S3 COMPANY
NEXT GENERATION DATA CENTER

Protection against **DDoS** attacks

www.s3c.bg

What is a **DDoS** attack?

A DDoS attack (Distributed Denial of Service Attack) is a hacker attack that aims to stop or partially delay the services of a given resource (called a victim), making them inaccessible to its target users.

The most common victims are well-known web servers, with the aim being to overload the targeted server or virtual resource, so that it is unable to execute requests from the internet.

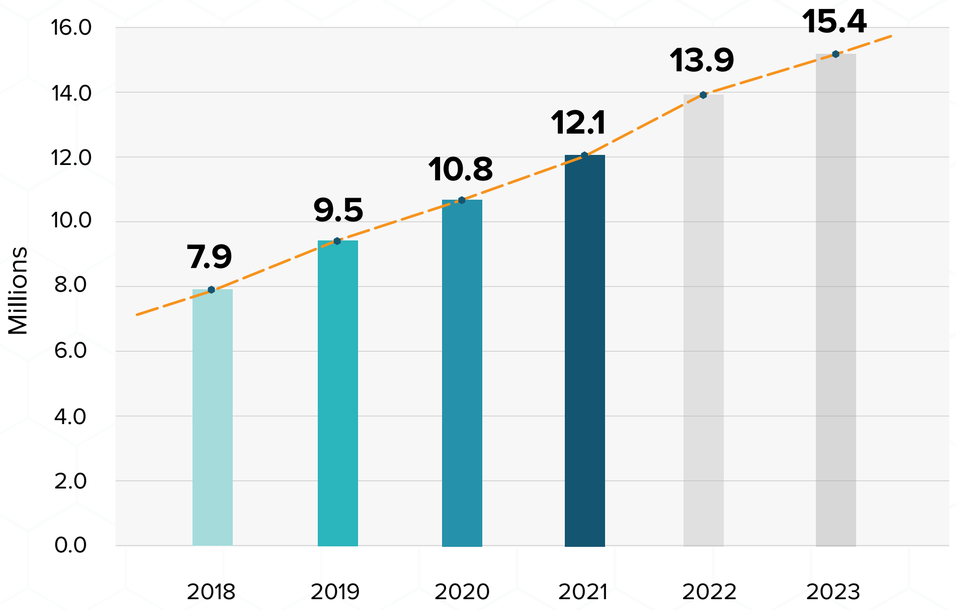
How can that affect your business?

- Financial Losses
- Reputation Crisis
- Loss of Clients

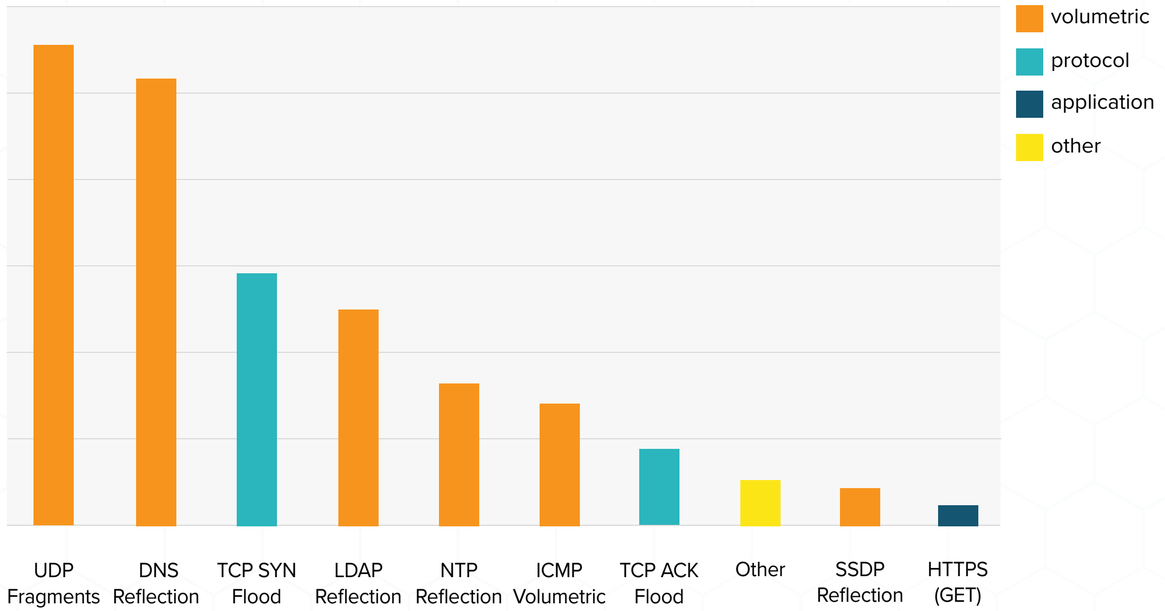
S3 COMPANY
NEXT GENERATION DATA CENTER

www.s3c.bg

Trend in DDoS attacks by year



Distribution of DDoS attack types



S3 COMPANY
NEXT GENERATION DATA CENTER

www.s3c.bg

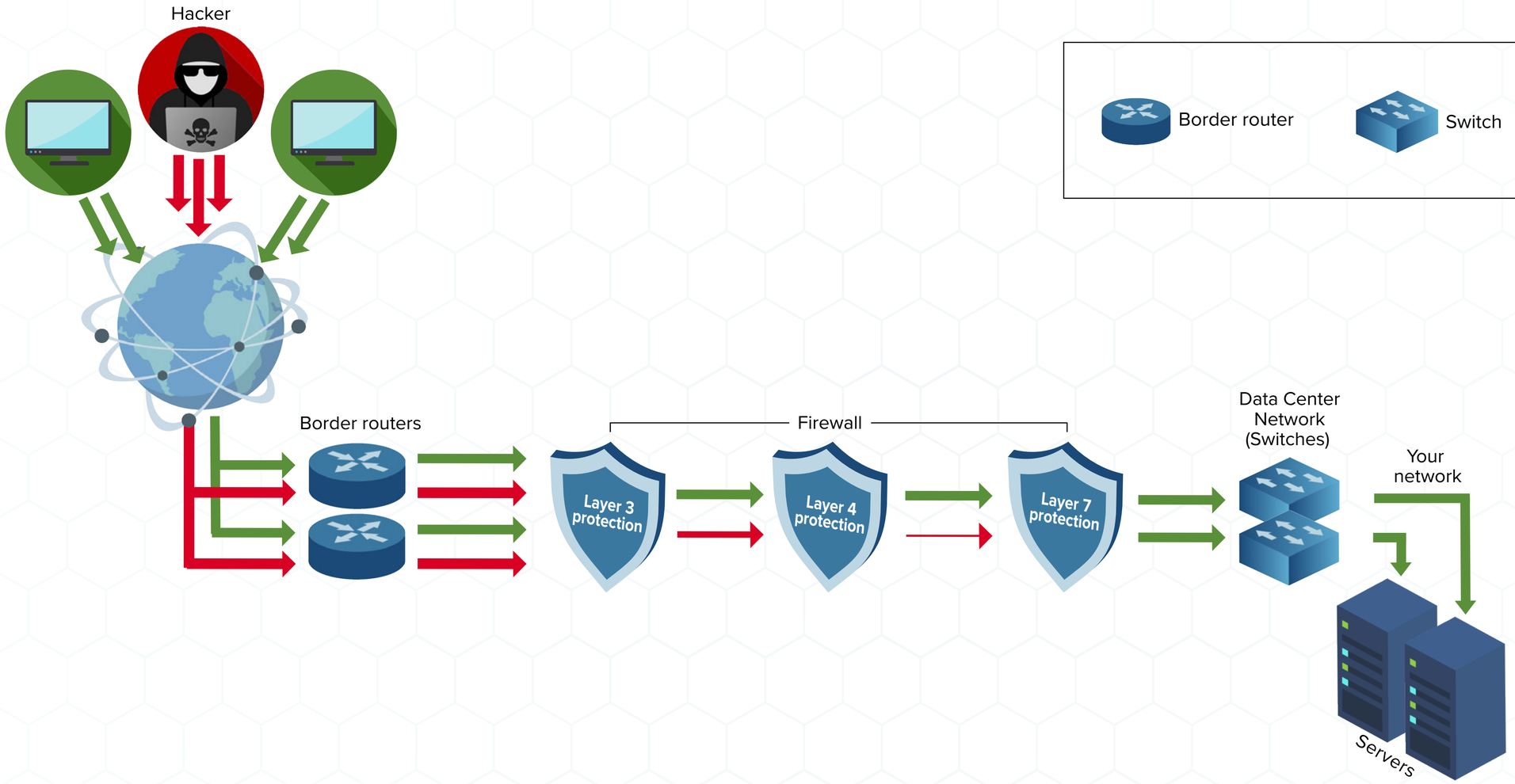
Why choose **S3C**?

- **Own DDoS Protection System**
- We recognize DDoS attacks from the very onset
- Intuitive client Web Portal
- Simple Activation
- Email/SMS Notifications, Charts and Detailed Reports for all Intercepted Attacks
- 24/7 access to a team of service maintenance experts

S3 COMPANY
NEXT GENERATION DATA CENTER

www.s3c.bg

How does our system work?



S3 COMPANY
NEXT GENERATION DATA CENTER

www.s3c.bg

A selection of **DDoS** attacks, that we successfully filter

TCP:

Invalid TCP MSS
Invalid TCP WIN
Invalid TCP SEQ
TCP Statefull check
Fragmented ACK Attack
Booters TCP Flood
TCP SYN+ACK Flood
TCP FIN Flood
TCP RESET Flood
TCP ACK + PSH Flood
TCP Fragments
HTTP Flood
HTTPS Flood
Brute Force
Connection Flood
Low rate attack
Slowloris Flood
Apache Killer
Buffer Overflow Attack
LOIC (Low Orbit Ion Cannon)

UDP:

Booters UDP scripts
Invalid Checksum
Invalid TTL
Invalid Packet size
HPING3 flooder UDP
null packets DNS
Reflection
NTP Reflection SSDP
Reflection MSSQL
Reflection Portmap
Reflection Chargen
Reflection SNMP
Reflection Bittorrent
Reflection Memcached
Reflection TFTP
Reflection
RIP Reflection
LDAP Reflection

OTHER:

IP Spoofed packets
ICMP port unreachable
ICMP flood
Smurf Attack
Ping of Death
Teardrop Attack
SIP Attacks
IPSec Attacks

With each new type of DDoS attack on our client's IP address, different from the ones known so far, we apply filtering to stop malicious traffic. The detected threat is then added automatically for all existing clients.
This protects the entire network and infrastructure from every new type of DDoS attack as soon as it is detected for the first time.

Advantages

- Easy activation without the need to reconfigure your existing equipment
- Consultation and full support before and after the activation of DDoS protection
- Your traffic will never be blackholed!
- Limitless scalability through cluster technology
- Possibility for devices to work on Layer 2 (bridge) and Layer 3 (routing)
- Possibility for 10G / 40G / 100G ports
- Redundancy - High Master-Master type Availability with full replication between devices
- Interactive Web panel for clients, with the ability to change the protection configuration

S3 COMPANY
NEXT GENERATION DATA CENTER

www.s3c.bg

Technical Parameters

- Linux-based systems with a network stack developed by us
- Hardware-accelerated network adapters for raw filtering
- Possibility for two-way and one-way analysis and filtering of traffic
- Fully compatible with RFC specification and parameters
- Stops attacks with a capacity of up to 500 Gbps

S3 COMPANY
NEXT GENERATION DATA CENTER

www.s3c.bg

S3 COMPANY

NEXT GENERATION DATA CENTER

Contact us:

sales@s3c.bg

+359 886 618 006

www.s3c.bg