network elements in the path. A typical installation would place it before the firewall so it could protect the firewall, load balancers, Internet service, and other internal servers. It is not necessary to protect the router as they are most generally capable of passing the flood onward.

However, any solution deployed within the organization's perimeter does not protect the Internet pipe from saturating. In this case it is important make sure that the ISP can solve massive network attacks and keep the pipe clean. This can be achieved by relying on the ISP's own DoS / DDoS mitigation technology, or by the ability to increase the pipe bandwidth quickly when needed.

- For further information see the case study under 'The Internet Server is not Necessarily the First to Fall'

Ensure Your DoS / DDoS Mitigation Solution Encompasses Multiple Technologies

The DoS / DDoS mitigation solution must also encompass multiple technologies to combat the combinations of attack vectors. Each technology has a limited scope and is designed to fight one type of attack. For example, web challenges work best against HTTP floods, SYN cookies fight SYN floods and Signatures fight slow rate attacks. To be protected against all the attack vectors the mitigation solution must be a cocktail of different protections.

- For further information see DoS / DDoS Attack Nature Becomes More APT Oriented

In addition to the different attack vectors, attack size can vary dramatically. It is difficult for an organization to estimate the attack size it may experience, but it is important to do so. For example, one organization can state it wants to be protected against a a 2Gbps network flood, a 2M PPS SYN flood, and 100K transactions-per-second HTTP flood. The organization should then test the solution and verify that the DoS / DDoS mitigation solution will protect it.

- For further information see Attacks Size Varies Dramatically

Have a Consolidated or “Context Aware” View into Enterprise Security

Even with dedicated security personnel, it’s tough to monitor the millions of messages and log records generated by various security edge devices. Even more difficult is identifying patterns occurring over time and across separate devices. A Security Event Information Management (SEIM) system can build a centralized architecture that makes such tasks more feasible and allows for speedy compliance reports and audits and is absolutely required when prosecution of a perpetrator is needed.

The SEIM system was designed to be the single ‘console’ in which an operator would get both total situational and context-awareness. It can provide the security leap-frog in a world of point solutions – to ensure there are no blind spots in your network security architecture

- For further details see No Blind Spots in Perimeter Security with Security Event Information Management

Invest in Education and Develop Good Internal Security Policies

Education is still paramount as another defense tool in the arsenal. Regularly refresh technical skills and practical experience within the security group. Up-to-date insight on newer or exotic threats can reduce unwanted surprises. The adage, ‘you don’t know what you don’t know’ factors strongly in the fight to stay ahead of nefarious aims. Additional concerns also surround making seemingly sound security policy decisions – such as single sign-on practices. These appear sound on the surface, but can lead to full-scale shutdowns if not properly backed by the appropriate techniques and tools. Lastly, trending infrastructure transformations such as cloud computing definitely force the security group to reconsider traditional thinking and security models.

All of the above should be accompanied by an investment in education outside of the immediate security group. This helps minimize opening up additional doors to exploitation. Core cautions include educating that security risks aren’t relegated to spam or known software bugs:

- The dangers of downloading apps and application services, whether free or paid or ‘brand name’, to clients, tablets, and smart devices

- Responsible use in the age of ‘bring your own device’ (BYOD); everyone is part of the extended security group now and should act with the same mindset – security is no longer solely the province of a specialized group within IT

- How social media use in the workplace (e.g., Twitter, LinkedIn) can turn employees into unwitting accomplices with the simple click of web link

- Staying compliant with changes in security policies/controls/governance of sensitive data, which can and often do lead to data breaches

Credits

Authors

Ziv Gadot
SOC/ERT Team Leader,
Radware

Matan Atad
Security Researcher,
Radware

Yotam Ben-Ezra
Senior Security Researcher,
Radware

Contributors

Iko Azoulay
Director of R&D,
Radware

Eyal Felstaine
VP Security,
Radware

Yuri Gushin,
Senior Security Specialist,
Radware

Ziv Ichilov
Product Manager,
Radware

Technical Writing

Janet Sack
JMR Associates

Special Thanks

Avi Chesla
CTO,
Radware

Carolyn Muzyka
Sr. Marketing Communications Manager,
Radware

Ron Meyran
Director, Security Product Marketing,
Radware

2012 SECURITY REPORT

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.

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