KASPERSKY lab

Protecting your business against financial and reputational losses with Kaspersky DDoS Protection

A Distributed Denial of Service (DDoS) attack is one of the most popular weapons in the cybercriminals' arsenal. It aims to make information systems such as websites or databases impossible for regular users to access normally. There can be different motives behind launching DDoS attacks, ranging from cyber-hooliganism to dirty tricks campaigns by competitors or even extortion. Any network node available in the Internet may become a target, be it a specific server, a network device or a disused address in the victim's sub-network.

There are two common scenarios for conducting DDoS attacks: sending requests directly to the attacked resource from a large number of bots, or launching a DDoS amplification attack through publicly available servers containing software vulnerabilities.

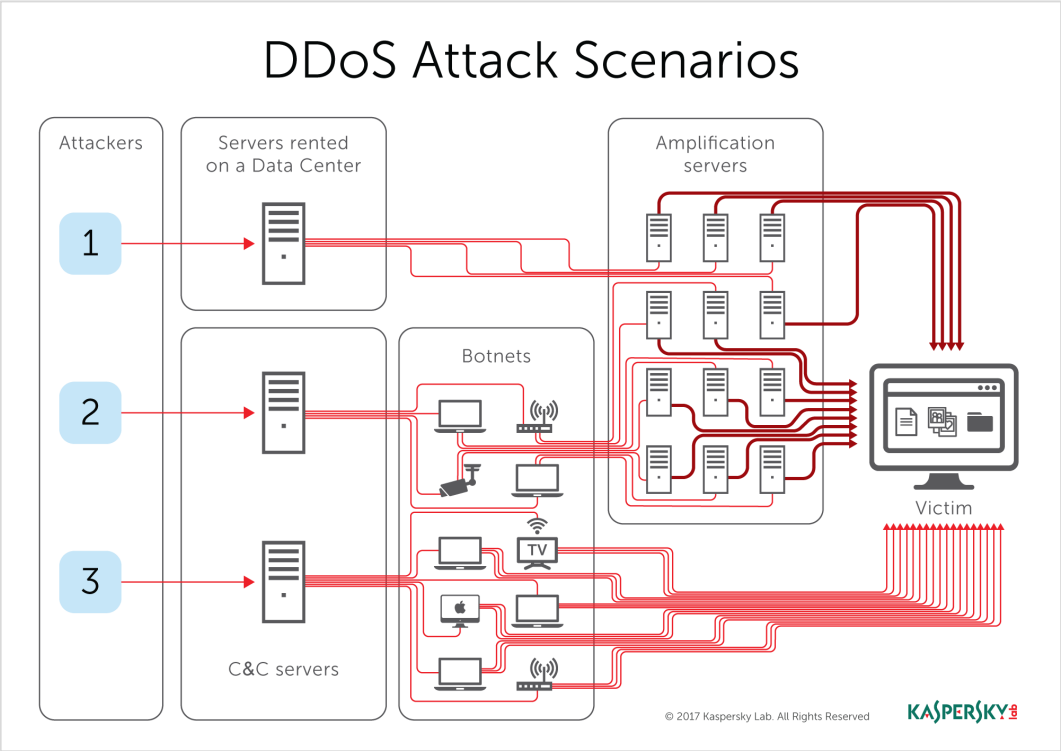

Figure 1. Flow diagram of most popular versions of DDoS attacks

In the first scenario, cybercriminals turn a multitude of computers, servers, IoT devices, etc. into remotely controlled "zombies" which then follow the master's command and simultaneously send requests to the victim's computing system (conducting a "distributed attack"). Sometimes, a group of users is recruited by hacktivists to do their dirty work. They are provided with special software designed to conduct DDoS attacks and then given orders to attack a target.

Under the second scenario involving an amplification attack, servers leased out from a data center can be used instead of bots. Public servers with vulnerable software are typically used for enhancement. Today, either DNS (domain name system) servers or NTP (network time protocol) servers can be used. In some cases, instead of vulnerable servers, cybercriminals can use sites created using WordPress CMS (usually blogs) with the Pingback function enabled. An attack is amplified by spoofing return IP addresses and sending a short request

to a server or website that requires a much longer response. The received response is sent to the spoofed IP address which belongs to the victim.

Counting the costs

There is another factor that makes the situation even more dangerous. The sheer amount of malware out there and vulnerable IoT devices and servers, which can be used by cybercriminals to create botnets or make DNS amplification attacks, means that almost anybody can launch this kind of attack. Cybercriminals advertise their services claiming that they can take down a specified site for just $50 a day. The low cost and relative ease of the attack makes it both attractive to those wanting to take down a site and profitable for those carrying out the attack. With payments typically made in cryptocurrency, it is almost impossible to track the orders through transaction flows.

Affordable prices mean that any online resource can be targeted in a DDoS attack – not just large, well-known organizations. Although it is generally more difficult to cause damage to the web-resources of large companies, if they are made unavailable, the cost of that downtime will be much greater. In addition to the direct losses resulting from missed business opportunities (such as online sales), companies which fall victim to DDoS attacks can face fines for defaulting on their obligations or expenses relating to extra measures to protect themselves from further attack. Reputation may also be damaged as a result of attack, causing companies to lose existing or future clients.

The total cost to a business depends on its size, the industry segment it serves and the type of service under attack. According to calculations by Kaspersky Lab and B2B International, the average cost of a DDoS attack can be about $106,000 for smaller companies and more than $1.6 million for enterprises, but there are reports that a single DDoS attack has cost a business $160 million.

Methods of countering DDoS attacks

With monetary and reputational damage at stake, businesses need to ensure they have robust protection in place to stop them from becoming the next victim. There are three main methods of protecting against DDoS attacks: (1) install special appliances in the company's information infrastructure, (2) use capabilities provided by the ISP and (3) enlist an anti-DDoS service provider to clean traffic from DDoS requests. No matter which approach you take, they all follow the same principle of filtering out the junk traffic (i.e. traffic created by cybercriminals). However, despite being built on the same underlying method, each one has differing degrees of success.

Installing filtering equipment or a firewall on the company's side is considered to be the least effective method. Firstly, it requires specially trained personnel within the company to regularly service the equipment and adjust its operation, creating extra costs and resource requirements. Secondly, it is only effective against attacks on the service, and does nothing to prevent attacks choking the Internet channel. A working service is of no use if it cannot be

accessed from the net. Due to amplified DDoS attacks and attacks using a large number of vulnerable IoT devices, it is very easy to overload a connection channel. Thirdly, built-in hardware is also not effective against 'smart' DDoS attacks, which are hard to filter with standard methods.

Relying on the Internet service provider to filter the traffic is more reliable, as there is a broader Internet channel which is much harder to clog up. However, ISPs are not specialists in security services and, as a result, only filter out the most obvious junk traffic, overlooking more subtle attacks, such as those that use encryption or imitate user behavior. Careful analysis of an attack and a prompt response require appropriate expertise and experience. Using protection provided by the ISP makes the client dependent on a specific provider and creates difficulties if the client needs to use a backup data channel or to change its provider.

The only way to fully neutralize DDoS attacks is to work with **an anti-DDoS service provider** who has its own scrubbing centers implementing a combination of various traffic filtration methods to catch and kill any attacks.

Kaspersky DDoS Protection

Kaspersky DDoS Protection safeguards against all types of DDoS attacks. The solution combines different methods.

Kaspersky Lab's arsenal

The first element of Kaspersky DDoS Protection is our **experts**. For 20 years, Kaspersky Lab has successfully dealt with a wide range of online threats. Over that time, our analysts have acquired a unique level of expertise, including a detailed understanding of how DDoS attacks work. The company's experts constantly watch the latest developments taking hold on the Internet, analyze current methods of conducting cyber-attacks, and improve existing protection tools to keep up with the pace. With this expertise at hand, it is possible to detect a DDoS attack as soon as it is launched and before it floods the target web resource. The solution can also modify filtration rules during the attacks if needed, to keep it effective even against the most sophisticated attacking methods.

The second element is a **sensor**, either installed in Kaspersky DDoS Protection cloud or at customer premises. It analyzes the traffic which goes to the client's resource: the types of protocols used, the number of bytes and data packets sent, the visitor's behavior on the client's website (i.e. the metadata, or information about the sent data). With this information, a statistics-based profile is created for each client. These profiles are records of typical information exchange patterns for each client. Changes in typical times of use are also recorded. Any time the traffic behavior is different from the statistics-based profile it may be indicative of an attack.

Underpinning Kaspersky DDoS Protection is its **scrubbing centers**. These are located in main Internet backbone lines, in places like Frankfurt and Amsterdam. Kaspersky Lab

simultaneously uses several scrubbing centers, so it can divide or redirect the traffic that needs to be cleaned. The processing centers are united into a common cloud-based information infrastructure and the data is processed within these boundaries. For example, the web traffic of European clients does not leave European territory.

The dedicated **emergency team** of Kaspersky Lab experts is available 24/7 to monitor anomalies in the client's traffic so the onset of any attack can be detected as soon as possible, and filters can be modified as required (attackers can change attacking scenarios in order to bypass protection and to disable the resource attacked).

Another key way of controlling DDoS-traffic is to filter it on the **provider side**. The ISP does not just supply an Internet channel, it can also enter a technology partnership with Kaspersky Lab. Thus, Kaspersky DDoS Protection can cut off the most obvious junk traffic, used in the majority of DDoS-attacks, as close to its point of origin as possible. This prevents the streams from merging into a single powerful attack and eases the burden on the scrubbing centers, which are free to handle more sophisticated junk traffic.

One more layer of protection is the **DDoS Intelligence system**. It is designed to intercept and analyze commands sent to bots from command and control (C&C) servers. This system helps Kaspersky Lab experts to gather additional information about DDoS attacks.

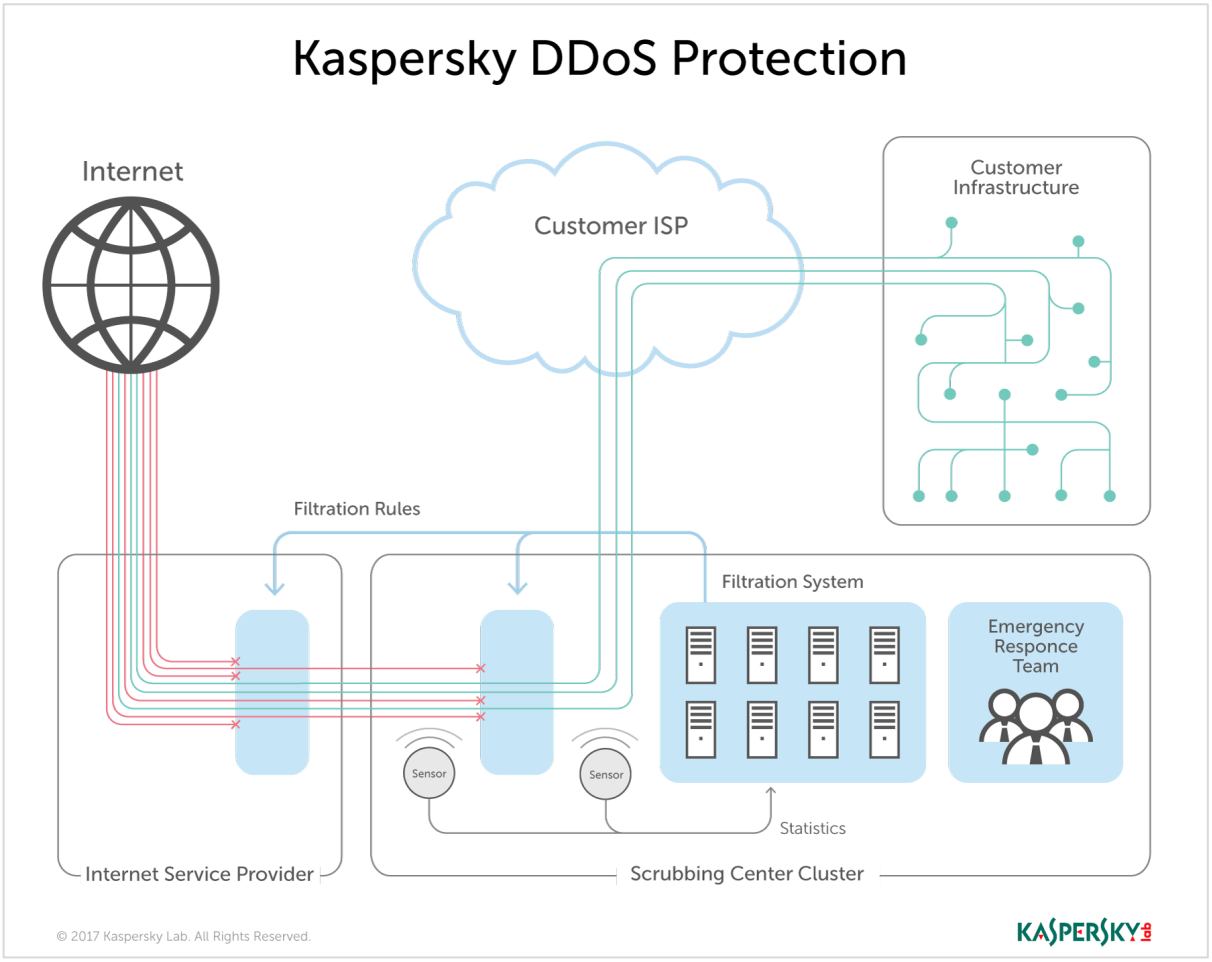

Figure 2. Kaspersky DDoS Protection: Operation Diagram

How it works

Traffic redirection and delivery

There are two types of traffic redirection: on-demand, when traffic routes to scrubbing centers only in the case of attack, and always-on, when traffic goes through scrubbing centers constantly.

The actual traffic redirection can be initiated using one of two methods – by announcing the client's subnet using a BGP dynamic routing protocol, or by modifying the DNS record. The first method requires the client to have an Autonomous System (AS) and an address range that is independent of the provider, such as a block of IP addresses provided by a regional Internet registrar.

There are also several approaches to delivering traffic, which is cleaned up from the junk, back to the client servers. It can be as easy and as fast as via a reverse proxy redirection or routing (through a GRE virtual tunnel or leased line between the scrubbing center and the client's IT infrastructure).

Methods of traffic redirection to the scrubbing center, cleaned traffic delivery and sensor location depend on the type of Kaspersky DDoS Protection chosen by the client:

Type of protection	Traffic redirection	Traffic delivery	Sensor location
Kaspersky DDoS Protection Control	BGP On-Demand	Routing	On premise
Kaspersky DDoS Protection Connect	DNS Always-On	Proxy, routing	In cloud
Kaspersky DDoS Protection Connect+	BGP Always-On	Routing	In cloud

Kaspersky DDoS Protection Control

This method re-routes traffic to the scrubbing centers only in the case of attack, and requires the sensor to be installed in the client's IT infrastructure. The sensor analyzes client's traffic without redirecting it to scrubbing centers.

When the on-duty DDoS expert at Kaspersky Lab receives a signal from the system that traffic arriving to the client does not match the statistical profile and the attack is confirmed, the client is notified of the attack. Client should give the order to redirect the traffic to the scrubbing centers. When the attack is over, traffic is directed back to the client's resources.

The traffic redirection is initiated by announcing the client's subnet using a BGP dynamic routing protocol. Cleaned traffic is delivered to the client site via a virtual tunnel or leased line between the scrubbing center and the client's network equipment.

This method is useful for big companies that do not want the traffic to be redirected to third party servers on a regular basis. They also should have enough resources to install servers with working sensors inside company's infrastructure and to allocate dedicated IT staff to be

on hand 24/7 in order to redirect traffic to Kaspersky Lab's scrubbing centers in the event of an attack.

Kaspersky DDoS Protection Connect

In this case, the sensor is installed within the Kaspersky Lab infrastructure and the client's traffic always goes through the scrubbing centers. It's a fully managed service located in the Kaspersky DDoS Protection cloud and monitored 24/7 by Kaspersky Lab's emergency team. Neither the sensor, nor Kaspersky Lab experts access specific content within the traffic, modify or copy it.

The client replaces the IP address in the DNS A-record with the IP address assigned by the scrubbing center. After this, all traffic arriving at the client's address will be sent to the scrubbing center first. However, to stop the attack on the old IP address continuing, the provider has to block all incoming traffic except data coming from the scrubbing center. The channels, through which the cleaned traffic is delivered to the client, can be arranged according to the Generic Routing Encapsulation (GRE) protocol or via a reverse proxy redirection.

This method is only useful for small companies that have a few IP addresses to be replaced with those of scrubbing centers.

Kaspersky DDoS Protection Connect+

For Kaspersky DDoS Protection Connect+, the sensor is also installed within the Kaspersky Lab infrastructure and the client's traffic always goes through the scrubbing centers. The difference is that the traffic redirection is initiated by announcing the client's subnet using a BGP dynamic routing protocol.

This method is best for big companies, which cannot suffer even a minute of downtime and need anti-DDoS protection to be permanently switched on, but cannot replace all IP addresses as required by Kaspersky DDoS Protection Connect, because have too many of them.

Cleaning process

As soon as Kaspersky Lab's technologies determine the type of the attack, specific cleaning rules are applied for the type of attack and the specific web resource. Some of the rules, designed to treat the crudest type of attacks, are communicated to the provider's infrastructure and applied on routers owned by the provider. The remaining traffic is delivered to the scrubbing center's servers and filtered according to a number of characteristic signs, such as IP addresses, geographical data, information from the HTTP headers, the correctness of protocols and exchange of SYN packets, etc.

The sensor continues to monitor the traffic as it comes to the client. If it still shows signs of a DDoS attack, the sensor alerts the scrubbing center, and the traffic undergoes deep behavior and signature analysis. With these methods, malicious traffic can be filtered out based on

signatures, i.e. a specific type of traffic can be completely blocked, or IP addresses can be blocked based on specific observed criteria. This way, even the most sophisticated attacks are filtered, including an HTTP and HTTPS flood attack. These attacks involve imitations of a user visiting a website, but they are actually chaotic, unnaturally fast, and typically come from a regiment of zombie computers. The use of encryption (HTTPS) makes it more difficult to detect an attack and protect against it because it requires traffic decryption to analyze queries to check whether it's 'clean' or 'junk'.

Kaspersky Lab's experts monitor the entire process using a dedicated interface. If an attack is more complicated than usual or is atypical, the expert may step in, change the filtering rules and reorganize the processes. Clients can also watch how the solution performs and how the traffic behaves, using their own interface.

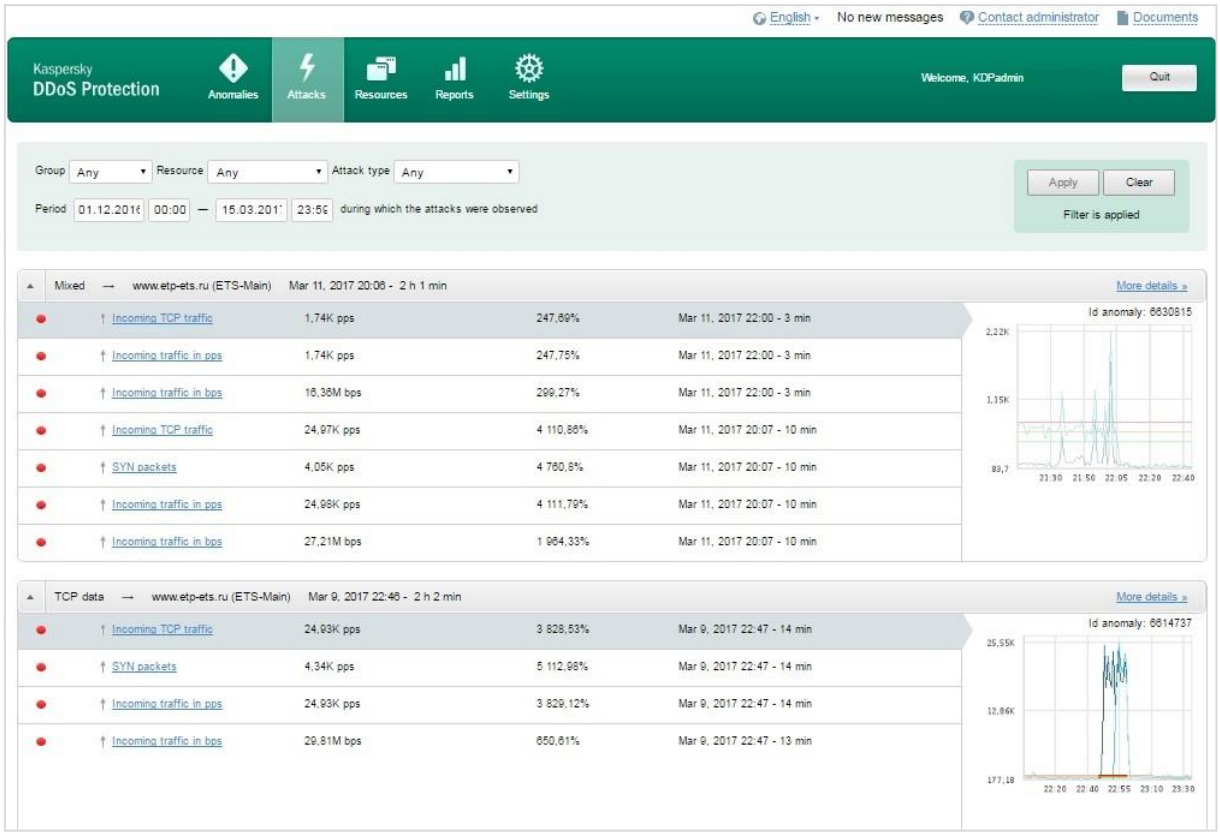

Figure 3. Example of the client's interface

When the attack is over, the client receives a detailed report of the attack, including a detailed account of how it developed, graphs plotting measurable parameters, and the geographical distribution of the attack sources.

Advantages of Kaspersky Lab's approach

- Proven 20-year expertise in researching cyberthreats and combating them worldwide;
- Flexible deployment options with Kaspersky DDoS Protection Control, Connect and Connect+ to address different business, security and network policies;
- Filtration rules are individually developed for each client depending on the specific online business services that need to be protected;
- Emergency Team experts monitor the process and quickly adjust filtration rules when necessary, as well as provide 24/7 support for a client;
- The protective actions can be launched almost immediately, even if a company is under attack and is not yet a Kaspersky Lab client;
- Close cooperation between Kaspersky DDoS Protection experts and Kaspersky Lab developers makes it possible to adapt the solution flexibly and rapidly, in response to changing circumstances;
- Close cooperation with ISPs helps to filter out all types of DDoS attacks – large-scale attacks, 'smart' attacks, IoT botnet attacks, etc.;
- To ensure the highest possible level of reliability, Kaspersky Lab only uses equipment and service suppliers located in European countries;
- Kaspersky Lab has accumulated a wealth of experience applying this technology in Russia, where it successfully protects leading financial institutions, commercial and government agencies, online shops, etc.

To find out more about Kaspersky DDoS Protection, please visit https://www.kaspersky.com/small-to-medium-business-security/ddos-protection.