



**STAY SAFE IN CYBER SPACE**  
DISTRIBUTED DENIAL OF SERVICE ATTACKS –  
INSIGHTS AND SOLUTIONS



LIFE IS FOR SHARING.

# STAYING SAFE IN CYBER SPACE

## DISTRIBUTED DENIAL OF SERVICE ATTACKS

### - INSIGHTS AND SOLUTIONS

## TABLE OF CONTENTS

Introduction .....	3
What is DDoS? .....	4
The Price Tag .....	5
New Opportunities and Motives.....	6
IT Evolution Invites Threat .....	7
Why Read Further? .....	8
The Changing Landscape of DDoS Attacks .....	9
New Methods of Attack.....	9
Multi-Vector Attacks.....	9
Changing Criminal Incentives .....	10
Easier Access to Illegal Tools.....	10
More Opportunities .....	10
Smart Devices and DDoS Attacks .....	11
Assault on Estonia .....	11
Secret Cyber Weapons of an E-State .....	12
A Deeper Look at DDoS .....	13
Volumetric Attacks.....	13
ICMP Flood .....	14
TCP SYN Flood .....	14
UDP Flood .....	14
Domain Name System (DNS) Amplification Attacks.....	14
Application Layer Attacks.....	15
HTTP GET and HTTP POST Floods.....	15
Domain Name System (DNS) Attacks.....	16
Attack Tools.....	16
Low Orbit Ion Cannon (LOIC).....	16
Slowloris .....	16
Traditional Defense Products No Longer Effective .....	17
Firewalls .....	17
Intrusion Detection and Prevention Systems (IDS and IPS).....	17
Strategies for Defense Against DDoS Attacks .....	18
Deutsche Telekom Solutions .....	19
Backbone Protection from Deutsche Telekom.....	20
Cloud Protection from Deutsche Telekom .....	21
On-Premise Solutions from Deutsche Telekom .....	22
Benefits of the Deutsche Telekom's DDoS Defense Solutions .....	22
Many Sources of Protection from Deutsche Telekom.....	23

# STAYING SAFE IN CYBER SPACE

## DISTRIBUTED DENIAL OF SERVICE ATTACKS

### – INSIGHTS AND SOLUTIONS

## INTRODUCTION

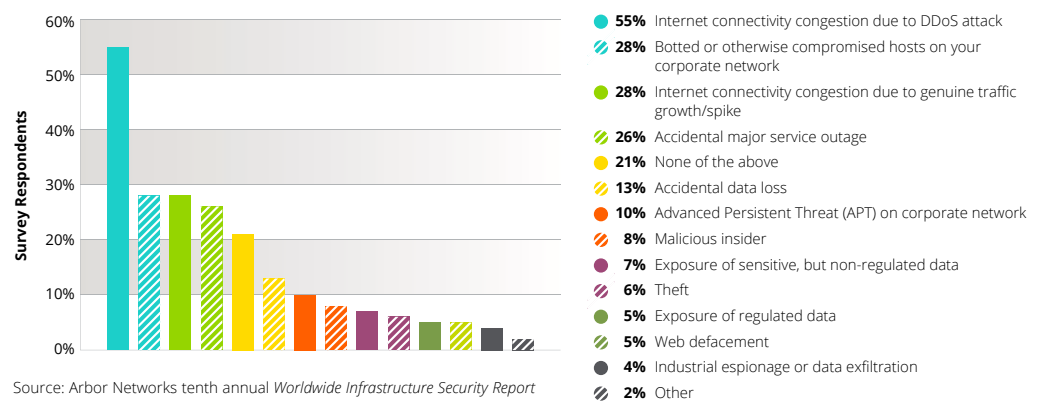
Are you wondering what the big deal is about cyber security and DDoS attacks? Think it will never affect your company because you have all the right firewalls and detection systems in place? Then consider what today's cyber criminals are capable of and how even the largest organizations have not been able to stop them.

Imagine you're an employee of a huge media or broadcasting company. You feel secure and never think that your sensitive information might be accessed. But one day you come to work and discover that cyber criminals have stolen your unfinished project, along with confidential files. In fact, they have managed to infiltrate devices across the company's entire IT infrastructure, stealing and erasing data on servers and PCs. The network contained email addresses, salary lists, bank account data and health insurance records, as well as your own personal credit card numbers.

Or think about what could happen if your online services were suddenly unavailable. In the morning you're paying bills on your computer, but in the afternoon none of the websites you normally use are reachable. In addition, you can't find out what's going on because the connections to your digital newspaper and government websites have been cut off. This time it's the work of a group of cyber criminals who demand ransom to return your data.

According to the Arbor Networks Worldwide Infrastructure Security Report, more than half of the respondents reported that internet connectivity congestion due to DDoS attack was the most commonly observed threat experienced on corporate networks.

Internal Network Security Threats



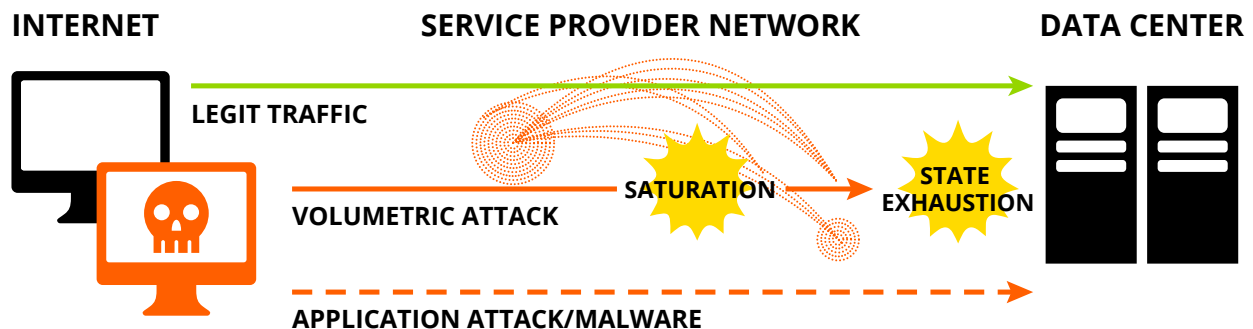
These scenarios are just two everyday examples of the devastating effects an attack can have. Indeed, according to Akamai's Q1 2016 State of the Internet Security Report, DDoS attacks have increased 125% year over year. It is therefore of utmost importance to make sure your organization has the most up-to-date security measures in effect. Today's modern cyber protection systems, unlike legacy products and conventional methods, are capable of predicting, identifying and mitigating attacks in real time across both physical premises and cloud-based networks.

# STAYING SAFE IN CYBER SPACE

## DISTRIBUTED DENIAL OF SERVICE ATTACKS – INSIGHTS AND SOLUTIONS

### WHAT IS DDoS?

DDoS is a distributed denial of service attack, where an attempt is made to impair access for legitimate users to any internet facing application or service. This is often done by transmitting a series of data packets from computers or other computing devices that have been infected with so-called malware: viruses and trojans. These corrupted computing devices are then called ‘bots’, and collectively they can form a network called a ‘botnet’. Controlled by a central command server, botnets can be used for many nefarious purposes, including DDoS attacks.



Viruses and trojans are easily spread, often as seemingly innocuous emails that, once opened, infect the PC. Due to their dynamic adaptability, they are very difficult to detect. In addition, there are still vast numbers of machines connected to the internet that aren't running the latest patched software or up-to-date virus detection tools.

According to SC Magazine UK, currently 1.5 billion machines are potentially infected<sup>1</sup>. In fact, many bots remain unnoticed for years while being used to help steal data, generate DDoS attacks, distribute spam emails, overload online systems or disrupt communications.

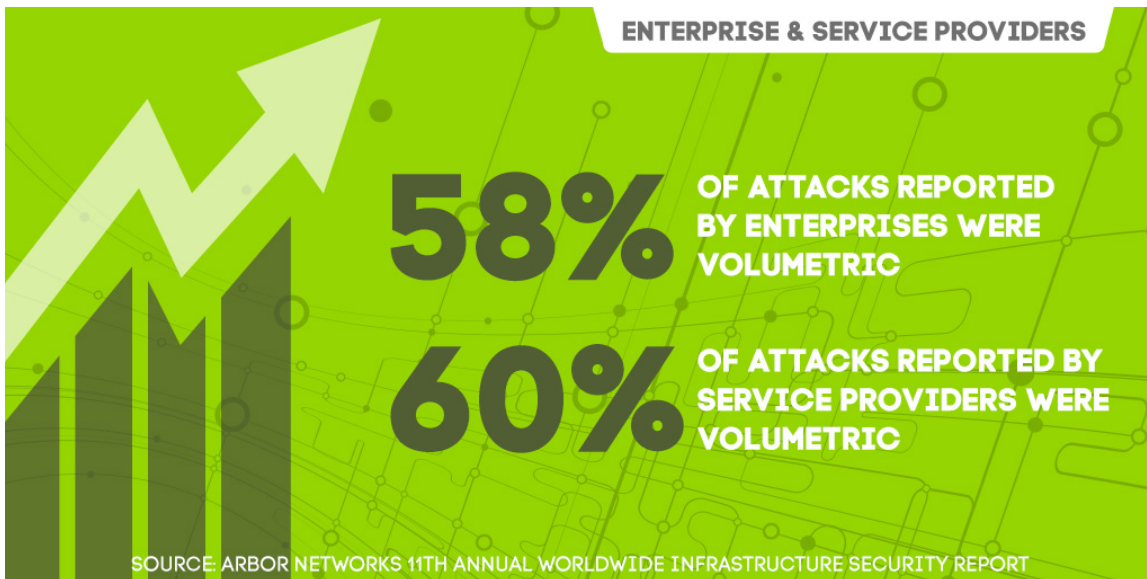
---

<sup>1</sup> SC Magazine UK, June 1, 2016, <http://www.scmagazineuk.com/15-billion-windows-computers-potentially-affected-by-unpatched-0-day-exploit/article/499854/>

# STAYING SAFE IN CYBER SPACE

## DISTRIBUTED DENIAL OF SERVICE ATTACKS – INSIGHTS AND SOLUTIONS

The DDoS landscape has greatly changed over the last few years, making the possibility of assaults greater than ever before. For example, it is now simple to find online criminal organizations that rent botnets on a pay-for-volume scheme, offer guidelines on how to build a botnet, or ask for volunteers to help with their campaigns. Attacks have also increased in size and sophistication and are therefore more difficult to identify and mitigate.



### THE PRICE TAG

According to a survey conducted by the market research agency B2B International spanning the months between April 2014 and May 2015 and encompassing 38 countries with 5,564 respondents, over 90% of the reviewed businesses experienced some form of external cyber threat<sup>2</sup>. The survey also stated that the average cost of data breaches ran between \$38,000 and \$551,000 per company. In addition to stolen assets, subsequent costs of security leaks include legal fees, defense expenses, lost business and in some cases increased insurance premiums. Harder to calculate in terms of monetary impact are the loss of reputation and damage to a company's image.

---

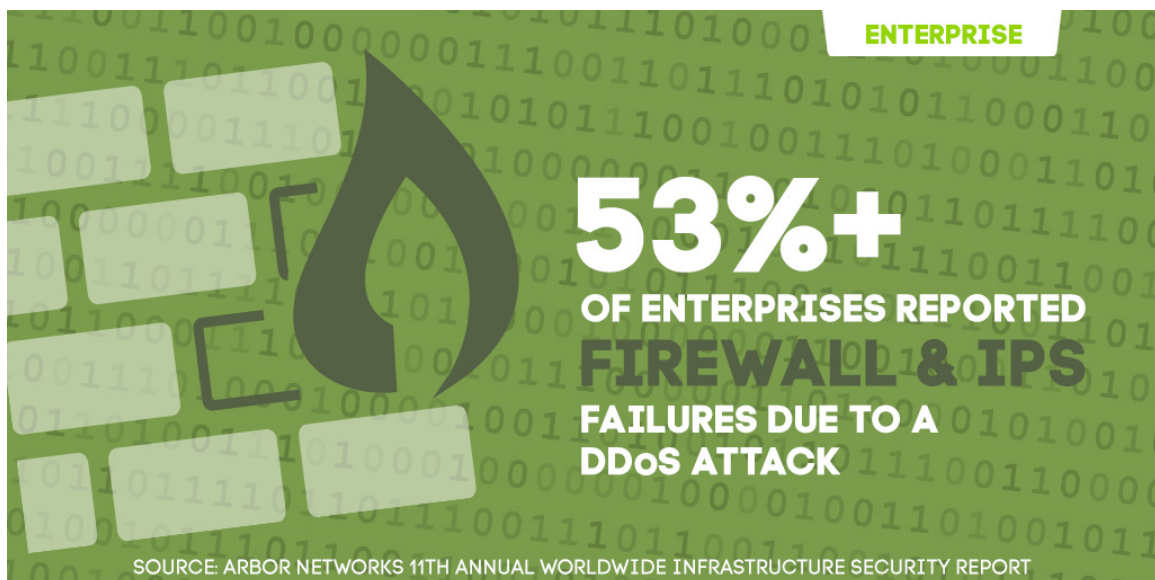
<sup>2</sup> Global IT Security Risks Survey 2015, conducted by B2B International and analyzed by Kaspersky Labs

# STAYING SAFE IN CYBER SPACE

## DISTRIBUTED DENIAL OF SERVICE ATTACKS – INSIGHTS AND SOLUTIONS

### NEW OPPORTUNITIES AND MOTIVES

Businesses have become increasingly dependent on the internet, which enables the offering of higher quantities of products and services to a broader customer base. Yet it is exactly this great influx of online revenue that has made it a lucrative target for cyber criminals. There is a lot of money to be made with data and identity theft, fraud and extortion. Direct economic gain is, however, not the only motivation behind DDoS attacks. There has also been growing momentum behind politically or ideologically inspired attacks, as well as assaults against business rivals in order to gain a competitive advantage.



The harm to enterprises as a result of DDoS strikes can be enormous. Direct financial damages can run into the millions, especially for time-sensitive transactions such as trading. At the same time, long-term effects are incalculable. Although a downed website or a service interruption can be extremely costly, loss of brand reputation can be economically disastrous and require years to recover. Customers are very likely to switch to competitors if their credit card information, passwords or other personal data have been compromised due to a security breach.

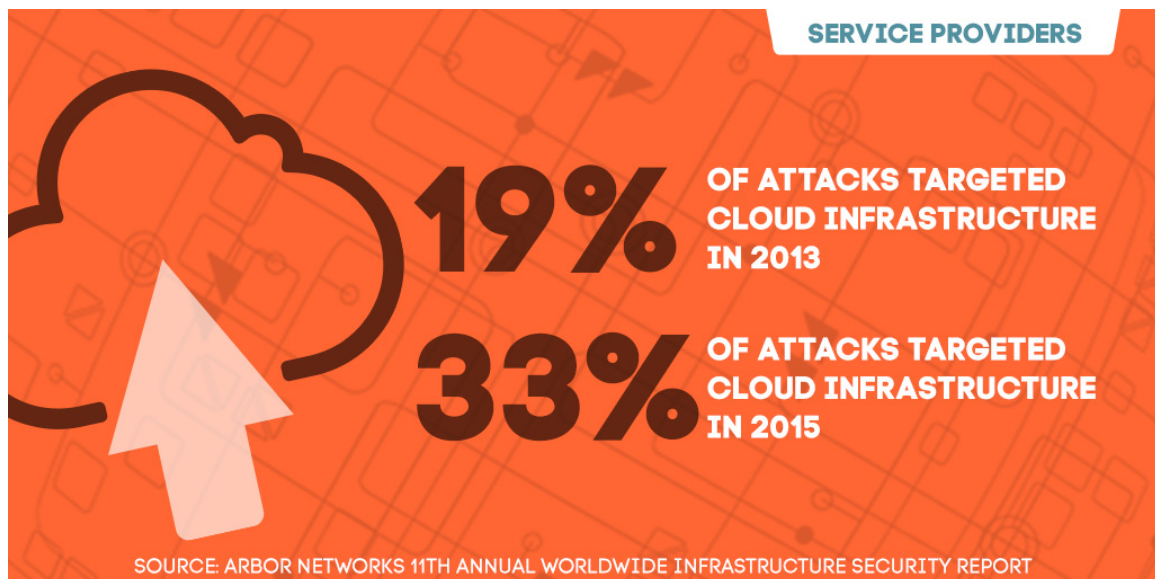
# STAYING SAFE IN CYBER SPACE

## DISTRIBUTED DENIAL OF SERVICE ATTACKS

### – INSIGHTS AND SOLUTIONS

### IT EVOLUTION INVITES THREAT

As the communication and IT landscapes evolve, they also open up new avenues for security breaches. In the excitement of implementing new technologies, businesses often overlook their potential to invite attacks. Many companies are today investing in virtualization and cloud applications and allow their employees to bring their own devices. Yet this distribution of resources results in a much more complex protection scenario while increasing the number of entry points for attackers. This is just one reason why it is more and more important to develop a tailored defense solution that exactly matches specific organizational requirements in order to proactively defend assets.

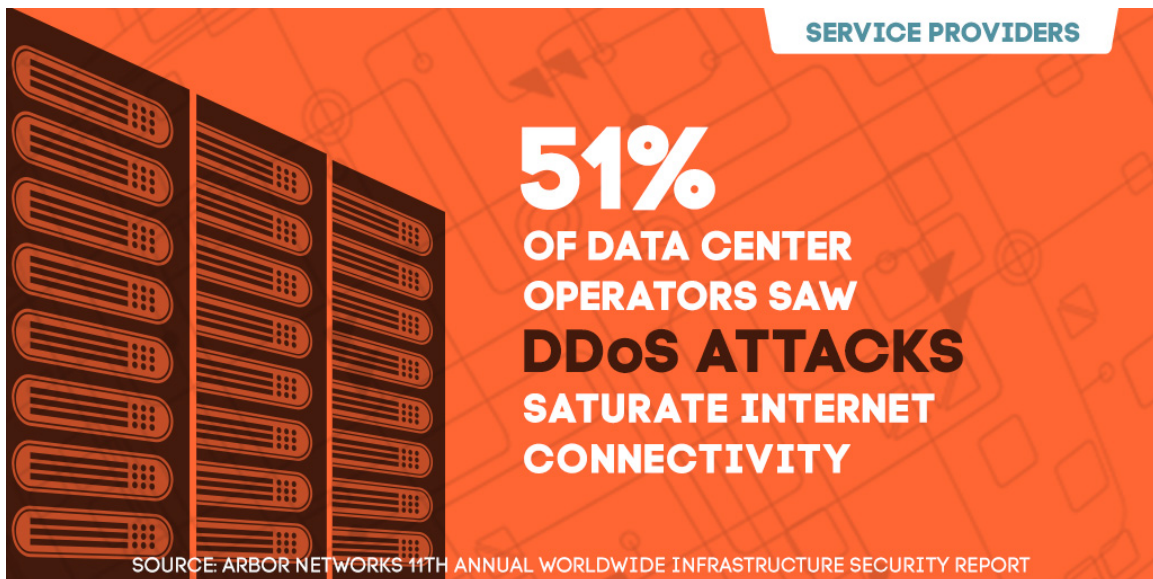


# STAYING SAFE IN CYBER SPACE

## DISTRIBUTED DENIAL OF SERVICE ATTACKS – INSIGHTS AND SOLUTIONS

### WHY READ FURTHER?

This white paper will provide both general background information about DDoS attacks and afford a technical overview on how they work. It will also examine how DDoS assaults have and will continue to evolve, and discuss why traditional defense systems are no longer effective. To cope with the ever-rising threat of security breaches, modern approaches must be implemented. Deutsche Telekom's DDoS defense solutions not only help contain an attack, they are also able to identify an assault exactly when it starts through real-time analysis. By implementing new and sophisticated technologies, your organization can realize substantial benefits that will protect your customer's resources and employees.





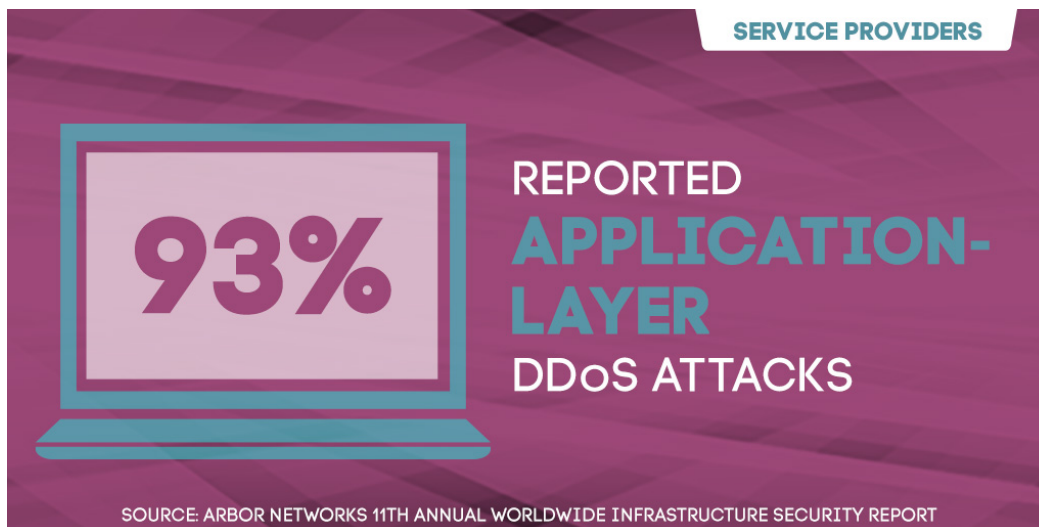
## THE CHANGING LANDSCAPE OF DDOS ATTACKS

### NEW METHODS OF ATTACK

Today, the main types of attacks are either volume or application based – or a combination of both. However, just as the internet is in a constant state of growth and adaptation, so the methods used for DDoS attacks continue to evolve. Assaults have not only grown in size, frequency and sophistication; they have also become much harder to detect and mitigate.

### MULTI-VECTOR ATTACKS

While the number of volumetric attacks has decreased, their strength has significantly increased, with levels over 100 Gbps not uncommon. In fact, in 2015 the largest confirmed attack was a massive 500 Gbps. However, even more complex and difficult to combat is the increasing use of multi-vector attacks. These are simultaneous strikes against both the network layer (OSI Layers 3 and 4) where volumetric attacks occur, and the application layer (OSI Layer 7) where, as the name implies, application attacks transpire.



Multi-vector attacks can use a wide variety of techniques. A recent attack that occurred in Europe, for example, showed a combination of six different vectors. Those included DNS reflection and UDP fragmentation, as well as SYN, PUSH, TCP and UDP floods. While this was an extremely widespread hit, attackers often use multi-vector attacks to lure victims into concentrating mitigation efforts on one area while simultaneously launching an unnoticed attack on more data-sensitive regions.

It's very easy, for example, to send a volumetric DDoS attack that a company's IT team works on fixing, while also transmitting an application layer attack called a 'state exhaustion' to crash the firewall or IPS in the network. In a desperate attempt to get connectivity back, the IT team bypasses the failing firewall, leaving the doors wide open for the attacker to infiltrate the network with malware.

# **STAYING SAFE IN CYBER SPACE**

## DISTRIBUTED DENIAL OF SERVICE ATTACKS – INSIGHTS AND SOLUTIONS

### **CHANGING CRIMINAL INCENTIVES**

Another change that has come about is the motivation of hackers. In the past, criminals were mostly concerned with financial gain. Their goal was to extort money from businesses, often holding websites “to ransom” until a specified amount was paid. Others were simply malicious wrongdoers who wanted to see if they could cause damage to their targets.

Today, the stimulus for many cyber criminals is to propagate their personal beliefs or ideologies. These so-called “hacktivists” have gone after banking structures or governmental institutions in a vigilante style. They believe they are helping to undermine social conventions or business systems they consider to be corrupt or immoral. Volunteers have even been known to offer their PCs as one of the foot soldiers in a botnet army. One of the most publicized attacks involving this sort of activism occurred in Estonia in 2007. What ensued was a series of wide-reaching and innovative reforms that has resulted in the country’s ability to systematically secure its internet infrastructure.

### **EASIER ACCESS TO ILLEGAL TOOLS**

Cyber criminality has become simpler to carry out. This is partly due to the proliferation of black market offerings, with cyber thugs selling botnet creation kits for less than 20 US dollars or even renting out a complete botnet solution. In addition, the upsurge in open source software tools has made the development of attack applications easier. One example is Low Orbit Ion Cannon (LOIC). It started as an open source device to test network stress, but was then modified by hackers to start life anew as an attack tool.

### **MORE OPPORTUNITIES**

To understand how attacks have and will continue to develop, it’s important to understand the way the internet has changed. There has been exponential growth over the last decade in the amount of people using the internet as well as the number of ways in which the internet is used. We have come to rely on the internet for many basic tasks, such as banking, communication and entertainment. This alone has provided greater opportunities for cyber thieves to create online havoc.

In addition, telecommunication providers are migrating to all-IP networks, in order to take advantage of opportunities offered by quality and performance enhancements. However, this move also opens carriers up to an increase in security breaches due to the more extensive and open distribution of their environments. This is another reason why it is increasingly important to take proactive, real-time measures to defend against DDoS attacks.

# **STAYING SAFE IN CYBER SPACE**

## **DISTRIBUTED DENIAL OF SERVICE ATTACKS**

### **– INSIGHTS AND SOLUTIONS**

#### **SMART DEVICES AND DDOS ATTACKS**

To make our lives easier, smart devices, the Internet of Things and machine-to-machine modules have now entered our homes, cars and workplaces. Unfortunately, these have often been neglected as potential sources of botnet infection. Smart devices have their own IP addresses, are connected to the internet and are sometimes in direct communication with a user's other devices.

At the same time, smart devices are not very sophisticated, have limited user interfaces and typically possess none of the usual security tools normally found on a PC. These deficiencies make it possible for scenarios to arise that sound like science fiction. For example, a hacker could infiltrate a user's home heating control unit, using it as a bot to disrupt the navigation service of the user's car. Or, by using a host of these internet-capable devices, a widespread attack could be launched against a financial institution.

#### **ASSAULT ON ESTONIA**

In April 2007, the Baltic state of Estonia experienced what has been called the world's first cyber war. Prior to that date, the country had made significant inroads into the areas of information technology and telecommunications. In 2007, Estonia was considered by many to be the most wired country in Europe, with citizens relying on the internet for many everyday tasks such as online banking, filing taxes and voting online. This dependence on the internet also made the country an extremely vulnerable target.

The attacks are believed to have been started as a protest against the government's plans to remove a Soviet war monument that was erected in 1947<sup>3</sup>. The political situation in the country had already been intense, with a large division between ethnic Estonians and Russians living within the country. The first discovery of the attack occurred when the Minister of Defense found he could not reach the Prime Minister's website. Soon other governmental sites were targeted, and the attacks rapidly spread to media sites, the Estonian banking system and Estonian universities.

To mitigate the attacks, all incoming international traffic to endangered sites was blocked. This led to many media and government websites being completely cut off from the rest of the world, with international communications limited to telephone and fax. After deeper analysis of traffic, more precise blocks were implemented and traffic again became manageable within a little over two weeks. Although serious accusations were leveled at the time, to this day the identity of the attackers is not clear. As with the majority of DDoS attacks, it is extremely difficult if not impossible to ascertain the culprits.

The cyber assault on Estonia's internet infrastructure was a decisive element in shaping the country's future e-strategy. Today, Estonia has become a true e-state, with massive transformations in the weaponry used to fight cyber crime.

---

3 International Affairs Review, April 4, 2009, <http://www.iar-gwu.org/node/65>

# **STAYING SAFE IN CYBER SPACE**

## **DISTRIBUTED DENIAL OF SERVICE ATTACKS**

### **– INSIGHTS AND SOLUTIONS**

#### **SECRET CYBER WEAPONS OF AN E-STATE**

The Republic of Estonia is one of the world's most advanced countries in terms of digital connectivity, for private as well as business use. In fact, Estonia calls itself an e-state, one that uses IT for almost all segments of governmental administration – such as allowing its citizens to vote from their homes or report taxes during a few online minutes. This reliance on an overarching IT structure necessitates a strong cyber security agenda.

“Our secret weapon is people,” asserts Anto Veldre, an analyst at Estonia's Information System Authority. He revealed that all of the country's information security professionals personally meet throughout the year and have formed a community to monitor potential attacks. If an attack is discovered, those in the group – individuals from banks, private industry and government offices – work together to repel the assault. They make up what Veldre calls a “secondary communication channel” to ensure that information during an attack keeps flowing so that corrective action can be quickly taken.

Estonia's remedial response consists of coordinating the individual skills within the community in order to analyze where the attack originated and to identify the opponent. Veldre says this is necessary so that a prediction can be made about the attacker's capabilities and objectives. Only then is it possible to decide what defensive steps should be taken. For example, a small attack with little potential for growth can be handled by the target alone, but if it saturates the network, providers must get involved.

Another way to keep data out of unsanctioned hands is through transparency, according to Taavi Kotka, Estonia's CIO in the Ministry of Economic Affairs and Communications. He calls transparency “the key to a digital society” and maintains that it provides security because it is always possible to see who accessed files as well as when and how it was done. Estonia has adopted strict rules regarding who can retrieve data and under what conditions. That means that if someone has illegally breached information, that fact is immediately discovered.

Decentralized infrastructure is also one of Estonia's foremost methods of defense against DDoS attacks. To that end, Estonia has initiated a communication system between databases called X-road. The key to its defense mechanism is that there is no central database to steal. Each organization – government offices, police authorities or hospitals – maintains its own original data. Therefore, if there has been a leak, the affected party can continue operations because only one copy would have been taken. The X-road initiative has in fact been such a success that Estonia was asked by neighboring Finland to help set up a version of the system in their country. Besides working autonomously within their respective borders, Finland and Estonia are cooperating to digitally connect both countries by the autumn of 2016.

# STAYING SAFE IN CYBER SPACE

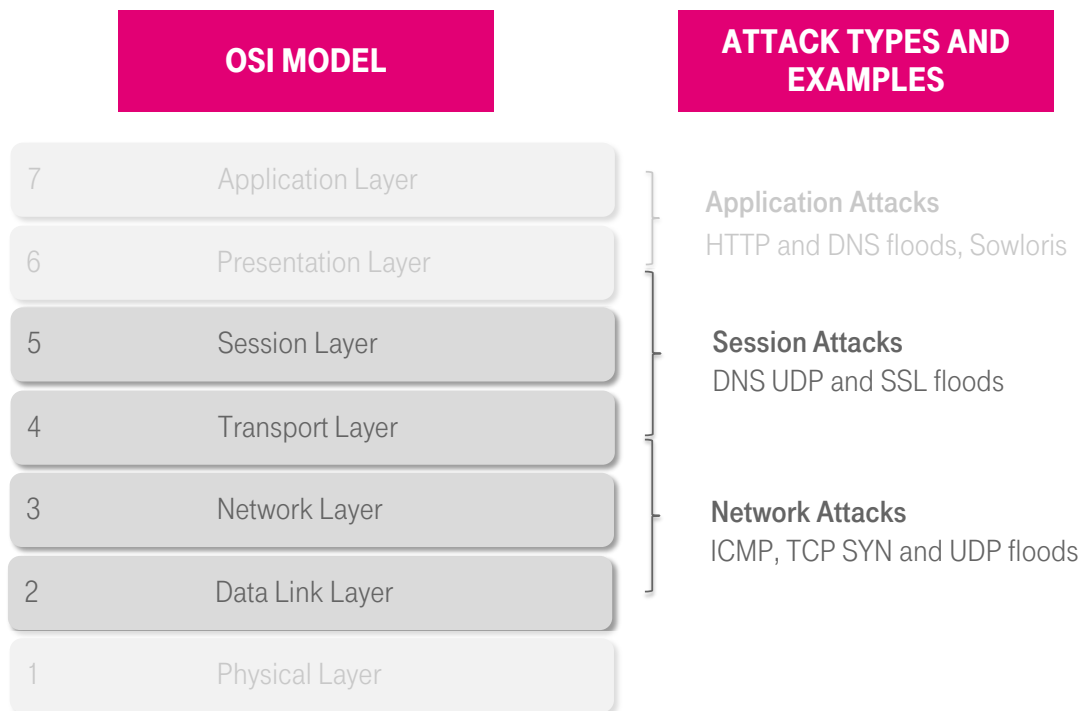
## DISTRIBUTED DENIAL OF SERVICE ATTACKS – INSIGHTS AND SOLUTIONS

### A DEEPER LOOK AT DDoS

To better understand why DDoS is a crucial topic for business security, it's important to be aware of the variety of forms it can take and how these cause damage. The following is an overview of some of the most popular methods of attack.

### VOLUMETRIC ATTACKS

One common type of attack depends on brute force, which works by completely flooding a targeted network with traffic and saturating the available bandwidth. This is characterized as a volumetric attack on the network and transport layers of the Open System Interconnection (OSI) model. In this scenario hackers overload the victim's resource capabilities within minutes, thus degrading service or even rendering the target completely inaccessible for legitimate users. Several types of these volumetric attacks on OSI Layers 3 and 4 include ICMP, TCP SYN and UDP floods.



# **STAYING SAFE IN CYBER SPACE**

## **DISTRIBUTED DENIAL OF SERVICE ATTACKS**

### **- INSIGHTS AND SOLUTIONS**

#### **ICMP FLOOD**

An ICMP (Internet Control Message Protocol) is a diagnostic and error reporting utility that forms an integral part of any IP implementation. Routers and network devices use it to send messages to other devices in the form of IP packets. These communicate faults and difficulties, such as sending notification that the originating devices cannot be reached for delivery. An ICMP attack occurs when an attacker intentionally floods the host with IP packets bigger than its capacity. As an attempt is made to respond, capacity is overloaded and the system fails.

#### **TCP SYN FLOOD**

A TCP SYN flood works by exploiting the design of the Transmission Control Protocol (TCP). This common protocol for email and web based services makes it a readily available target, as well as one that is relatively simple to attack. A TCP connection relies on the "3-way handshake" of the SYN-ACK (synchronize-acknowledgement) messaging system. Basically, a request comes in and remains in a received state until the legitimacy of the inquiry has been verified. To keep the connection open, attackers utilize source IP addresses that cannot be confirmed. When verification is unable to be established, the received state requests begin to back up and eventually deluge the system.

#### **UDP FLOOD**

The user datagram protocol (UDP) is a computer networking protocol used to transmit messages on an IP network without prior setup or acknowledgement of receipt. The advantage lies in its speed, and it is useful for situations where error detection is necessary but validation is not. As is the case with an ICMP flood, an attacker sends numerous UDP packets that the victim attempts to answer but cannot, thus congesting the system. An effective way of generating very large UDP floods is to use a technique called DNS amplification.

#### **DOMAIN NAME SYSTEM (DNS) AMPLIFICATION ATTACKS**

Attackers have been able to easily exploit DNS, which was not established with security in mind but for reliability. Whenever a user types a domain name into a browser, the Domain Name System goes into action to find that domain by translating it into an IP address – all those numbers with dots between. The DNS servers look up the domain in their cache. If it is not found, the request goes on to the next server and the next until it is found.

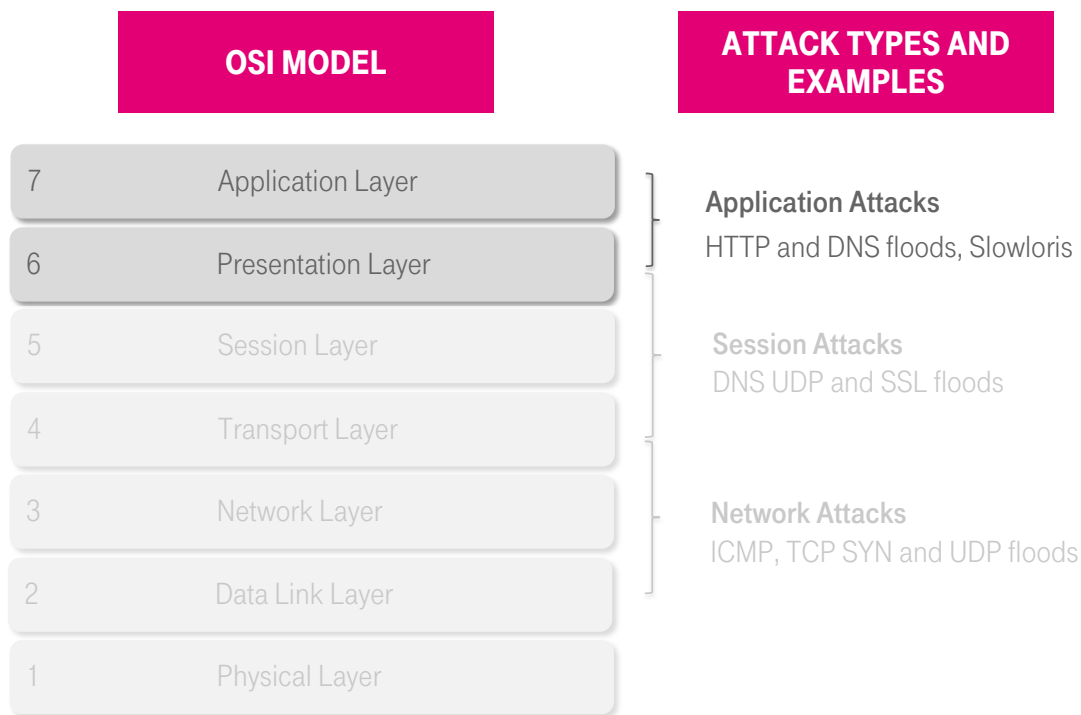
A DNS attack exploits the vulnerabilities of the DNS infrastructure, which implements both UDP and TCP depending on the task that needs to be accomplished. There are several different attack methods. One is by spoofing the address of their target instead of sending the request from their own IP address. This causes the DNS server to respond to the spoofed address (target of the attack). The DNS response however can be up to 70 times larger than the initial request, thereby amplifying the attack size. By utilizing a botnet, responses to these queries can inundate the target and leave it incapacitated. This technique is solely responsible for the very large attack sizes we see today that are often over 100G and have reached 500G.

# STAYING SAFE IN CYBER SPACE

## DISTRIBUTED DENIAL OF SERVICE ATTACKS – INSIGHTS AND SOLUTIONS

### APPLICATION LAYER ATTACKS

An application layer DDoS attack is an assault on Layer 7 of the OSI model, which supports end-user functions such as web browsers and email services. In contrast to brute force or volumetric attacks, application layer attacks are much more sophisticated and effective in that they aim to drain vital web resources instead of overwhelming the target. In these types of attacks, it is the application itself that denies service instead of the host, as in OSI Layer 3 and 4 attacks.



Another characteristic of application layer attacks is that they appear as legitimate transactions and are thus able to better deceive DDoS defense mechanisms. This also makes them difficult to mitigate without blocking access to legitimate users. Attacks on OSI Layer 7 often have low bitrates and involve applications such as Hypertext Transfer Protocol (HTTP) or Domain Name Systems (DNS).

### HTTP GET AND HTTP POST FLOODS

HTTP facilitates communication between clients and servers, for example between a web browser and a server. Two common methods for this type of request-response protocol are GET and POST. GET asks for data such as images or scripts to be retrieved from a specific resource, while POST submits data that should be processed to a specific resource. The attacker's goal with these strikes is to flood the server with so many requests that its resources are simply overwhelmed by being forced to respond to every request.

# STAYING SAFE IN CYBER SPACE

## DISTRIBUTED DENIAL OF SERVICE ATTACKS – INSIGHTS AND SOLUTIONS

### DOMAIN NAME SYSTEM (DNS) ATTACKS

A DNS cache spoofing attack exploits the vulnerabilities of the DNS infrastructure, which has been mentioned previously. Attackers can spoof or poison DNS responses to redirect all inbound queries to any server they choose and, because the users believe they are on the legitimate website, collect sensitive information such as passwords and credit card data.

### ATTACK TOOLS

According to Arbor Networks 2016 Worldwide Infrastructure Security Report<sup>4</sup>, the number, scale, complexity and costs of DDoS attacks continue to grow. In fact, a whopping one-third of respondents experienced DDoS attacks over the last 12 months. Arbor Networks also reported that 51% of data center operators had experienced DDoS attacks that completely saturated their internet connectivity.

As attack methods have become more refined they have also become more dangerous and costly. Multi-vector attacks – a combination of volumetric, TCP flood and application layer attacks – are an example of more sophisticated approaches. Often a first attack on the 3rd and 4th OSI layers is only a diversion meant to distract from a larger assault on the application layer, using tools such as Low Orbit Ion Cannon (LOIC) and Slowloris.

### LOW ORBIT ION CANNON (LOIC)

LOIC was originally developed as an open-source diagnostic application for testing network stress. However, after being released into the public domain, it was modified by criminal minds to perform DDoS attacks. It works by generating high amounts of traffic that flood a target with TCP, UDP OR HTTP packets. By using the “Hive Mind” mode, an attacker can connect a copy of LOIC to an Internet Relay Chat (IRC) channel and thus use thousands of these copies on many devices to strike a target.

LOIC has been widely used by the hacker group Anonymous. However, since it does not disguise its users’ IP addresses by default, some people who volunteered their devices for use as bots were identified and arrested. This has led to a reduction in its use and is a possible reason for the development by Anonymous of High Orbit Ion Cannon, a successor application that needs fewer devices for an attack of the same strength.

### SLOWLORIS

What we’re talking about here are not the primates with large, wide-open eyes that hang around trees in Southeast Asia, although that is where its name comes from. Slowloris is a DDoS tool that attempts to keep as many connections to the target server open as possible, thus blocking access for legitimate users. True to its name, Slowloris works by sending requests in very small portions as slowly as possible, which forces the server to wait until the next portion arrives. In this way, Slowloris does not require a huge amount of traffic or a lot of bandwidth.

---

4 Worldwide Infrastructure Security Report Volume XI, Arbor Networks



# STAYING SAFE IN CYBER SPACE

## DISTRIBUTED DENIAL OF SERVICE ATTACKS

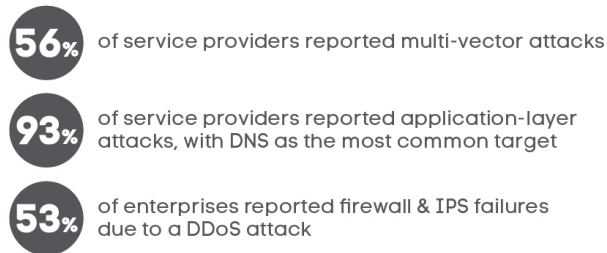
### – INSIGHTS AND SOLUTIONS

## TRADITIONAL DEFENSE PRODUCTS NO LONGER EFFECTIVE

The most commonly used types of defense against cyber criminality have been firewalls, Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS). Unfortunately, these methods alone will not protect systems against the wiles of modern-day DDoS attackers and are now often the target of attacks themselves.

## WITH COMPLEX ATTACKS ON THE RISE

Existing Infrastructure is Not Enough



## FIREWALLS

A simple explanation of how firewalls work is that they monitor the state of network connections that pass through them, such as source and destination IP addresses, and store this information in a memory table called a 'state table'. Any data packet within the pre-screened memory will be allowed through, while recognized threats and patterns will be blocked. However if an attacker sends large numbers of these sessions to a firewall, the state table can fill up. Once full, it will either deny new sessions or often will just crash under the load. Either way, a firewall is often the first inline device between the internet and all the internet facing services the enterprise has, so if it fails or stops accepting new connections, everything behind it is now disconnected from the internet.

## INTRUSION DETECTION AND PREVENTION SYSTEMS (IDS AND IPS)

As the names imply, an Intrusion Detection System (IDS) discovers malicious attempts to attack a system or network, while an Intrusion Prevention System (IPS) blocks those attempts. These devices are usually implemented together with firewalls. They work by retaining and screening a database that holds patterns of malicious attacks, abnormal behavior as defined by administrators, and/or pre-configured security policies. Any identified anomalies in the network are denied access. Because of their reliance on processing power and memory, their resources can be easily exhausted when encountering DDoS application layer attacks. In addition, since they only detect threats that are in their memory, newly devised ones (zero day) can readily slip through.

# STAYING SAFE IN CYBER SPACE

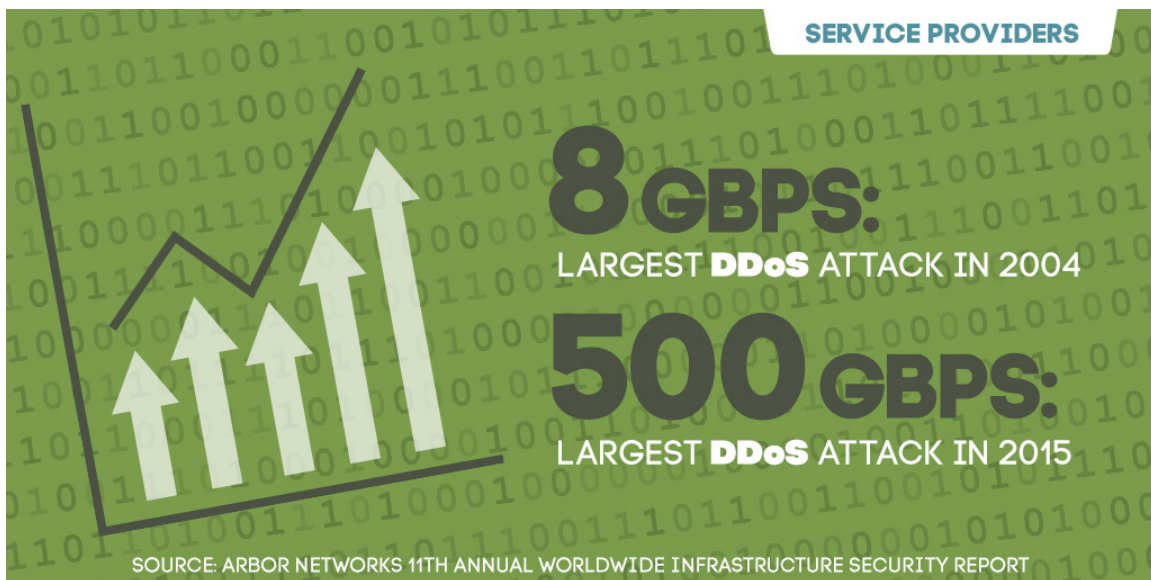
## DISTRIBUTED DENIAL OF SERVICE ATTACKS

### – INSIGHTS AND SOLUTIONS

## STRATEGIES FOR DEFENSE AGAINST DDoS ATTACKS

Modern-day DDoS attacks increasingly consist of a combination of volumetric and application layer vectors, making them more difficult than ever to combat. Adding to the problem is the fact that assaults are growing in both size and complexity. For these reasons, effective countermeasures must take a tiered approach, with on-premise as well as cloud or backbone protection. Only with a wholly integrated service from specialized providers is it possible to stop today's multi-vector DDoS attacks.

According to the Arbor Networks Worldwide Infrastructure Security Report 2016, over one-third of the service providers, enterprises, and government and educational institutions surveyed<sup>5</sup> experienced DDoS attacks over the last 12 months. Of those, nearly one-quarter suffered attacks over 100 Gbps, a significant increase over the previous 12 months. Application layer attacks were also on the rise, from 86% in 2013 to a current 93%. However, most problematic was the upsurge in multi-vector attacks, which escalated to 56% in 2015.




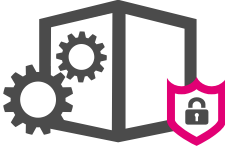
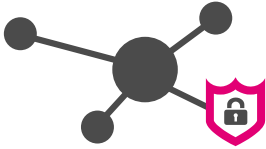
5 52% service providers, 38% enterprise organizations, 6% government, 4% education

# STAYING SAFE IN CYBER SPACE

## DISTRIBUTED DENIAL OF SERVICE ATTACKS - INSIGHTS AND SOLUTIONS

### DEUTSCHE TELEKOM SOLUTIONS

In partnership with the security experts at Arbor Networks, Deutsche Telekom offers a layered DDoS security strategy that can handle even the most severe assault scenarios. For massive volumetric attacks, the only viable answer is backbone protection or a cloud solution. This is because perimeter-based protections can only block attacks that do not exceed the capacity of the internet connection, and gearing up to stop modern-day volumes would be financially unrealistic. Defense systems on customer premises are, however, equally imperative, as application layer attacks should be stopped close to where applications reside and moreover are not detected by cloud-based solutions. This layered approach to DDoS protection is now well understood by the industry as the best common practice, with many vendors and industry analysts supporting this approach.

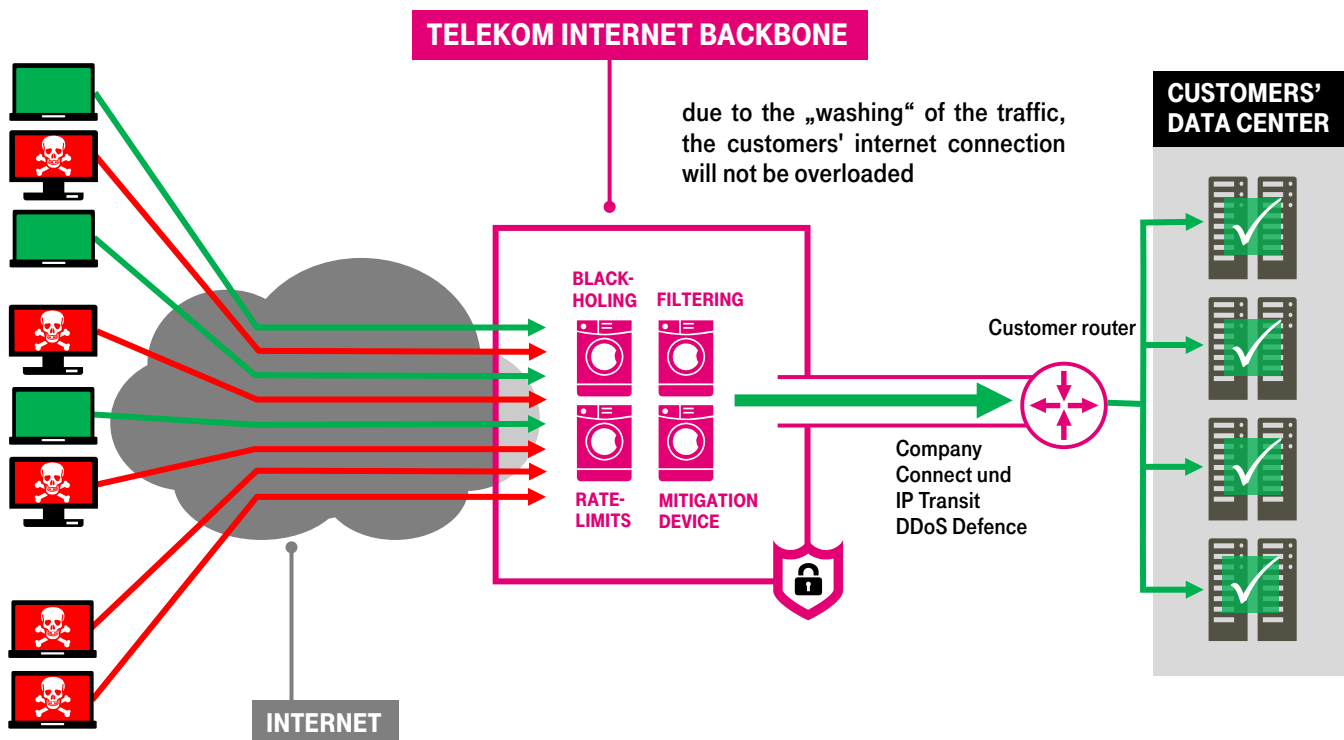
CLOUD DDOS PROTECTION	ON PREMISES DDOS PROTECTION	BACKBONE DDOS PROTECTION
		
High-end protection against complex volumetric attacks	Sophisticated protection against smart (Layer 7) DDoS attacks	High-end protection against complex volumetric attacks
Over 2 Tbps of global and redundant mitigation capacity	Complex targeted attacks on systems and applications	For attacks on networks and bandwidth
For global companies, organizations that have multiple internet providers	Local always-on protection	For companies that have Deutsche Telekom as an internet service provider

# STAYING SAFE IN CYBER SPACE

## DISTRIBUTED DENIAL OF SERVICE ATTACKS – INSIGHTS AND SOLUTIONS

### BACKBONE PROTECTION FROM DEUTSCHE TELEKOM

DDoS Defense is an IP backbone defense solution offered by Deutsche Telekom for its business internet access and IP Transit customers. It protects against volumetric DDoS attacks that are routed via Deutsche Telekom to the customer's network. With a transparent reporting and management system, DDoS Defense spots attacks in advance so they can be stopped before causing damage. When discovered, traffic is rerouted to Deutsche Telekom's security farm and filtered with defense tools from Arbor Networks. This backbone protection should, however, be considered only a first, initial step toward mitigating attacks as it will not react in real time to application layer attacks. Hence the need for a layered approach.



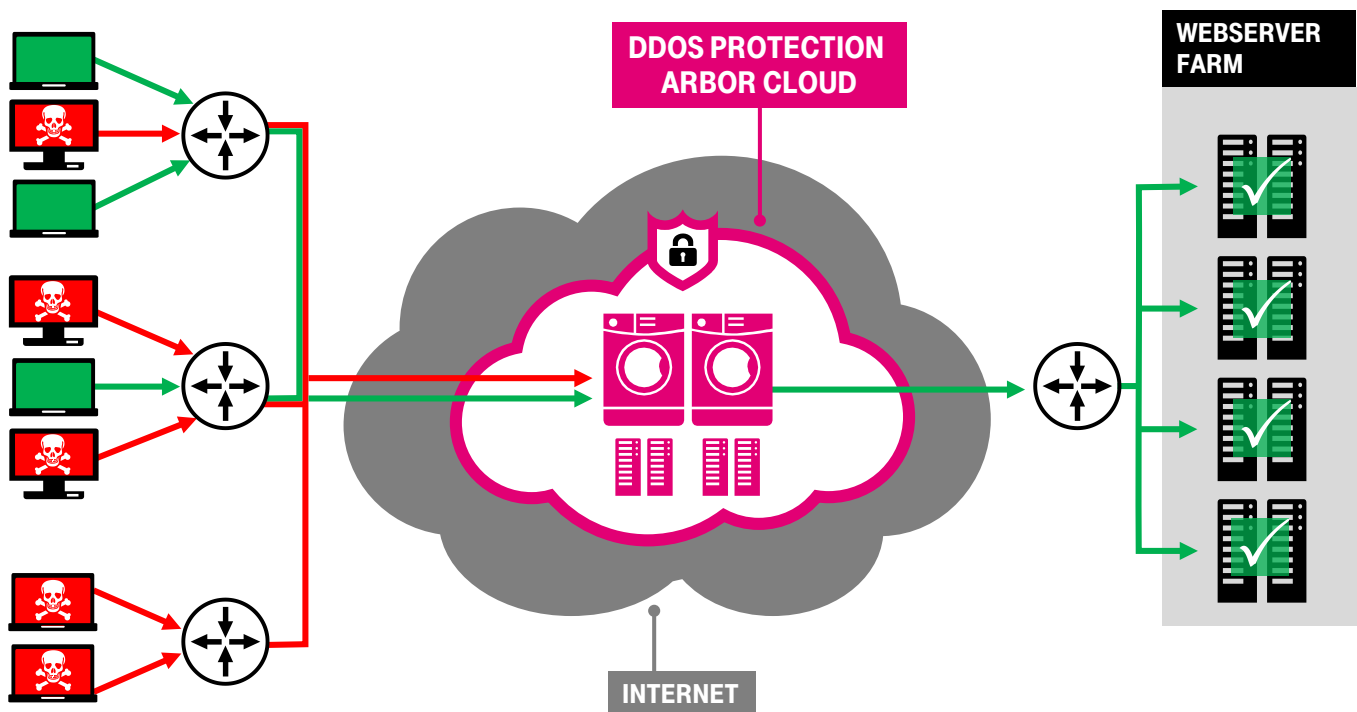
# STAYING SAFE IN CYBER SPACE

## DISTRIBUTED DENIAL OF SERVICE ATTACKS – INSIGHTS AND SOLUTIONS

### CLOUD PROTECTION FROM DEUTSCHE TELEKOM

Deutsche Telekom additionally offers an Arbor Networks-based cloud solution with over 2 Tbps of global and redundant mitigation capacity. This solution reroutes traffic to Arbor Networks four (expanding to eight in 2016) global scrubbing centers for immediate cleaning. Clean traffic is then quickly sent back to the client via a GRE tunnel. As this solution is ISP agnostic, it can be implemented by any organization regardless of their current provider. This makes it ideal for organizations with distributed global presence or with multiple upstream internet providers, that want a single unified solution.

Due to the ANYCAST model of the scrubbing centers, if anyone were to fail, traffic would dynamically be sent on to the other centers. For maximum reliability, every location implements multiple 40 Gbps mitigation devices. With the centers certified as carrier class, the cloud platform's SLA for availability is 99.999%, a figure that would be difficult for other providers to replicate.



# STAYING SAFE IN CYBER SPACE

## DISTRIBUTED DENIAL OF SERVICE ATTACKS

### – INSIGHTS AND SOLUTIONS

#### ON-PREMISE SOLUTIONS FROM DEUTSCHE TELEKOM

Deutsche Telekom offers a range of on-premise solutions developed to fit every need, including virtualized. Local protection is the only method for blocking demanding application layer and state exhaustion attacks. These solutions are always on and therefore ensure real-time and automatic protection. They work by identifying and blocking targeted attacks using local intelligence and a centralized, DDoS-specific data feed that is updated hourly. However, on-premise devices are only truly effective in combination with cloud mechanisms that can handle the large volumetric components of the attack.

One of the on-premise products offered by Deutsche Telekom is the Availability Protection System (APS). This is an always-on appliance or virtual platform for in-line detection and mitigation of application layer and low-bandwidth volumetric attacks up to the client's access bandwidth (500M to 10G per link). It implements a stateless analysis filtering engine, which means it is not burdened with the heavy processing weight of stateful inspection, e.g., firewalls and IPS. Therefore, APS easily detects smaller volume attacks and can also effectively analyze threats and detect patterns that can be used to establish future defense capabilities.

However, due to the nature and variety of DDoS, it is crucial to build a protection solution that is customized to the specific needs of your organization. It isn't enough to just capture perceived dangerous packets. A successful solution must be able to differentiate between good and bad traffic patterns and only block the latter without impacting legitimate traffic. This is why it's important to work with a provider such as Deutsche Telekom, which is able to intelligently identify where an attack is coming from and predict how it could evolve.

#### BENEFITS OF THE DEUTSCHE TELEKOM'S DDOS DEFENSE SOLUTIONS

By utilizing Deutsche Telekom protection solutions, customers have access to the company's specialist intelligence and research capabilities, such as the "DTAG Community Honeypot Project." With the support of partners, Deutsche Telekom has positioned sensors across the globe to capture data and provide an overview of current cyber attacks. This data is made available to the public on the website [www.sicherheitstacho.de](http://www.sicherheitstacho.de), with observed threats visualized over a world map and/or charts that react in real time. The result is a transparent, global view of DDoS attacks that provides information necessary to stop ongoing attacks and predict future events.

With Deutsche Telekom's advanced monitoring systems, it is possible to detect when clients' devices have been infected. When that occurs, the company immediately sends an email or letter to the client and directs them to the website [www.botfrei.de](http://www.botfrei.de). This is an anti-botnet advisory center, of which Deutsche Telekom is a participating partner. Botfrei gives instructions on how to mitigate security problems and offers a hotline for difficult-to-solve cases. The gravity of the problem can be illustrated by the fact that Deutsche Telekom sends up to forty thousand notifications of infection to clients every month.

# **STAYING SAFE IN CYBER SPACE**

## DISTRIBUTED DENIAL OF SERVICE ATTACKS – INSIGHTS AND SOLUTIONS

An additional asset for customers is Arbor Networks ongoing work to help protect the internet from attacks. The company operates a global threat analysis system, similar to the one from Deutsche Telekom, called ATLAS. This is an international network consisting of Arbor Networks experts and customers that amass and share data about traffic flow and attacks they are seeing. The result is a timely and detailed analysis of how DDoS is evolving around the world.

Arbor Networks also has a dedicated security research organization named ASERT (Arbor Security Engineering and Response Team), which has developed a very large malware platform that is recognized as the global authority in finding, reversing and stopping DDoS-focused malware toolkits. These patented DDoS defense technologies along with the know-how and backing of Deutsche Telekom, offer customers a complete package that effectively detects threats and delivers solutions that are clear, decisive and powerful.

### **MANY SOURCES OF PROTECTION FROM DEUTSCHE TELEKOM**

To defend against high-volume attacks, Deutsche Telekom offers two solutions. Existing clients with only Deutsche Telekom as a provider can take advantage of the company's backbone protection solution. However, some enterprises have more than one provider and need the simplicity of protection from a single source. In this case, the cloud protection provides the perfect answer for current as well as new customers.

To handle application attacks, however, the best common practice endorsed by experts globally is to implement on-premise devices that can statelessly protect your internet assets in real time. As attacks today increasingly make use of a combination of volumetric and application layers, the most effective defense system consists of on-premise devices combined with backbone or cloud protection.

DDoS attacks are on the increase, with no end in sight. That's why, no matter which solutions are chosen, a customized strategy will provide the best possible defense. Every business has special requirements as well as distinctive weak points that need to be taken into account when planning defense mechanisms. No organization can afford to wait until it is faced with a ransom attack, theft of sensitive data or a complete blockage of services.

**STAYING SAFE IN CYBER SPACE**  
DISTRIBUTED DENIAL OF SERVICE ATTACKS  
– INSIGHTS AND SOLUTIONS

**ANY QUESTIONS?**

For more information, see  
[www.telekom-icss.com/ddosdefense](http://www.telekom-icss.com/ddosdefense)

**PUBLISHED BY**

Deutsche Telekom AG  
International Carrier Sales & Solutions (ICSS)  
Friedrich-Ebert-Allee 71-77  
D-53113 Bonn, Germany



**LIFE IS FOR SHARING.**