radware

Global Application & Network Security Report **2013**

Table of Contents

01 Executive Summary
Most Important Findings

02 Methodology and Sources
Radware Emergency Response Team Cases
Security Industry Survey
Security Executive Survey

03 DoS/DDoS Risk Score
Increasing DoS/DDoS Risk Scores
Service Outage and Degradation

04 DoS/DDoS Ring of Fire
Industries at High Likelihood for Attacks
Industries at Medium Likelihood for Attacks
Industries at Low Likelihood for Attacks

05 Business Concerns of DoS/DDoS Attacks
Financial Impact
Budgeting for DoS/DDoS Attacks
Application Scrubbing Centers

06 DoS/DDoS Attack Vector Landscape
Application Attacks are Increasing
Multi-Vector Attacks are on the Rise
Internet Pipe, Firewall and Web Server are Primary Targets
Attackers Response Time Got Shorter

07 2013 Notable Attack Vectors
SSL-Based Attacks Continue to Threaten Organizations
Login Page Attacks are on the Rise
Account Lockdown
DNS Reflective Attacks Spread
Mechanics of a Reflective DNS Attack
Maintaining Anonymity – IP Spoofing
Attack Amplification

08 Unprecedented Severity Introduced by Operation Ababil
Timeline of Events
An Inside View - Organization Under Attack

09 Summary
DoS/DDoS Protection Best Practices
Three Important Features for DoS/DDoS Protection
Multi-Layer Approach
SSL Attack Mitigation

Global Application & Network Security Report **2013**

01 Executive Summary

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 2013 DoS/DDoS attacks from a business and technical perspective. Its purpose is to provide best-practices that organizations should implement to mitigate a family of attacks and allow organizations to win the extended and persistent DoS/DDoS battle.

What Changed in Security in 2013?

Denial of Service/Distributed Denial of Services (DoS/DDoS) attacks are a destructive cyber weapon that have become a major tool increasingly used by cyber-hacktivists groups – like Anonymous and Cyber Fighters of Izz Ad-Din Al-Qassam – over the past three years.

DoS/DDoS Risk Score Increases

In 2013 DoS/DDoS attacks became a mainstream occurrence with increasing severity. Radware's DoS/DSoS Risk Score[1] is a system that quantifies attacks based on duration, complexity and number of vectors used. It enables ranking attacks by severity, with each attack assigned a score between 1 and 10 (10 being the most powerful). Attack scores increased with **28%** of 2013 DoS/DDoS attacks getting a score of **8** and above, as compared to 8% in 2012.

Risk is Increasing for Some Industries

The 2011 and 2012 versions of this annual Global Application & Network Security Report informed that government organizations were at high risk for DoS/DDoS attacks as a result of malicious hactivist activities. In 2013, financial services joined government organizations in the DoS/DDoS Ring of Fire, which maps verticals susceptible to DoS/DDoS attacks. The risk for financial services increased dramatically in part because of hacktivists (most notably Operation Ababil attack campaign) and the use of DoS/DDoS attacks as a way to divert attention from simultaneous fraudulent activities.

---

1 The name has been changed from 2012's Advanced Persistent Threat (APT) Score to DoS/DDoS Risk Score to better describe what this index is measuring.

Service Degradation and Outage

87% of respondents to Radware's Security Industry and Security Executive Surveys stated that they experience service level issues – 60% encountered service degradation, while 27% experienced outage. While a service outage is obviously bad, we encourage you to think also about the consequences of major service degradation such as financial impact and effect on customer satisfaction.

Multi-Vector Attack Campaigns

Generally attackers continue to use multi-vector attack campaigns with more than **50%** of attack campaigns deploying **5 or more attack vectors**.

Attackers Are Quicker to Defeat New Mitigation Tools

We noticed that attackers have drastically shortened the response time, developing new attack vectors that defeat newly deployed mitigation tools— in a matter of days and sometimes even hours after the mitigation tools are deployed.

The Rise of Web-Stealth Attacks

On the technical front we saw a more frequent appearance of a set of attack vectors that we grouped as "Web Stealth" attack vectors. Web Stealth attacks are a set of DoS/DDoS attack vectors that include brute-force attacks (e.g. attacks on the login page), file upload violations, SSL encrypted application attacks and more. These attack vectors are built on HTTP packets that conform to relevant Web traffic specifications, and thus cannot be detected by standard network security tools such as IPS, firewall, and rate-limit based DoS/DDoS protection tools.

A popular Web Stealth attack vector is the use of SSL encrypted traffic. Attackers use the evasive nature of HTTPS and other SSL encrypted mechanisms as well as the asymmetric nature of these attacks to bypass network security mechanisms and attack servers deep inside the network topology. This is where they are more susceptible for resource saturation. The portion of encrypted application based attacks was **50% of all Web based attacks**.

DNS Attacks

We also saw a steady increase in the trend of DNS based attacks, to the extent that these attacks are now considered to be the **second most frequent attack vector**.

The Geo-Political Connection

Attacks during 2013 demonstrated a clear correlation between geo-political events and DoS/DDoS attacks. Many geo-political events were followed by one or a series of malicious hacktivits activities such as DoS/DDos attacks.

02 Methodology and Sources

The report draws its information from the following sources:

Radware's Emergency Response Team (ERT) 2013 Cases

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 ERT's service is to mitigate attacks and help customers recover, the team gets a unique view of each attack. Due to hands-on involvement, the ERT 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 provides a deep forensic examination of DoS/DDoS attacks that could not be achieved through just the survey.

The source for the quantitative sections of the report is a statistical analysis of over 300 cases handled by the ERT in 2013. The qualitative sections of the report are based primarily on first-hand experience of ERT members while helping customers mitigate DoS/DDoS attacks. Though the ERT assists in a variety of DoS/DDoS mitigation cases, only those cases that caused substantial outage periods were included in this report.

Security Industry Survey

The second source is from 198 individual responders to a Security Industry Survey, which was conducted by Radware. The survey was sent to a wide variety of organizations globally – the majority of which are not Radware customers – and was designed to collect objective vendor-neutral information about issues organizations faced while combating DoS/DDoS attacks.

Security Executive Survey

The qualitative date for this report was derived from a Security Executive Survey, which was conducted by Radware. We selected fifteen top security officers from an equal number of organizations and conducted in-depth interviews about their experience with availability-based threats.

03 DoS/DDoS Risk Score

DoS/DDoS Risk Scores Have Increased in 2013. Though Attack Duration Remained the Same as 2012, Complexity and Intensity of Attack Vectors Increased, Resulting in Higher Overall Scores.

To quantify the severity of attacks, Radware uses a DoS/DSoS Risk Score[2]. This scoring system enables ranking DoS/DDoS attacks methodically by severity. Each attack is assigned a risk score between 1 and 10 (10 being the most powerful), based on three factors:

- **Attack duration** – the longer the attack lasts, the higher its risk score
- **Number of attack vectors** – a higher number of detected attack vectors increases the risk score. Over the past few years, there has been a variety of attack vectors used including Web based attacks, DNS floods, SSL garbage floods, etc.
- **Attack complexity** – the more complicated the attack vectors, the higher the risk score. For example, attacks that are based on a SYN flood get 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 1 illustrates the DoS/DDoS Risk Score and the distribution between medium and high risk attacks over the years. As attacks with a low-risk score are easily mitigated by most organizations, they are not included.

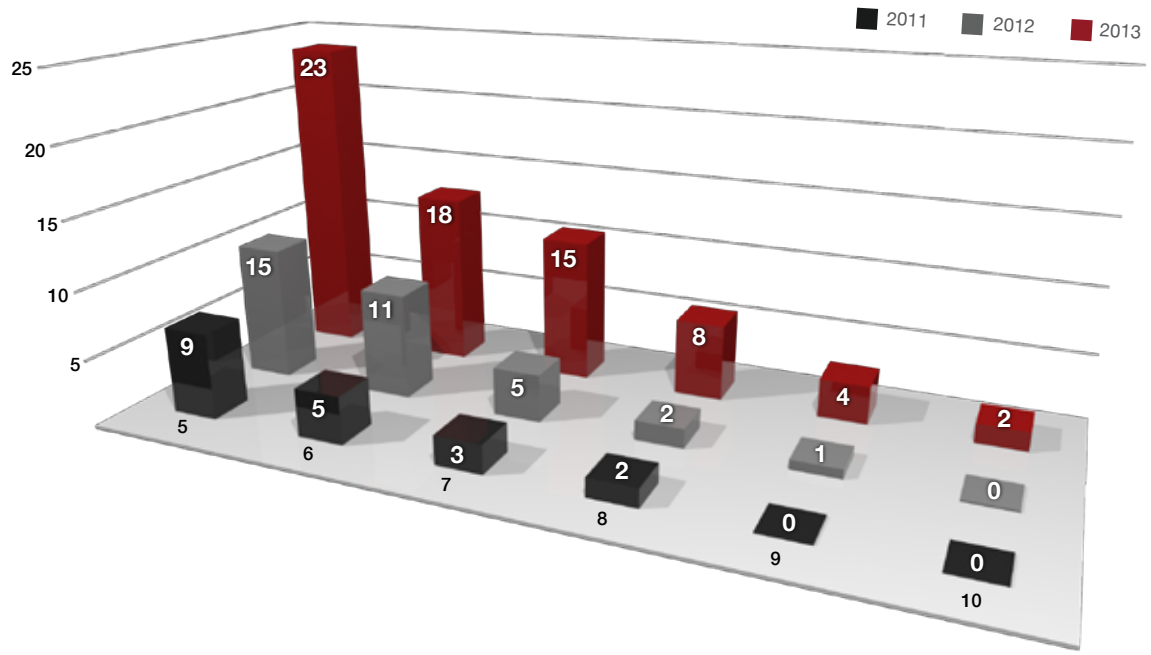


Figure 1: DoS/DDoS Risk Score distribution. Percentage of attacks based on the overall incidents tracked by ERT.

2 The name has been changed from 2012's Advanced Persistent Threat (APT) Score to DoS/DDoS Risk Score to better describe what this index is measuring.

Comparing data from 2011 and 2012, it is clear to see that 2013 attacks have higher DoS/DDoS Risk Scores. While powerful attacks appeared in 2011 and 2012, the overall intensity of the attacks and percentage of attacks with high DoS/DDoS Risk Scores have increased over the past three years. The trend is perceptible in 2013 more than ever.

When examining each risk score parameter, similar trends appear. Attacks are becoming more intense and more complex. Attack duration is the only parameter where our observations show an unchanged level (with a minor increase of two percentage points in the frequency of extremely long attacks in 2013 compared to 2012). Figure 2 shows the distribution of attacks from 2011 – 2013 based on the duration of the attack. Note that in 2013 we saw Operation Ababil as the longest attack campaign, lasting for over a year, with attack periods that lasted days in each attack wave.

Attack vector complexity is a subjective measurement that shows how sophisticated the attack vector(s) is. There is an increase of sophisticated attacks that include more application level attack vectors. Attackers are using evasive techniques and are successfully trying to stay below the detection radar of rate-limit based detection tools that are commonly used in the market today.

Figure 3 illustrates the distribution of attack vectors based on vector complexity. We see an increase with complex attacks (with complexity score of 7 – 8) while the really exotic attacks remain similar to the popularity level in 2012.

Similar to previous editions of this report, we have not included a DoS/DDoS attack traffic volume as one of the criteria that calculates the risk score. In 2013 we saw some massive attacks in terms of bandwidth, with the 300 GBPS attack on Spamhaus in March 2013, breaking the 100 GBPS ceiling of attack volume; however we still don't consider bandwidth of the attack as an important factor.

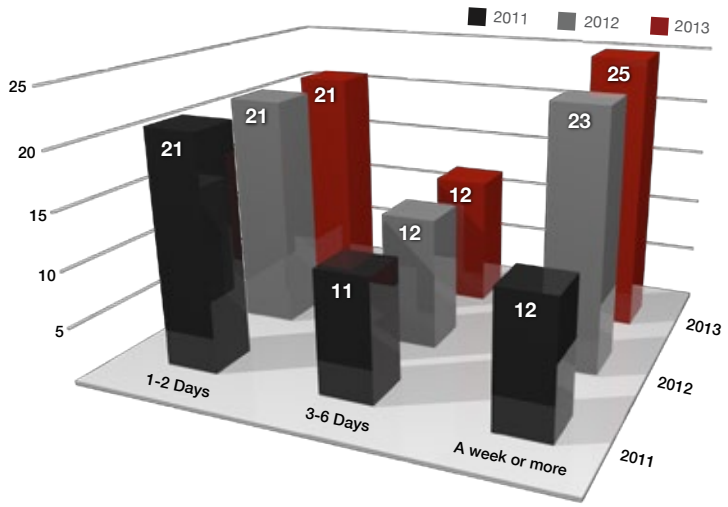


Figure 2:
Attack duration. Percentage of attacks based on the overall incidents tracked by ERT.

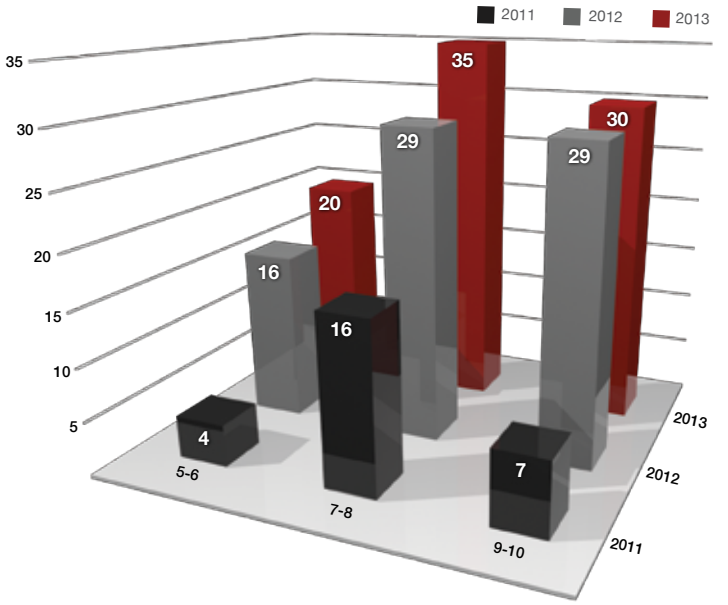


Figure 3:
Attack vector complexity. Percentage of attacks based on the overall incidents tracked by ERT.

DoS/DDoS is No Longer Only About Service Outage. 60% of Survey Respondents Say Service Level Degradation is the Bigger Issue.

Service Degradation Has a Serious Business Impact

DoS/DDoS attacks are often incorrectly associated only with service outage. Whether it is a public web site or an internal web-based application, we were taught to believe that a successful DoS/DDoS attack results in a service outage. However, the Security Industry Survey uncovered that the biggest impact of DoS/DDoS attacks in 2013 is service level degradation, which in most cases is felt as service slowness.

Figure 4 shows the effect of the most destructive DoS/DDoS attacks, according to respondents. According to recent research report, 57% of online consumers will abandon a web site after waiting 3 seconds for a page to load[3], and 88% of online consumers are less likely to return to a site after a bad experience[4]. The immediate conclusion is that slowness as the result of a DoS/DDoS attack results in immediate revenue loss.

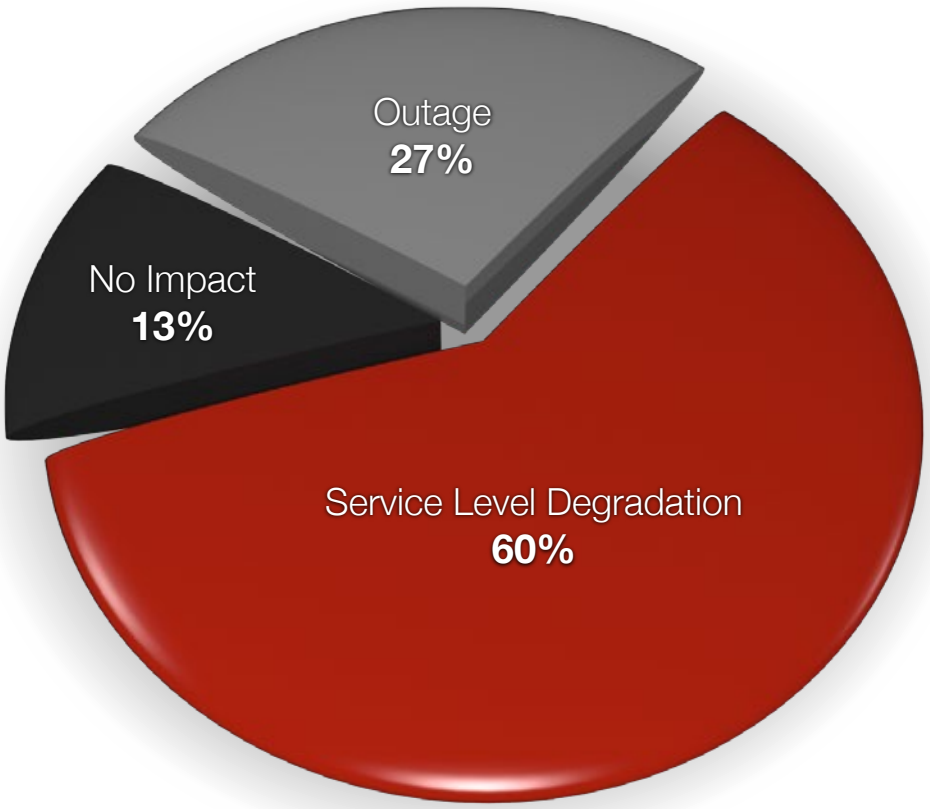


Figure 4: Impact of DoS/DDoS attack.

3 State of the Union, Ecommerce Page Speed & Web Performance, Fall 2013
4 Why Web Performance Matters: Is Your Site Driving Customers Away, Gomez

04 DoS/DDoS Ring of Fire

The DoS/DDoS Ring of Fire is a way to map verticals susceptible to DoS/DDoS attack and the likelihood that organizations in these verticals will experience attacks. It is divided into five different risk levels. As organizations closer to the red center are more likely to experience DoS/DDoS attacks, the frequency in which these attacks occur will increase.

Figure 5 illustrates the different verticals and the likelihood that they will experience a DoS/DDoS attack. The red arrows show verticals that have changed position in the current report compared to last year's report. This means that the overall numbers of DoS/DDoS attacks, as well as the frequency and intensity of these attacks has increased in 2013. And we don't have any evidence that it will decrease in any vertical moving forward.

As Companies Change Position in the DoS/DDoS Ring of Fire, They Are Susceptible to Outages, as a Security Gap is Created.

Note that as always, change brings risk. As companies change position in the DoS/DDoS Ring of Fire, experiencing higher likelihood to be the target of an attack, and as mitigation assumptions still match a previous position in the circle, the likelihood of a DoS/DDoS attack that will result in datacenter outage increases drastically. Organizations that are part of the verticals that were marked with a red arrow in Figure 5 should quickly adjust mitigation solutions and adjust them to the new risk level.

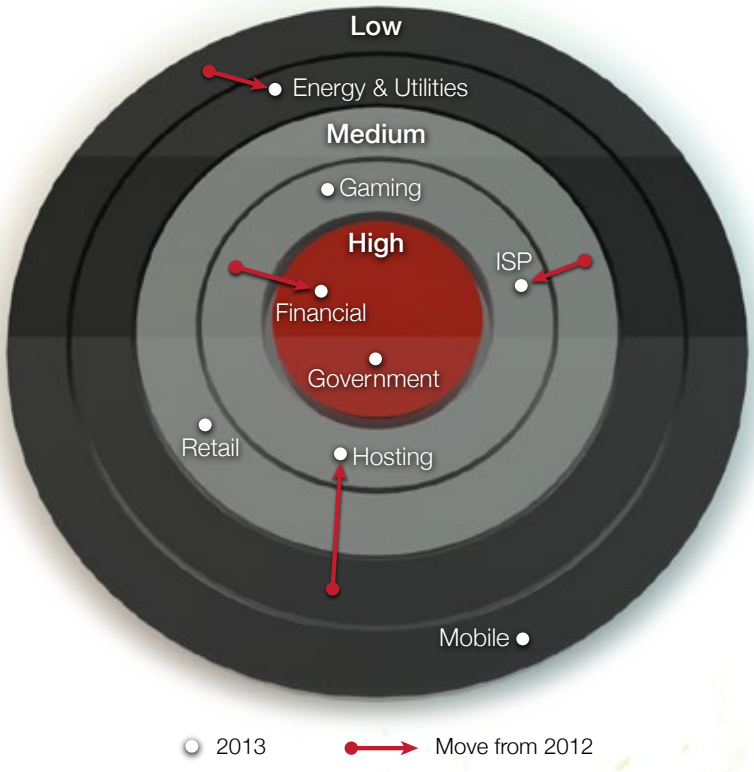


Figure 5: DoS/DDoS Ring of Fire

Government Organizations and Financial Services are Most Likely to Experience DoS/DDoS Attacks. The Risk for Hosting Companies, ISPs and Energy & Utility Companies Has Increased.

High Likelihood for Attacks

Government Agencies and Web Sites

Government agencies, and government related web sites continue to be at the highest risk for DoS/DDoS attacks. In today's geo-political environment, one can draw a clear line between geo-political events and attacks on related government agencies or web sites.

One of the most notable 2013 attacks in this vertical targeted Colombian government agencies on "The Colombian Independence Day Attack" (on July 20) which was the most successful single day cyber-attack that ever took place. The attack targeted thirty Colombian government websites. Most of these web sites were either defaced or completely shut down for the entire day of the attack, as a result of both Web and network based attacks.

A few other examples of attacks happening in this vertical included: the attacks on the North and South Korean government agencies, which happened in parallel to the North Korean Nuclear crisis in March; attacks on Egyptian government sites that happened at the time of the Egyptian military revolution in the summer; and attacks on Ukraine government agencies in parallel to the December riots.

Financial Services

Financial service organizations are very likely to experience a DoS/DDoS attack. The move from medium to high likelihood is attributed to two main triggers. First, Operation Ababil which targeted top U.S. financial institutions, was the longest cyber-attack in recent history. The attacks started September 18, 2012 and lasted throughout most of 2013. With a total of four different attack phases and numerous 'waves' within each phase, this attack campaign was one of the most successful perpetrated attacks. While Operation Ababil is officially over, we expect to see targeted hacktivist attacks against financial services continue to increase in 2014.

In addition, 2013 revealed a large number of cyber attacks targeting financial services, with DoS/DDoS attacks serving as a way to distract the IT personnel and perform fraudulent activities. During 2013 a number of financial services all over the world were attacked, generally with a combination of DoS/DDoS attacks and additional application level attacks that targeted application vulnerability, with the aim to get unauthorized access of the organization's critical infrastructure. BitCoin exchange agencies and BitCoin marketplaces had been attacked with a large number of attacks happening this past year. The attacks targeted Denmark-based BIPS.me in November and on French-based company inpots.io in October.

Medium Likelihood for Attacks

Gaming

In Radware's DoS/DDoS Risk Score we combine both massive-multiplayer online games (MMOG) and gambling sites under the gaming category. These verticals stayed unchanged in 2013, with medium likelihood for an attack. The motivation for DoS/DDoS attacks on gaming sites is similar to the motivation factors in financial services. It is a combination of cyber-crimes and fraudulent activities with a mix of hacktivism. In addition, some Security Industry Survey respondents cited unsatisfied users as the motivation for attacks on gambling or MMOG sites.

A notable attack in this category took place on June 2, 2013, as two of today's most popular online games, EVE and DUST 514 went offline for more than a day because of a DoS/DDoS attack. Both games are developed and hosted by an Icelandic company, Crowd Control Productions (CCP).

Web Hosting

A new entrant to the medium circle is the web hosting vertical, in which there was an increase in attacks. Web hosting companies suffer from dedicated attacks on their infrastructure, most notably on Domain Name Systems (DNS) servers. Over the past two years, attacks on DNS servers have been one of the most popular attack vectors, with a continued increase in its popularity in 2013. As hosting companies usually host DNS servers, they are the direct or indirect target of such attacks.

Web hosting companies are also susceptible to an outgoing DoS/DDoS attack. In 2013 we saw an increase in the number of incidents where hackers were using server-based bots for DoS/DDoS attacks. In most cases these server-based bots were activated on servers that were hosted by Web-hosting companies, causing these hosting companies to be affected by the outgoing DoS/DDoS attack traffic as well as from incoming attacks.

Internet Service Providers

The Internet Service Providers (ISP) vertical is also a new entrant to the medium circle. ISPs are usually indirect victims of nation-wide attack campaigns, as they manage the core network of the nation. In addition ISPs also experience indirect attacks that are side-effects of DNS reflective attacks, as well as direct targeted attacks on the infrastructure.

The combination of these three different attack types and the rise of national attacks and DNS related attacks have drastically increased the likelihood for ISPs to experience a DoS/DDoS attack and move it to the higher medium circle.

Retail

eRetailers kept their position in the lower tier of the medium circle. Suffering from hacktivism, unsatisfied customers, and cybercriminals looking to commit fraud, eRetailers were targeted with a number of DoS/DDoS attacks.

Low Likelihood for Attacks

Energy and Utilities

Regulators all over the world are working on new specifications to prevent DoS/DDoS attacks on critical infrastructures of energy and utility companies. The increased regulation activity has included the North American Electric Reliability Corporation (NERC), the Federal Energy Regulatory Commission (FERC) and Presidential Security Order 13636 in the United States. These regulation efforts have slightly moved the position of the energy and utilities vertical between the two lower tiers.

While hackers show an increased interest in bringing down utility company operational networks, either as a result of hacktivism or as part of a cyber-warfare, it is important to note that utility companies keep operational and data networks separated, making the operational network DoS/DDoS-attack proof. Past attacks on utility companies' public sites, and data networks as well as intrusion attempts have shown the motivation attackers have in this vertical. As the potential impact of attack on the operational network is devastating, we have moved the energy and utilities vertical slightly to a more risky environment.

Mobile Networks

While the risk of DoS/DDoS attacks on mobile networks exists[5], we believe that such attacks are of low probability based on the 2013 DoS/DDoS activities. Mobile network's operators remain at the lower likelihood of attacks.

5 Mobile Network Security - Availability Risks in Mobile Networks, Radware ERT Research Report, 2013

05 Business Concerns of DoS/DDoS Attacks

We found an interesting anecdote comparing the number of outage time organizations experience to the frequency of the attack. Figure 6 illustrates organizations experiencing weekly or even daily attacks suffer from shorter outages. On the other hand, organizations that were attacked at a much lower frequency (once or twice per year) suffer from more lengthy outages. The explanation for this anomaly is quite simple. Organizations that are being attacked frequently, such as government agencies, or financial services, allocate more resources for protection against such attacks, and thus are more prepared to defeat these attacks.

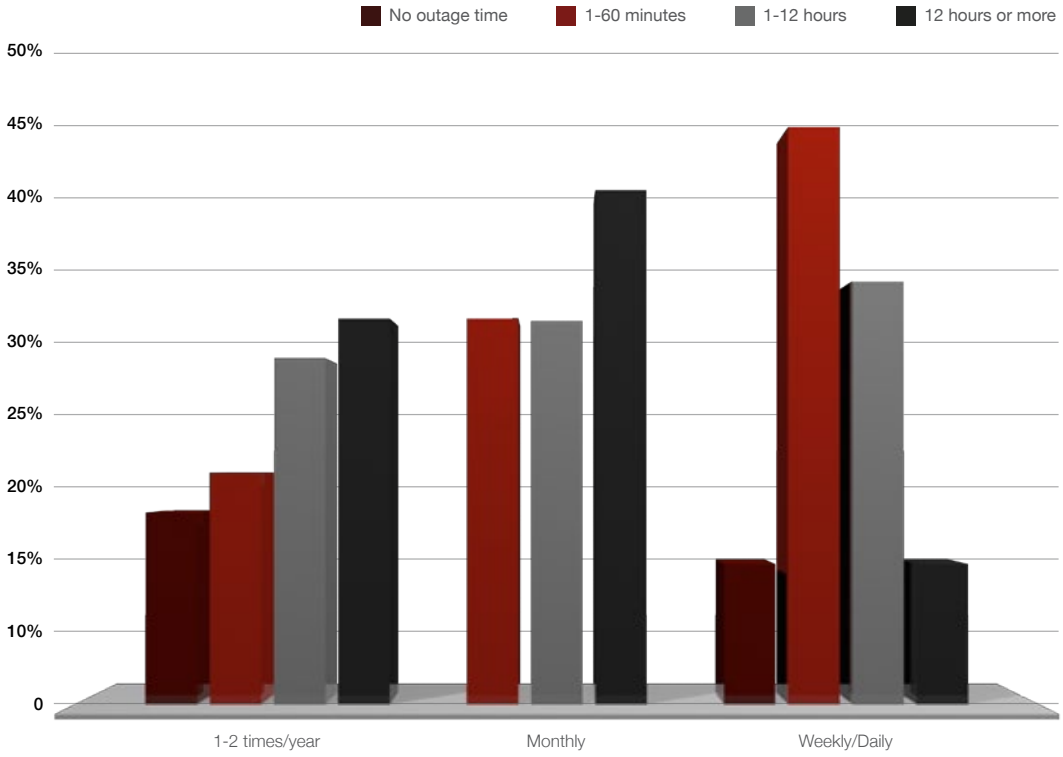


Figure 6: Outage duration as a function of attack frequency.

Financial Impact

In a research paper[6] Ponemon Institute noted that the total cost of unplanned datacenter outages caused by DoS/DDoS attack was estimated to be $822,000 in 2013 (compared to $613,000 in 2010). In our surveys we asked respondents what are the key business concerns that are related to DoS/DDoS attacks.

6 "2013 Cost of Data Center Outages", Ponemon Institute, December 2013

Following the Ponemon findings, it is not surprising that 91.9% of Security Industry Survey respondents perceive DoS/DDoS attacks as causing a negative financial impact. Figure 7 shows the business concerns that respondents mentioned when asked about DoS/DDoS attack mitigation. None of the findings in Figure 7 should come as a surprise to the readers of this report. Most of the concerns relate to direct or indirect revenue loss and direct or indirect increased expenses.

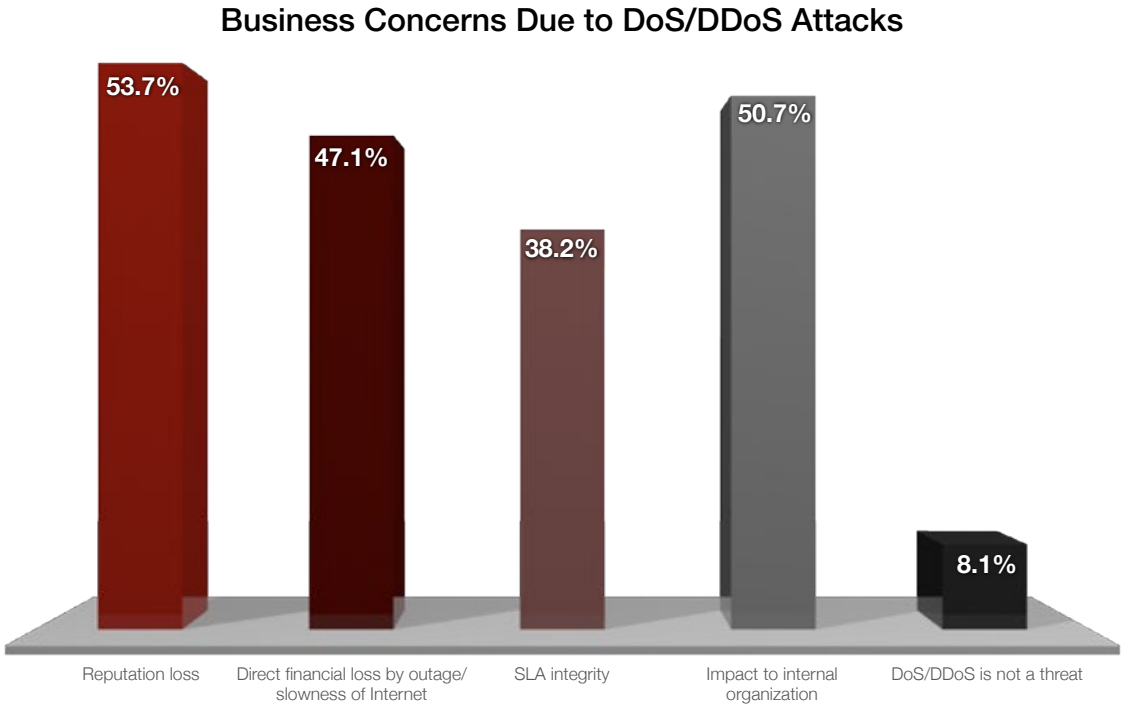


Figure7: Business concerns due to Dos/DDoS attacks.

Budgeting for DoS/DDoS Attacks

Figure 7 showed us that more than 90% of Security Industry Survey respondents perceive DoS/DDoS attacks as a business threat. Next we asked the respondents how they budgeted for DoS/DDoS mitigation tools in 2013 compared to the planned budget for 2014. 71% of respondents are budgeting DoS/DDoS mitigation solutions in 2014. This is an increase of 15 percentage points compared to last year. We believe that the increased number of companies budgeting for DoS/DDoS mitigation solutions is the result of the increased threat landscape and the increased public awareness. Note that 29% that have not budgeted for a dedicated DoS/DDoS mitigation solution in 2014 (and the 44% that did not in 2013) rely on adjacent technologies such as firewall, or intrusion prevention systems. However, such technologies have little success in attempting to mitigate sophisticated DoS/DDoS attacks.

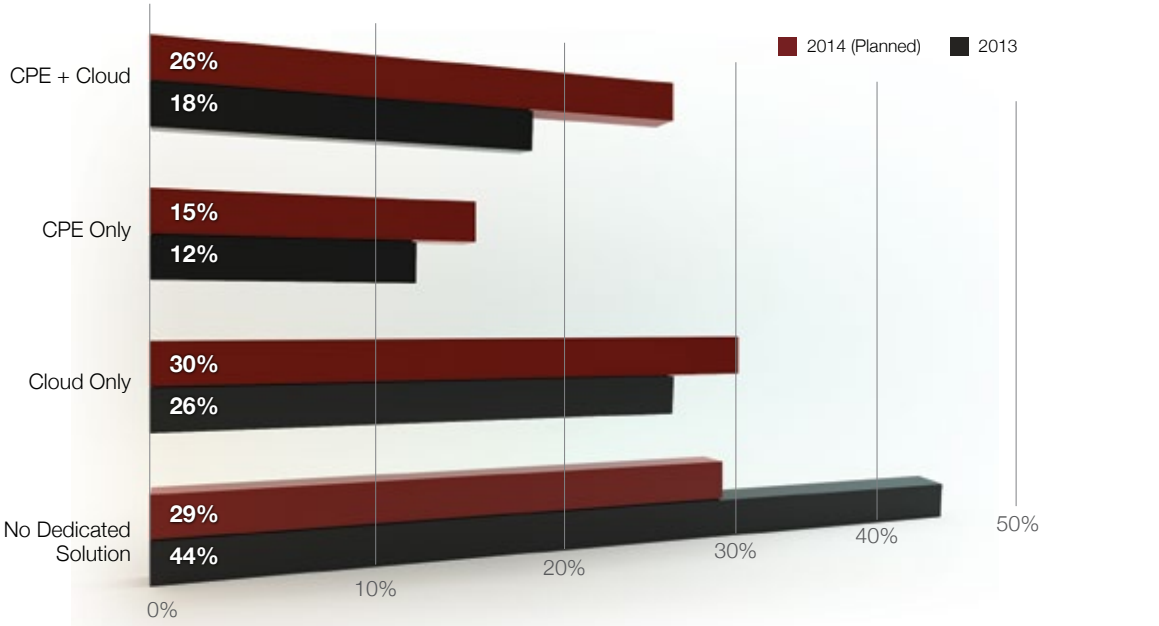


Figure 8: Budgeting for DDoS Mitigation Tools

According to the Security Industry Survey, a slight increase in the deployment of on-premise solutions is expected in 2014. Organizations that are planning to deploy Customer Premise Equipment (CPE) as a sole solution should bear in mind that while on-premise mitigation solutions can handle a wide variety of DoS/DDoS attacks, they have one prominent flaw – the inability to handle volumetric floods that saturate the organizational internet pipe.

A similar increase is seen in organizations that are expected to deploy cloud based anti-DoS/DDoS solutions. Organizations that are planning to deploy cloud-based DoS/DDoS mitigation solutions with no CPE should notice the latency associated with the diversion of traffic that is happening with most of the cloud-based solution providers. Cloud-based services fall short in mitigating SSL encrypted solutions. Please refer to SSL based attack decryption in the notable attack vectors section to learn more about SSL encrypted attacks and the consequences.

The largest increase is seen with organizations that are expected to deploy a multi-layer architecture with a combination of CPE and cloud-based services. 26% of organizations have plans to deploy such solution in 2014. In 2013 attacks clearly drove organizations towards multi-layer mitigation solutions. Figure 9 illustrates such architecture.

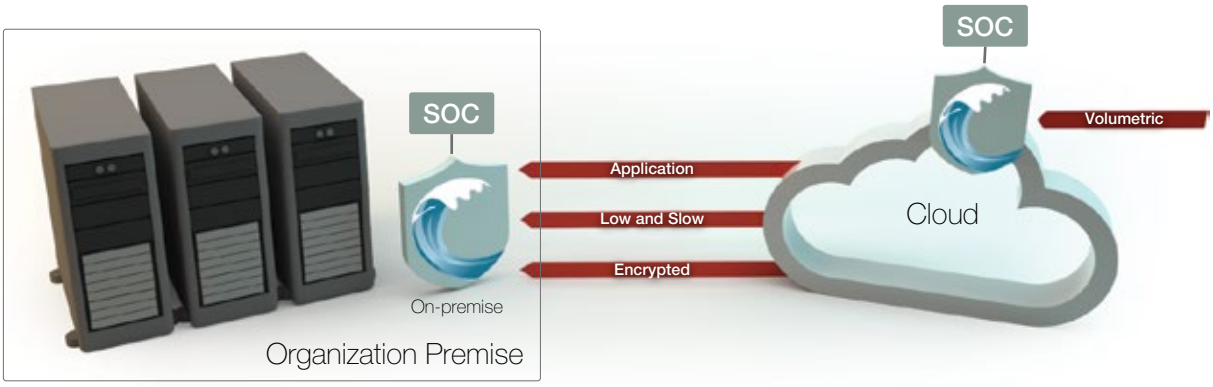


Figure 9: DoS/DDoS multi-layer mitigation with CPE and cloud-based solution.

Multi-layer architecture resolves the inadequacies of single-layer solutions. The cloud-based protection solution blocks volumetric attacks and the CPE blocks all other, non-volumetric attack vectors such as application attacks, low-and-slow attacks and encrypted attacks, which require encrypted key certification.

An additional feature of a multi-layer protection solution that was implemented today by some DoS/DDoS mitigation solution vendors is signaling. This is the ability of the on-premise equipment and cloud based solution to communicate with each other, sending alerts and sharing data about attacks.

Application Scrubbing Centers

One of the well-known defense tactics is diverting combat away from your territory to distance any damage or destruction away from home. The next generation of DoS/DDoS solutions can apply this concept with the adoption of application scrubbing centers. The concept is illustrated in the diagram below.

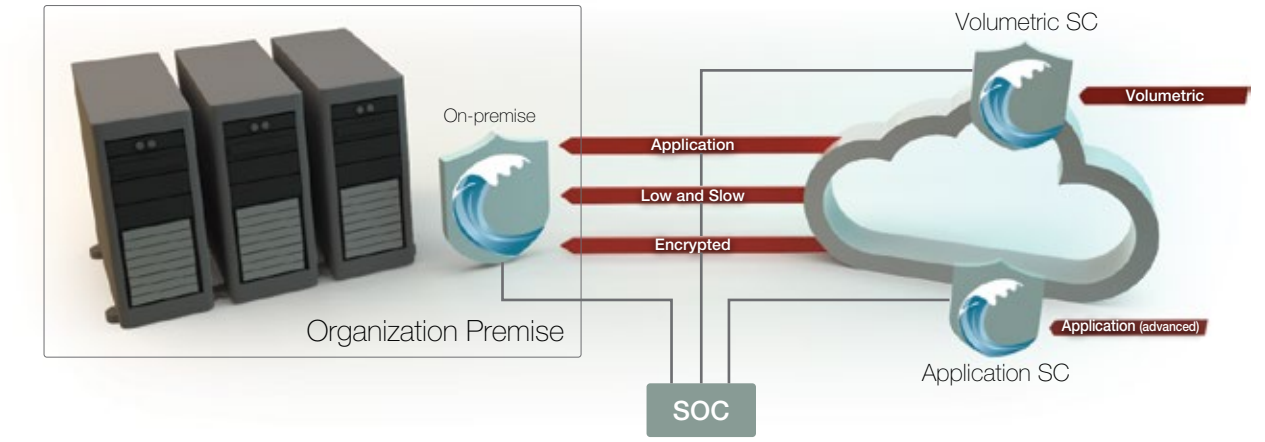


Figure 9b: Application scrubbing center.

In 2013 we noticed an accelerated pace of the cat-and-mouse game between attackers and defenders. Increasingly, target organizations had to respond in real-time to unknown application attacks that succeed in bypassing all challenges. Typically this is done through the rapid development of new mitigation challenges during the actual attack. The difficulty, however, is that organizations are extremely sensitive to firmware and software updates that are implemented hurriedly, and are reluctant to risk systems with rapidly developed and tested code.

An application scrubbing center addresses this challenge by enabling the diversion of relevant application traffic during an attack. Traffic is scrubbed using a mitigation code specifically developed for the attack, with legitimate traffic redirected back to the organization. This process will be done on demand, only in cases where the on-premise equipment fails to mitigate an attack.

06 DoS/DDoS Attack Vector Landscape

This section reviews the different attack vectors that were popular in 2013. It will examine the most frequently used attack vectors organizations have experienced, combining two types of information. Attack vectors captured by the ERT and responses to the Security Industry Survey state three largest attacks they've experienced. Figure 10 illustrates the most popular attack vectors in 2013.

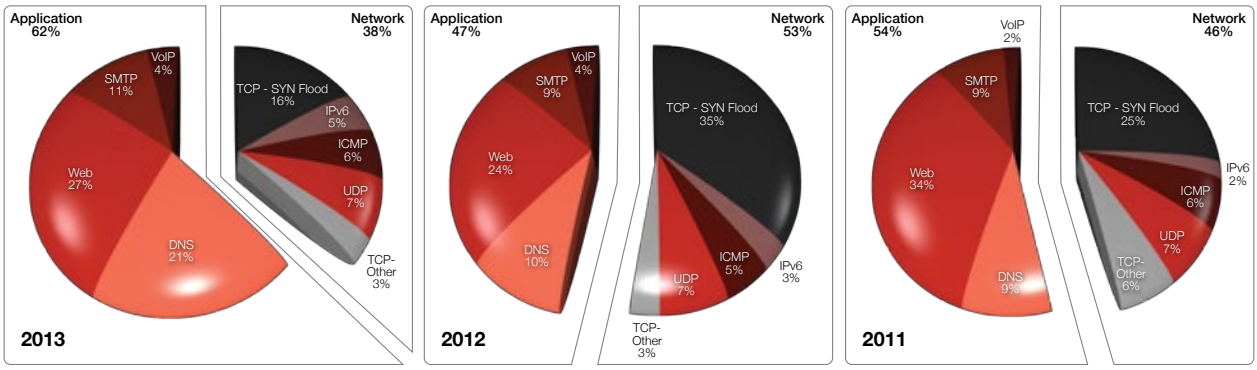


Figure 10: Diversity of DoS/DDoS attack vectors.

It is easy to see that attack vector-diversity is maintained. Moreover, our experience shows that in most destructive attacks, attackers were using multiple vulnerability attack campaigns. The motivation behind using multi-vulnerability attacks were discussed in details in last year's report. Last year's report showed that attackers only needed one attack vector to successfully hit the target and create the outage/damage. The likelihood of a successful attack increases with the number of attack vectors that are being used. Moreover multi-vulnerabilities create confusion and de-moralization in the target organization which, just as in any warfare, serves as important features for the attackers.

Application Attacks Seem More Threatening as Network Based Attacks are Easier to Mitigate

Comparing 2013 results to the 2012 figures, it is easy to see that Web-based DoS/DDoS attacks (including both HTTP and HTTPs) continue to dominate as the most frequent attack vectors. In this analysis we have gathered the attack vectors into two different groups: application attacks and network attacks. In 2013 we saw an increase in the application attacks over network attacks. Part of this change relates to the mitigation capabilities that organizations deployed over the last couple of years. As network based DoS/DDoS attacks are much easier to mitigate, they are not perceived as one of the top hard-to-defeat attacks.

More Than 50% of Attack Campaigns Deployed 5 or More Attack Vectors

As discussed above, the DoS/DDoS mitigation tools have evolved and organizations today can experience massive network and application level attacks without causing outage. However, attackers may use a number of attack vectors looking for the attack vector that is not covered by the mitigation arsenal that the victim's organization deployed. More than half of Security Industry Survey respondents reported that they've experienced multi-vector attacks with more than 5 attack vectors (see Figure 11). Note that this number of attack vectors per campaign is also part of parameters Radware uses to calculate its DoS/DDoS Risk Score.

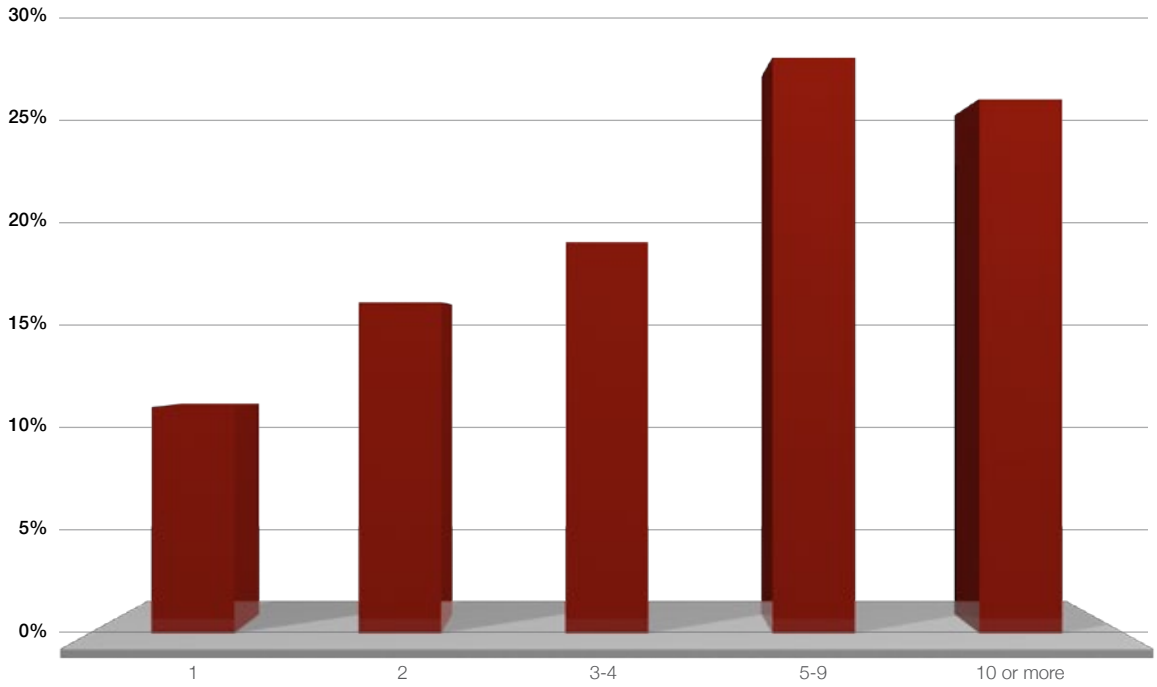


Figure 11: Number of attack vectors used in a single DoS/DDoS attack campaign.

Attackers will often not use the entire arsenal at once and instead will let the victim handle attack vectors sequentially. Only when one attack vector is blocked, the attacker will launch the next one. Under a massive attack, an organization may block four or five attack vectors, but the single attack vector that cannot be mitigated will be the one causing the damage.

Application Server Denial of Service Does Not Mean a Direct Attack on Application Server

In most cases a successful DoS/DDoS attack results in a web site that is not responding or responding very slowly. The plethora of attack vectors shown in Figure 12 does not necessarily target the Web server. The organization's Internet pipe, firewall and Web server remain the primary targets of DoS/DDoS attacks. While we saw an increase in the volumetric attacks that cause the saturation of the Internet pipe, the organization's firewall and the application web server come next. Together these are the three most common network components that are being affected by the attack (see Figure 12).

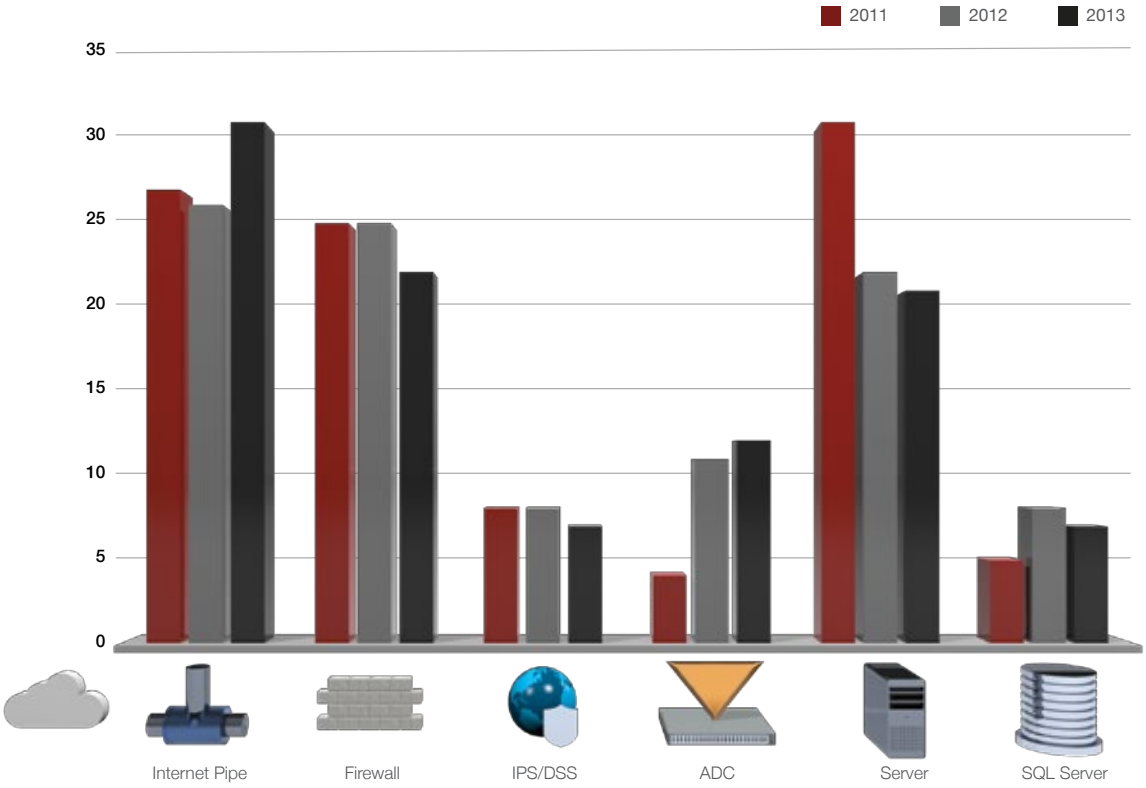


Figure 12: Network components being attacked.

Attackers Response Time Got Shorter

There is nothing new about hackers and cyber security experts playing cat and mouse. This is an endless loop: attackers creating an attack, info-security specialists building mitigation tools, and attackers finding new ways to bypass these mitigation tools. This endless loop has been common in the info-security market since its inception.

However, this traditional attack mitigation and attack cycle has managed to get dramatically shorter in the DoS/DDoS market in 2013, as attackers managed to bypass the most advanced mitigation efforts. One of the attack vectors where this cycle had shortened this year is the HTTP flood attacks. HTTP flood attacks happen when the attacker bombarded the target web server with a large number of HTTP Get/Post requests, saturating the server computing resources.

A known group of mitigation methods, mitigating HTTP flood attacks, is the HTTP challenges. While the use of HTTP challenges has become common in 2013 by DoS/DDoS web-layer mitigation solutions, this mitigation method was overcame by a new hacking tool called “Kill’ em All”. The tool was introduced at the 2013 BlackHat conference. In the conference a group of researchers presented a proof-of-concept tool that was tested against common DoS/DDoS mitigation solutions and popular web sites known to be protected by specific technologies. By emulating legitimate traffic characteristics and executing combined attacks, ‘Kill em All’ succeeded bypassing all layers of protection, including JavaScript challenges, and also claimed to pass CAPTHA protection. Regardless of the exact details, it is evident that knowledge and capabilities are out there and may surface at any time. ‘Kill ‘em All’ was used in one of the attacks the Radware ERT team was called to help mitigate. While the mitigation bypassing was very successful at the beginning of the campaign, the ERT managed to improve the mitigation capabilities and eventually stop the attack so the attackers could not bypass the mitigation solution.

07 2013 Notable Attack Vectors

SSL-Based Attacks Continue to Threaten Organizations

According to our Security Industry Survey, HTTP attacks are still more common than HTTPS attacks. Organizations have reported that the most concerning attacks they've experienced were HTTPS based attacks, mainly because HTTPS attacks commonly have no easy mitigation solution.

In 2013, about 50% of all Web attacks were using HTTPS communication, or SSL based encrypted communications for the attack. This is up 5% from just 2 years ago. Fraud and other hacking activities and a long list of privacy regulations have moved organizations to use HTTPS and encrypted communication as a default communication method. According to a number of market surveys published recently, more than 90% of enterprises are using HTTPS for any public facing web interaction. Normally HTTPS messages are being decrypted at a very late stage inside the organization network. This is illustrated in Figure 13, where the decryption is being done at the load-balancer, deep inside the organizational network.

Figure 13: Network Architecture

Attackers use this feature of encrypted messages as an evasive technique, making the front line network security tools (anti-DoS/DDoS, Firewall and IPS/IDS tools) blind to the attack. The naïve reader may suggest moving the SSL decryption (aka SSL termination) functionality to the perimeter of the organization, with a deployment of an SSL terminator tool. However, such a solution may break the network segmentation concept of segmenting network areas that deal with clear (not encrypted) sensitive data vs. encrypted sensitive data.

This network segmentation concept is crucial for complying with different info-security regulations like the Payment Card Industry Data Security Standard (PCI-DSS) and the European Union privacy legislation under EU Directive 95/46/EC. Network segments that deal with clear sensitive data may be subject to rigid limitations and audit. Decrypting SSL encrypted traffic too soon, may create huge compliance issues with the mentioned regulations and many others. This forces the SSL encrypted messages to be decrypted as deep as possible in the network, leaving the network security products blind to the possible attack.

Another interesting feature of SSL based DoS/DDoS attacks is the asymmetric nature of SSL encryption and the fact that decrypting the message takes about ten times more resources than encrypting the message (or creating the attack). Using this asymmetric feature, attackers can create a highly destructive attack with relatively low resources. Using the evasive techniques discussed above, attackers, using tools like SSL-TCH-DOS, manage to get malicious messages deep inside the network where the servers and different modules are more susceptible to lower volumes of traffic in order to create unacceptable latency or a total outage.

The trend of using SSL encrypted messages for malicious activities gained popularity in recent years in different areas of the hacking space. As noted, out of the DoS/DDoS attack vectors analyzed by the ERT team, SSL based attacks were about 50% of Web based attacks (which make about 13% of all DoS/DDoS attacks) using this technique in 2013. This trend is likely to increase. In a recent research it was estimated that in 2017, more than half of the network attacks targeting enterprises will use encrypted traffic to bypass controls[7].

Login Page Attacks Are on the Rise

In 2013 we saw an increasing number of attacks targeting a Web application login page. Almost half of Security Industry Survey participants responded that they have experienced at least one login attack this year, with 15% reporting their organization faces such attacks on a daily basis (see Figure 14).

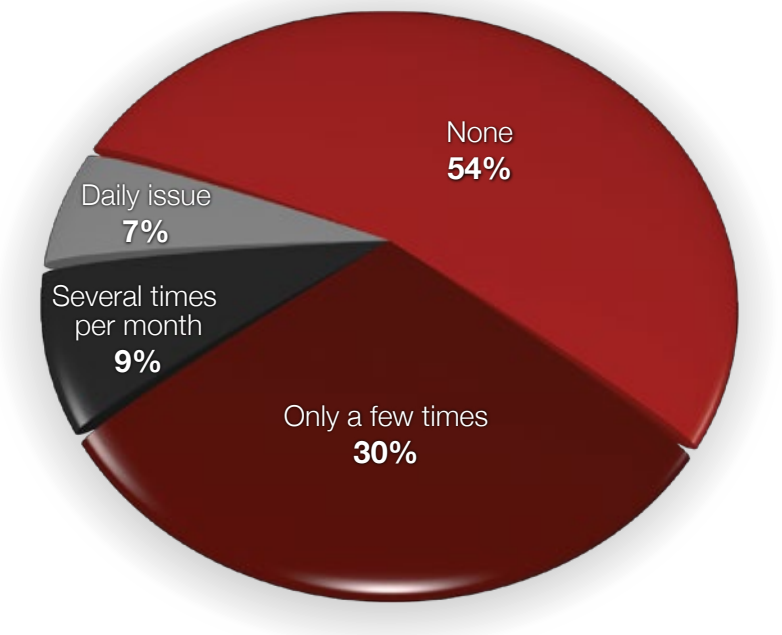


Figure 14: Frequency of Login Page attacks.

Login page attacks epitomize the concept of simplicity winning over sophistication, with some attacks compromising a vast number of web servers and overwhelming some of the world largest hosting environments.

Organizations have invested heavily in Identity and Access Management (IAM) systems to protect its sensitive assets. The front line of these systems are the login pages in which users are asked to enter credentials to be identified, authorized and gain access rights to the organizational assets.

7 "Security Leaders Must Address Threats From Rising SSL Traffic", Jeremy D'Hoinne, Adam Hils, Gartner, December 2013

Paradoxically, attackers are leveraging these security mechanisms to perform Denial of Service attacks. The attack is based on a number of weaknesses in the user-login process:

- The username/password verification process of the user-credentials entered in the Login Page requires dynamic processing. No caching mechanisms (e.g. CDN infrastructure) can prevent the processing of each login request. Moreover dynamic processing requires intensive CPU usage compared to loading static HTML page.

- User names and passwords are stored encrypted in the database. The process of verifying a valid combination of username involves cryptographic operation and database search. Both are heavy resource consuming operations. Database scalability (or lack of scalability) can frequently create traffic bottlenecks.

- Login requests are usually secured by SSL. As discussed before, SSL processing consumes much more resources than calling a non-secured page, due to cryptographic operations. This adds even more risk of resource saturation in the process.

Figure 15 illustrates a login page denial of service attack. As the attacker manages to penetrate the internal layers of the network, the potential impact on the business and operations availability increases (as illustrated by the blue curve).

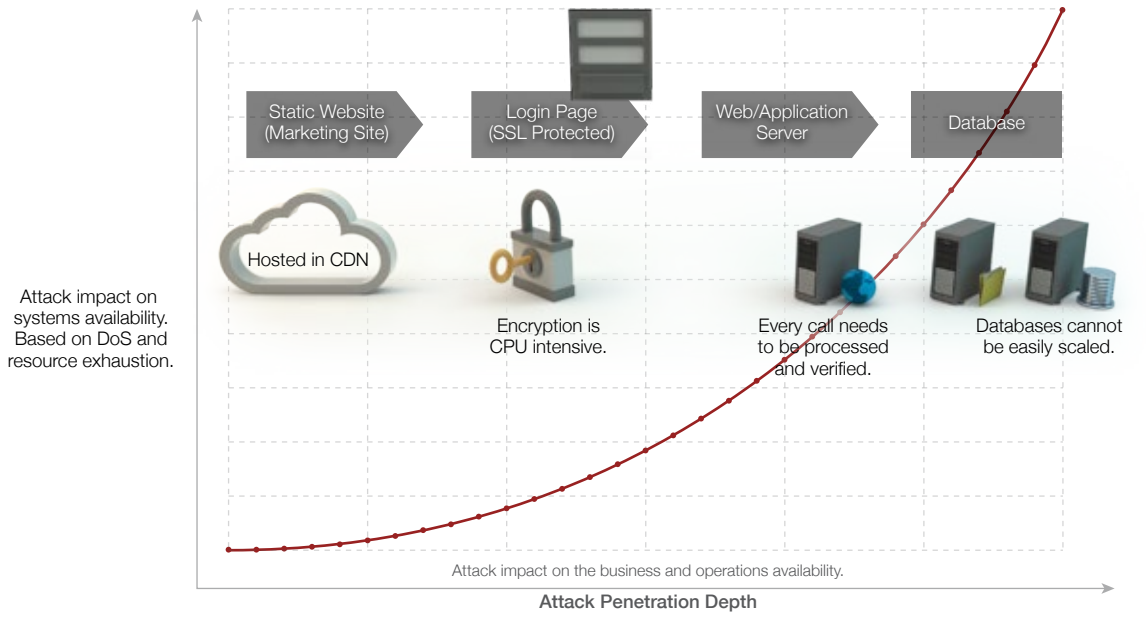


Figure 15: Login page DoS/DDoS attack flow.

Login Page DoS/DDoS attacks are virtually a low-and-slow attack[8], since they can easily bring down an entire organizational system using relatively little compute power, with a low-volume footprint sneaking under the radar of many detection systems.

8 Slow-Rate, or "Low and Slow" attacks involve legitimate traffic arriving at a seemingly legitimate albeit slow rate. Attack tools such as Slowloris, Sockstress, and R.U.D.Y. produce legitimate packets at a slow rate, allowing the packets to pass traditional mitigation strategies undetected. Traffic from such attacks is Slow-Rate, or "Low and Slow" attacks involve legitimate traffic arriving at a seemingly legitimate albeit slow rate. Attack tools such as Slowloris, Sockstress, and R.U.D.Y. produce legitimate packets at a slow rate, allowing the packets to pass traditional mitigation strategies undetected. Traffic from such attacks is often hard to detect because it looks like legitimate traffic.

Account Lockdown

Account lockdown is an innovative DoS/DDoS attack, somewhat related to the Login Page attacks discussed above. The ERT saw this attack being used in different attack campaigns. The attack is based on account lockdown policy that is mandated by most of info-security regulations. According to this requirement, users have a predefined limited amount of false tries trying to log on to the system before the account is locked. Attackers take advantage of this requirement and intentionally lock key user accounts such as senior management, to affect the performance of the entire organization. Account lockdown can also be used to manipulate online bidding, where a malicious user locks other bidder accounts, securing a win with an attractive price. The ERT has encountered this attack type in leading auction sites.

DNS Reflective Attacks Spread

DNS based volumetric floods ratio increased significantly (from 10% in 2012 to 21% in 2013), becoming the second most common attack vector. 50% of Security Industry Survey participants were able to point out that they have experienced a DNS attack. The growing popularity of DNS flood attacks can be attributed to these attacks' ability to generate massive traffic using limited resources. This ability is combined with the attacks' multi-layer architecture that makes it almost impossible to track down the attackers. The combination makes this attack-type very appealing to attackers.

One of the most notable DNS reflective flood attacks in 2013 was the DoS/DDoS attack in March on the anti-spam Swiss organization Spamhause. The attacker, allegedly a British teenager, arrested in September 2013, managed to divert 300 GBPs of DNS traffic to the Spamhause servers.

Domain Name Servers (DNS) protocol that is used to convert URLs to IP addresses introduces various vulnerabilities, exploited by attackers to launch different DNS-based attacks:

- **Basic flood**: a basic flood attack sends many DNS requests to a DNS server, exhausting its parser and cache database resources
- **Recursive DNS flood**: an attack that sends non-cached DNS requests to be resolved by a DNS server
- **Reflective DNS flood**: favorite among attackers, this type of attack is the focus of this chapter. Being asymmetric in nature, a reflective DNS Flood enables generating a massive network flood using limited resources and can be launched on organizations not hosting a DNS server. Using IP spoofing, these attacks are extremely difficult to track
- **Garbage flood**: this attack sends large packets to the DNS server using port 53, saturating the DNS internet connection and exhausting the DNS parser

In our research we found that 83% of all DNS attacks were reflective DNS floods, which enable saturating an organization's internet pipe. This is up from 11% in 2012. The growing appeal of reflective DNS attacks can be attributed to several factors – the top of which are the amplification effect, allowing attackers to generate a massive impact on the internet pipe with very little resources, and the ease of maintaining anonymity by hiding behind the intermediary DNS servers.

Mechanics of a Reflective DNS Attack

A reflective flood uses a two-step process to launch an attack:

1. First, a large number of requests are sent to one or more DNS servers. The requests use a spoofed source IP of the target victim.

2. The DNS server receiving the requests replies to the spoofed IP, thereby unknowingly launching an attack on the target victim with responses to requests that the victim never sent. The target organization, whose resources are exhausted, does not have to run a DNS server on its own, as the attack targets the entire network.

Figure 16 illustrates DNS reflective attacks. Also, Radware's DNS Amplification Attack video that graphically illustrates the structure and flow of a reflective DNS attack.

Figure 16: DNS Reflective attack

Maintaining Anonymity – IP Spoofing

How is the IP spoofing possible? Most DNS queries are carried out using UDP, a protocol that does not enable source IP validation. Consequently, the intermediary DNS server assumes the requests are arriving from the victim and sends it back the replies.

The IP spoofing makes it extremely difficult for the target server to detect the attacker, as it appears as if it is being attacked by a legitimate DNS server. IP spoofing also invalidates IP reputation services, which may assign a bad reputation to a legitimate DNS server.

For security experts who want to track the attack origin, IP spoofing makes the task quite difficult – due to the intermediary DNS servers that mask the real attackers. Figure 17 illustrates a reflective attack and illustrates the nature of such attack.

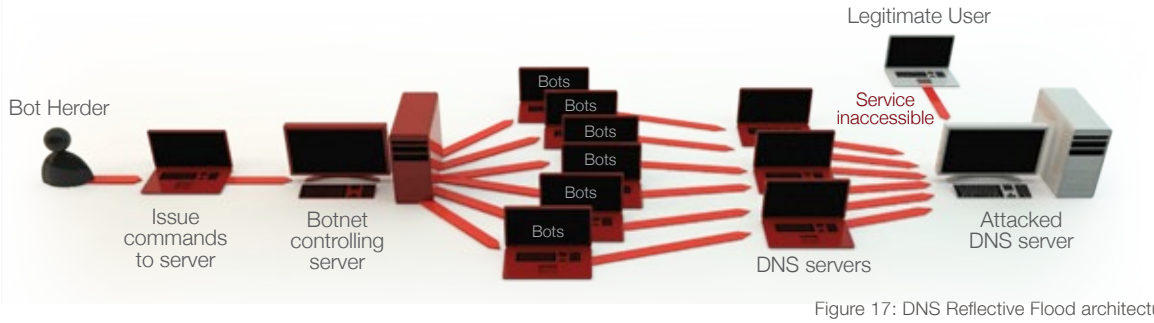


Figure 17: DNS Reflective Flood architecture.

Another characteristic of the spoofed IP (and port) is the ability to attack any server or service. The attacker can use the target's known server IP and port to make sure the attack is sent to any service, not just a DNS service. The attack will look like a garbage flood on the service, which will receive irrelevant data and will have to parse and examine the data to ensure it is not legitimate traffic, thus excusing its resources.

Attack Amplification

Another attribute contributing to the destructive potential of reflective DNS floods is message amplification, achieved by using DNS extensions. The possible size of the extension – 4096 bytes, allows the attacker to send a small number of short requests, while the replies sent by the DNS server are greatly amplified, exhausting the victim server resources. Each of the following techniques further extends the attack amplification:

- **Regular DNS replies**: in DNS, a normal reply is 3-4 times larger than the request. Consequently, a normal request to a legitimate cached object can result in a reply that is 4 times larger

- **Researched replies**: hackers can study the DNS server and find which legitimate queries can result in large replies. In some cases, the amplification factor can reach up to 10 times of the original request

- **Crafted replies**: an attacker can compromise a poorly secured DNS server and ensure that his requests are answered with the maximum DNS reply message (4096 bytes). Using this approach, attackers can reach an amplification factor of up to 100 times

This is best illustrated by a simple math equation. Assume an attacker with a 5 Mbps internet connection, which means he can send about 14k request of size 44 bytes per second. This small size of requests (14k RPS\5 Mbps) on its own can cause some damage to a normal DNS server.

However, if the attacker has a crafted reply with the maximum size of 4096 bytes, the victim server will receive ~465 bps of traffic, beyond its normal traffic bandwidth. Only three such attackers are needed to reach a 1.4 Gbps attack throughput, which will cause almost any service to immediately reach a denial of service state.

08 Unprecedented Severity Introduced by Operation Ababil

Hundreds of DoS/DDoS attacks are handled each year by Radware's ERT. Attacks vary immensely in characteristics, duration and impact. However, one attack stood out above them all: Operation Ababil.

Operation Ababil set new records as the most severe DoS/DDoS attack known to date. The attack lasted a full year with a net attack time of 100 days. It employed the most sophisticated attack vectors, introduced server-based botnets, and has succeeded passing known mitigation challenges that were never overcome before. On the impact side, Operation Ababil had the most devastating results, causing outages of public web-sites of numerous banks' web-sites that lasted hours and days.

Operation Ababil received extensive press coverage, which naturally focused on the visible attack perimeter aspects. But an insider view of the attack, given from a targeted organization perspective, provides educational insights on how such large-scale DoS/DDoS attacks enact, and the lessons that can be learned mitigating such attacks.

This section presents Operation Ababil as a case study that summarizes this entire report as it captures the essence of the attack landscape and our best practices.

Operation Ababil- Timeline of Events

The trigger for Operation Ababil is traced to the "Innocence of Muslims" movie trailer, which was published on YouTube. The film, which contained what some viewed as offending content, triggered demonstrations, violent protests and attacks on U.S. embassies in Muslim countries. A few days later, on September 18th, 2012 a group of hackers, called "Cyber Fighters of Izz ad-din Al Qassam" announced an upcoming cyber-attack campaign on what they claimed 'American and Zionist' targets. The attack targeted the US financial sector, initially focusing on Bank of America and NYSE. Next, it spread to the entire banking community.

The first phase of the attack lasted six weeks. After a pause, three additional phases followed, each lasting 6 to 8 weeks. In total, the attack lasted 10 months, with 100 days of net attack time.

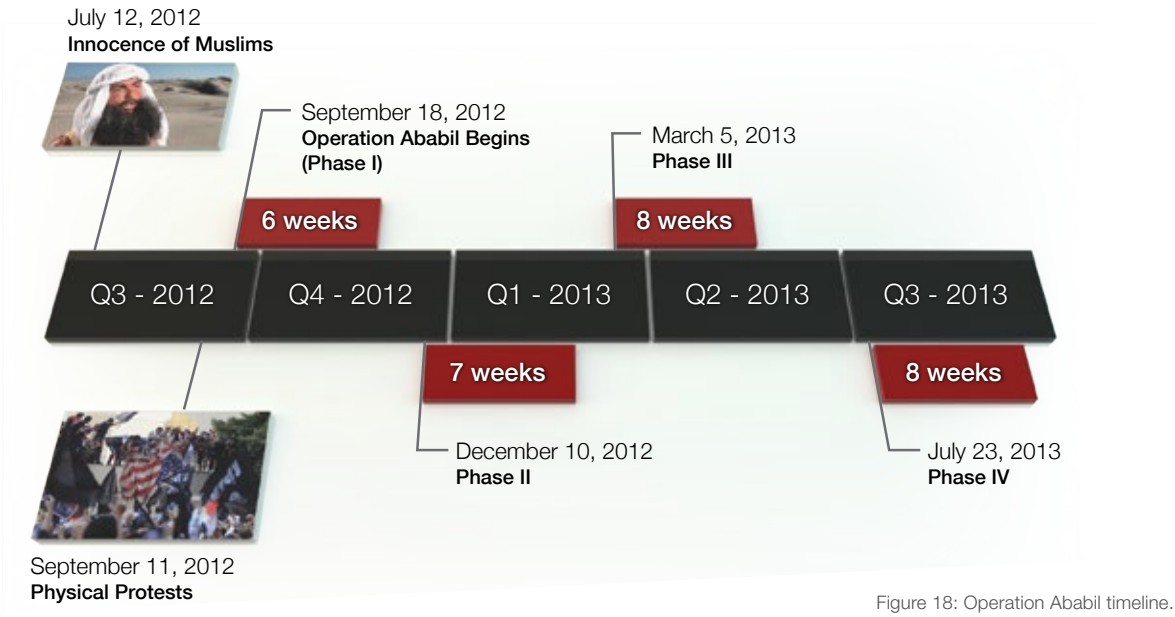


Figure 18: Operation Ababil timeline.

Operation Ababil not only broke attack duration records, but it also had a destructive impact. For example, in the third phase of the attack alone, 15 major U.S. bank sites were offline for a total of 249 hours - averaging 2.7 hours of weekly downtime per bank[9].

An Inside View - Organization Under Attack

How does a forceful and prolonged DoS/DDoS attack like operation Ababil look from the inside? The following tells the story of one of the banks that were the target of Operation Ababil. The organization received assistance from the ERT team at one of the later stages of the attack.

Initially, the bank's protection was based solely on the DoS/DDoS mitigation services provided by a cloud-based DoS/DDoS mitigation solution. Overall, the cloud based mitigation solution mitigated volumetric and network attacks successfully. However, application level attacks and HTTPS in particular, were not mitigated properly.

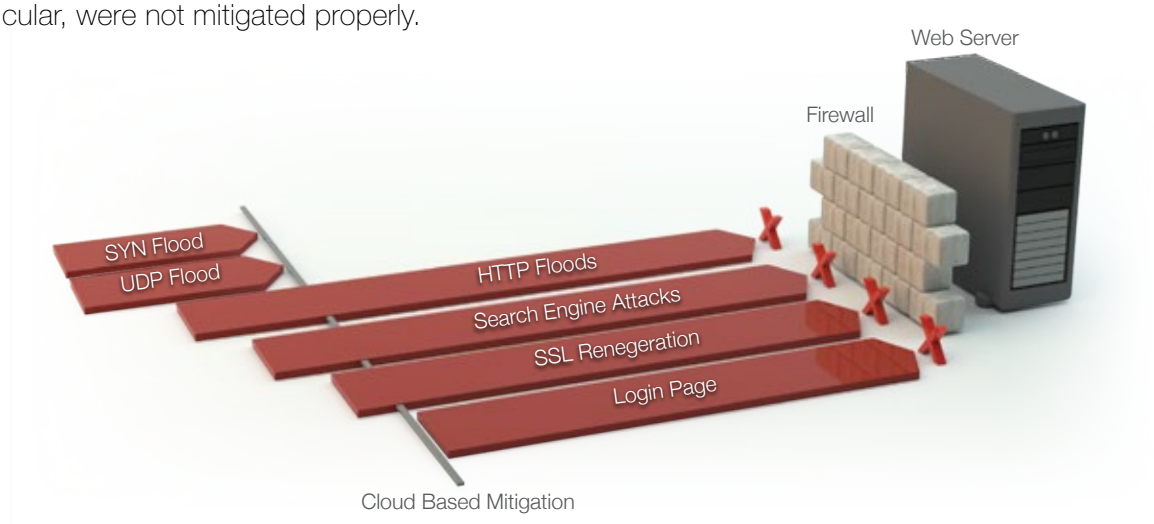


Figure 19: The attack landscape on the banks attack vectors and mitigation.

Over a dozen attack vectors were included in the attack campaign on the bank, as described in the following table:

Attack Vector	Type	Description	Mitigation
SYN floods	Network/Volumetric	The oldest DoS/DDoS attack in the book, but still a very effective one.	Cloud based mitigation
UDP floods	Network/Volumetric	A volumetric attack and one of the most popular attack vectors.	Cloud based Mitigation
HTTP Floods	Application	Multiple HTTP attacks that target different URLs. Was partially stopped by the IPSs.	X
Search engine floods	Application/ Low-and-slow	An application bordering low-and-slow type of attack that requires a web site to execute searches, consuming resources and impacting performance.	X
SSL renegotiation	Low-and-slow	A low-and-slow attack that renegotiates the SSL keys repeatedly, consuming server resources.	X
Login page attacks	Application (encrypted)	An encrypted (HTTPS) resource-intensive DoS/ DDoS attack targeting the Login page.	X

9 "Bank website attacks reach new high: 249 hours offline in past six weeks", MSNBC April 2013

SYN flood and UDP flood attacks were successfully mitigated by the cloud based mitigation solution. However, HTTP and HTTPS attacks could not be blocked and required a different strategy.

At that stage the bank blocked HTTP floods manually using an IPS technology creating ad hoc signatures for each attack. This process blocked the 'Search engine floods', the 'SSL renegotiation', and partially the other HTTP floods. Yet, the following day the attacking group changed the pattern and launched a new attack.

At that stage the bank moved to a more permanent solution, adding on-premises DoS/DDoS mitigation equipment to complement the existing cloud-based mitigation. Only after an HTTP challenge technology was implemented on premise, HTTP floods were mitigated automatically in full. Then, to stop **Login page floods**, HTTPS challenges were added. This required integration with SSL technology equipment.

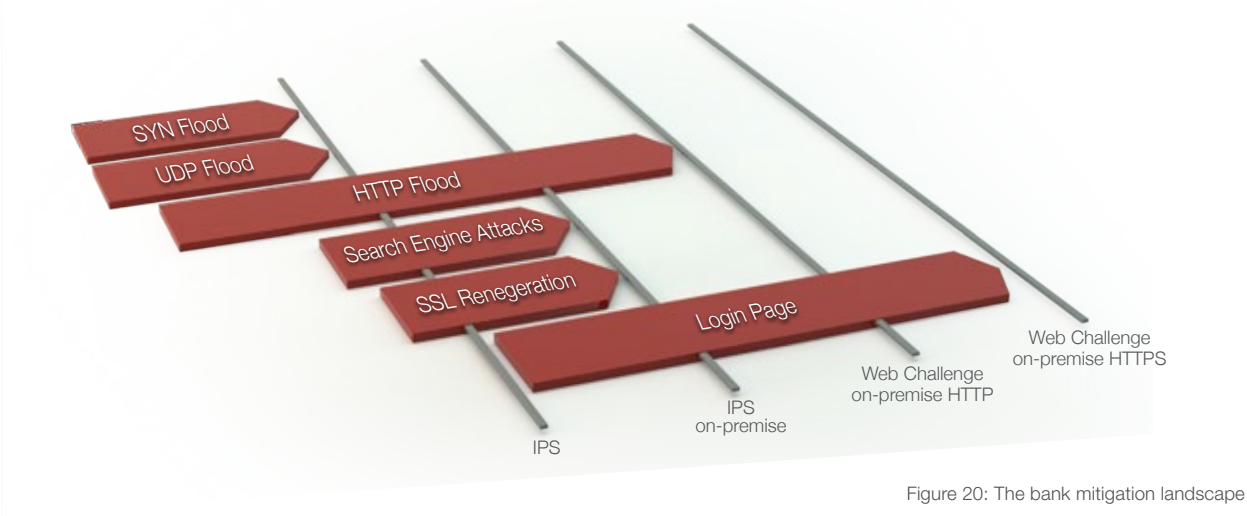


Figure 20: The bank mitigation landscape

While Operation Ababil was exceptional compared to other DoS/DDoS attacks, it cannot be viewed as an isolated, one-time event. Rather, it provides a clear indication that attackers are raising the bar in respect to multiple dimensions:

- **Attack duration** – long-lasting DoS/DDoS attack campaigns can run for months and re-surface several times
- **Attack vectors** – dozens of attack vectors may be used, which cannot be handled by a single mitigation solution
- **Sophistication** – attack complexity and intensity increases using server-based botnets and the ability to bypass advanced security challenges

It is reasonable to expect that attacks with the same scope and severity as Operation Ababil will surface in the future, requiring that organizations be prepared with the appropriate infrastructure, expertise and mind set.

09 DoS/DDoS Protection Best Practices

This section looks at this year's business and technical attack trends. It provides a set of best practices for organizations that are the target of DoS/DDoS attacks and mitigation strategies and tactics that they need to deploy.

Three Important Features for DoS/DDoS Protection

1. **Time to Mitigate**: The financial consequences of DoS/DDoS attacks were shown over and over again in 2013 and were discussed in details at the beginning of this report. When deploying DoS/DDoS mitigation solutions, organizations need to ensure that their detection and mitigation solutions can detect attacks and start the mitigation process within the shortest time possible.

   Solutions that require traffic diversion for attack mitigation may suffer from longer time to mitigate. In addition, when the DoS/DDoS mitigation solution is built from disparate separated solutions, the switch between the different mitigation solutions may delay the time the mitigation process starts. Organizations need to look at time-to-mitigation as a key success factor, and ensure that the solution they deploy provides the shortest time-to-mitigate.

2. **Mitigation Coverage**: Considering that more than 50% of Security Industry Survey's respondents suffer a multi-vector DoS/DDoS attack with more than five (5) different attack vectors on different layers of the infrastructure, organizations should look for a DoS/DDoS mitigation solution that offers wide attack coverage. Such solution should mitigate volumetric network attacks, SSL attacks, as well as application level attack vectors (more on multi-layer approach see below).

3. **Single Point of Contact in Case of an Attack**: With this wide range of detection and mitigation options on one hand, and the pressure to start the mitigation actions as soon as possible on the other hand, it is crucial that your organization will have a single point of contact in case of an attack. Be it an internal security team employed with DoS/DDoS experts that are ready to get to action in minutes, or an external emergency response team that can be called to action with minutes, these teams should help the organization choose the correct mitigation options and help divert the Internet traffic between the different mitigation solutions.

Multi-Layer Approach

2013 events have already driven organizations towards two-layer mitigation solutions. Two-layer architecture resolves the issues of single-point solutions. The cloud-based protection blocks volumetric attacks and the on-premises solution blocks all other, non-volumetric attacks:

- Application attacks
- Low-and-slow attacks
- Encrypted attacks, which require encrypted key certification

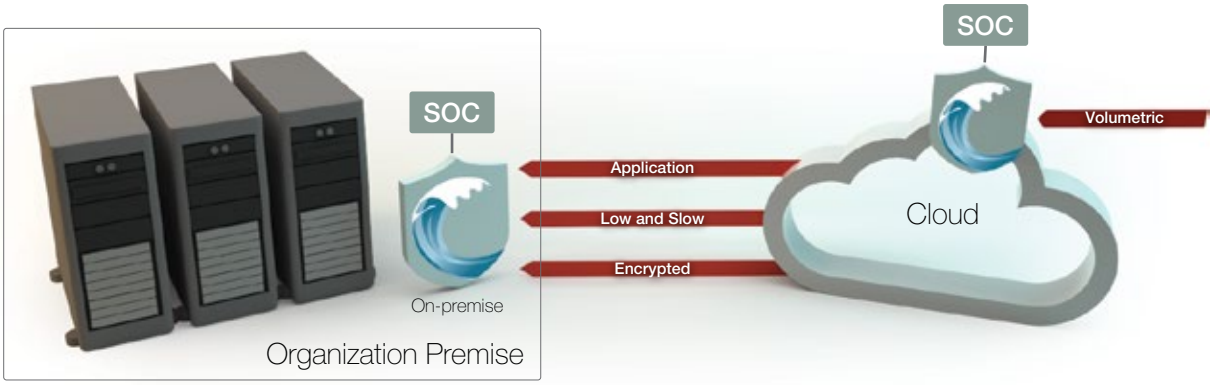


Figure 21: Two layer mitigation architecture

SSL Attack Mitigation

Based on the clear evidence of the rise of SSL attacks in 2013 and the difficulty of mitigating such attacks, it seems that SSL attacks may pose a major threat in 2014.

SSL DoS/DDoS attacks are inherently difficult to mitigate. Cloud mitigation solutions require that certificates will be exported outside the organization, yet this is rarely accepted by regulators. On-premise solutions require SSL termination capabilities, commonly done by dedicated hardware due to the resource intensive operation. Such hardware is not commonly deployed, meaning that during an attack, an organization cannot immediately turn on a switch or service to mitigate the attack.

Organizations should look for SSL based DoS/DDoS mitigation solutions with a deployment that does not affect the legit traffic performance.

Methods

Among the 198 organizations responding to the Security Industry Survey there was relatively a large portion of enterprises with annual revenues exceeding $1B in 2012[10]. Figure 22 shows the breakdown of respondents based on 2012 revenues.

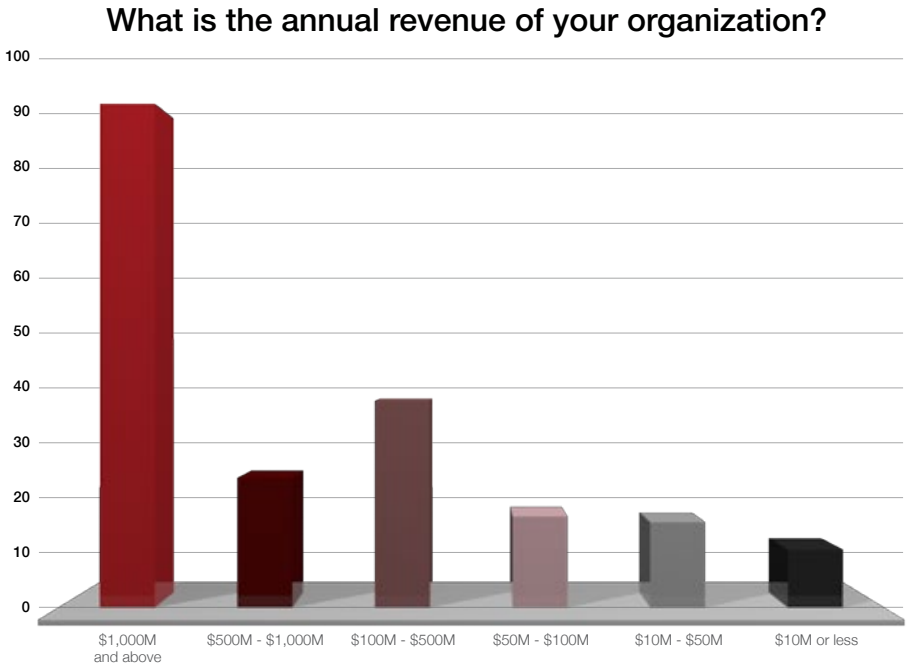


Figure 22: Annual revenue.

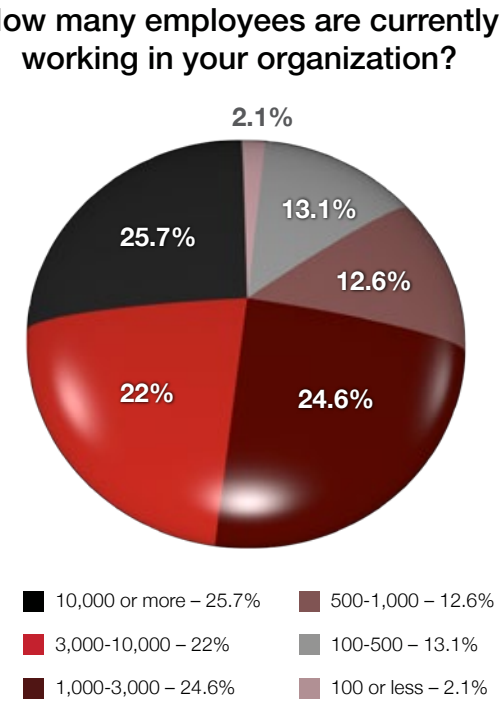


Figure 23: Number of employees in the organization.

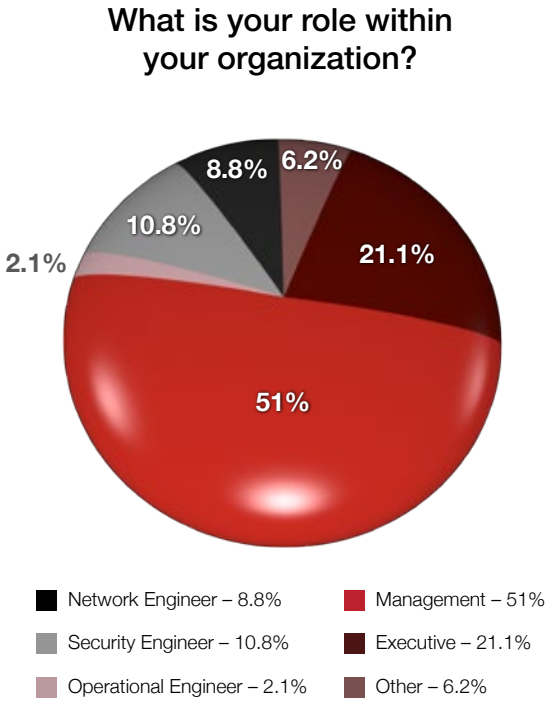


Figure 24: Employees' role within organization.

10 As most organizations were not concluded the 2013 fiscal year by the time the data was collected, we have asked organizations to report their 2012 revenues.

What is your organization type?

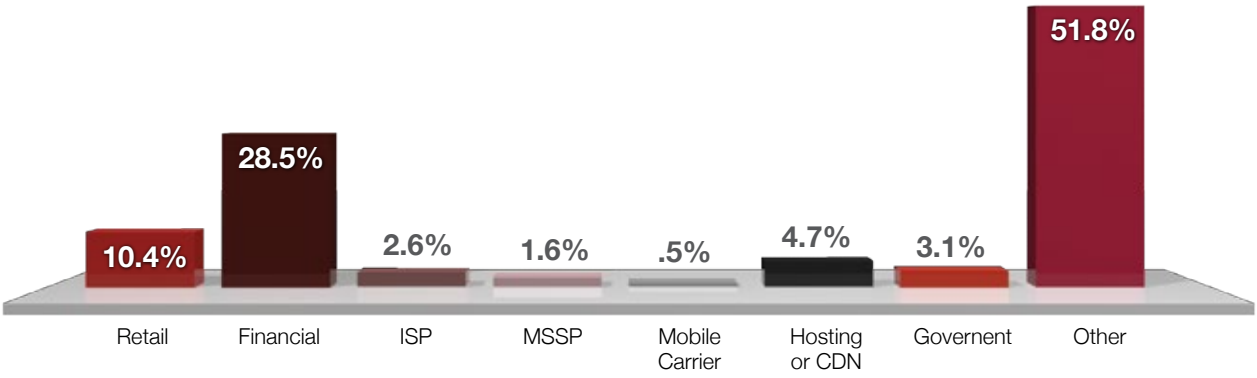
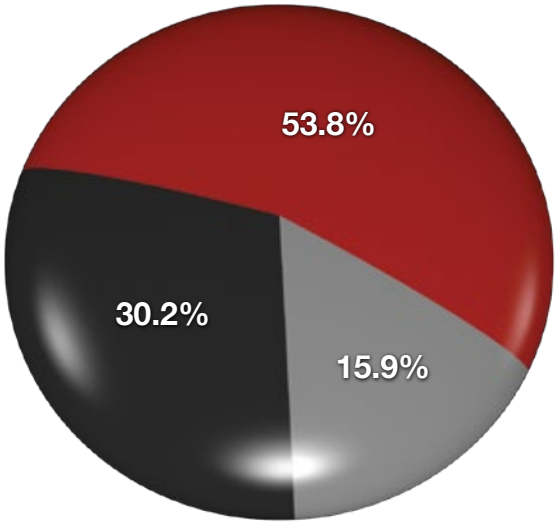


Figure 25: Organizations by type.

What is the scope of your organization's business?



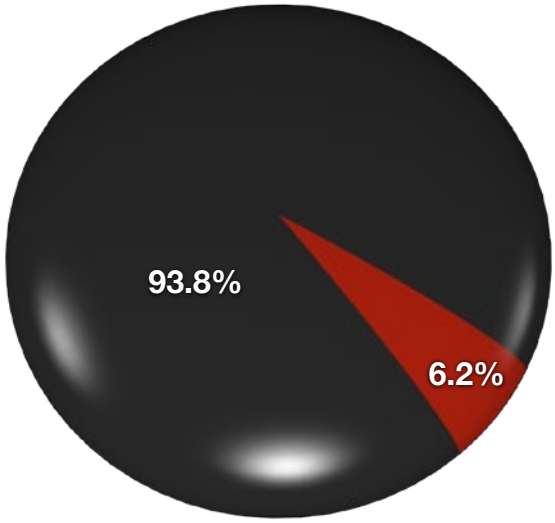
Country-wide e.g. U.S. – 30.2%

Region-wide e.g. North America – 15.9%

World-wide – 53.8%

Figure 26: Geographic scope of business.

Is your organization currently using Radware's security products?



Yes – 6.2%

No – 93.8%

Figure 27: Majority of Security Industry Survey responders are not Radware customers.

Credits

Authors

Ziv Gadot
SOC/ERT Group Leader
Radware

Motty Alon
Security Marketing Director
Radware

Lior Rozen,
Director of DefensePro R&D
Radware

Matan Atad
Security Researcher
Radware

Yosefa Shulman
R&D Group Leader
Radware

Vikalp Shrivastava
Security Solutions, APAC
Radware

Advisory Board

Avi Chesla
CTO
Radware

Carl Herberger
VP Security Solutions
Radware

Werner Thalmeier
Security Solutions, EMEA
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.

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 and www.ddoswarriors.com for additional expert resources and information.

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®.