S3 COMPANY
NEXT GENERATION DATA CENTER

Защита от DDoS атаки

www.s3c.bg

Какво е **DDoS** атака?

DDoS атака (дистрибутирана атака за отказ на услуга)
е хакерска атака, чиято цел е услугите на даден ресурс (наричан жертва), да спрат или частично да се забавят и да станат недостъпни за целевите му потребители.

Най-често биват атакувани популярни уеб сървъри, като целта е да се натовари набелязаният сървър или виртуален ресурс, така че да не може да изпълнява заявки от интернет.

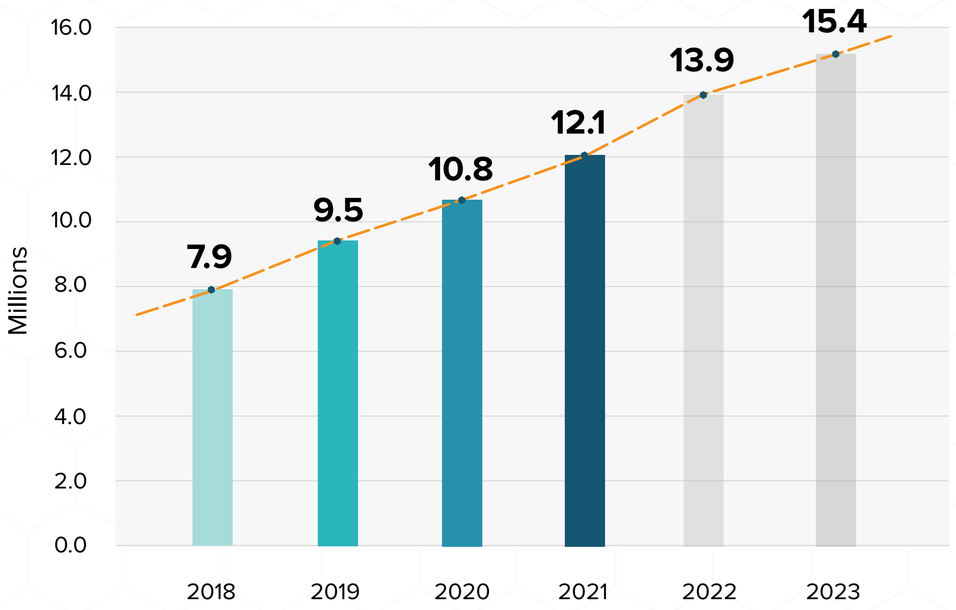
Как може да се отрази това на бизнеса ви?

- Финансови загуби
- Срив на репутацията
- Загуба на клиенти

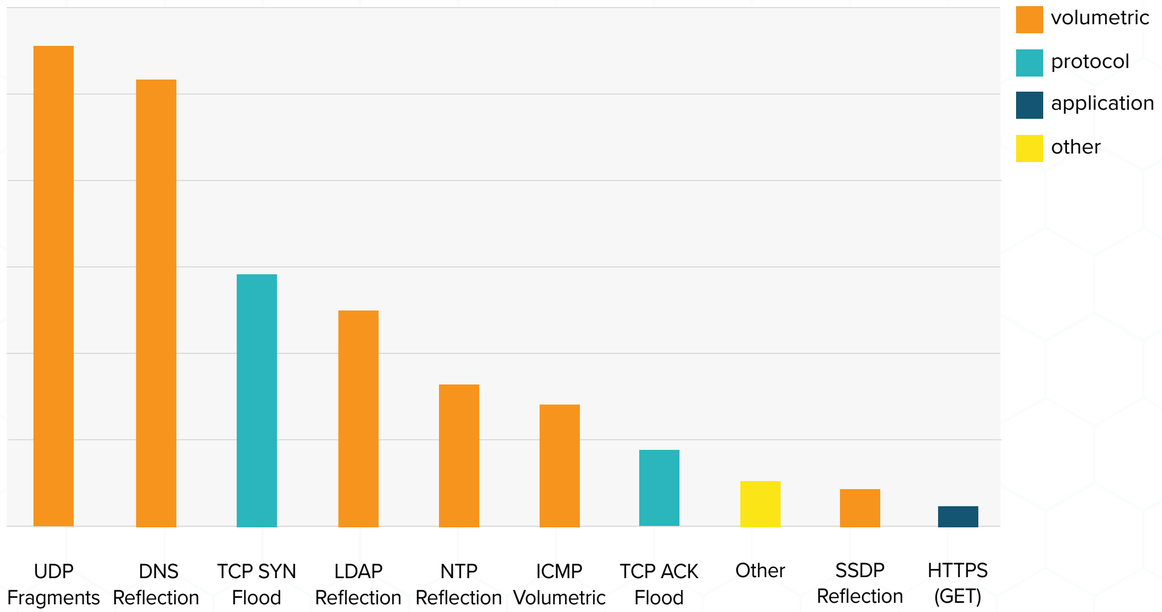
S3 COMPANY
NEXT GENERATION DATA CENTER

www.s3c.bg

Тенденция при DDoS атаките по години



Основни типове DDoS атаки



S3 COMPANY
NEXT GENERATION DATA CENTER

www.s3c.bg

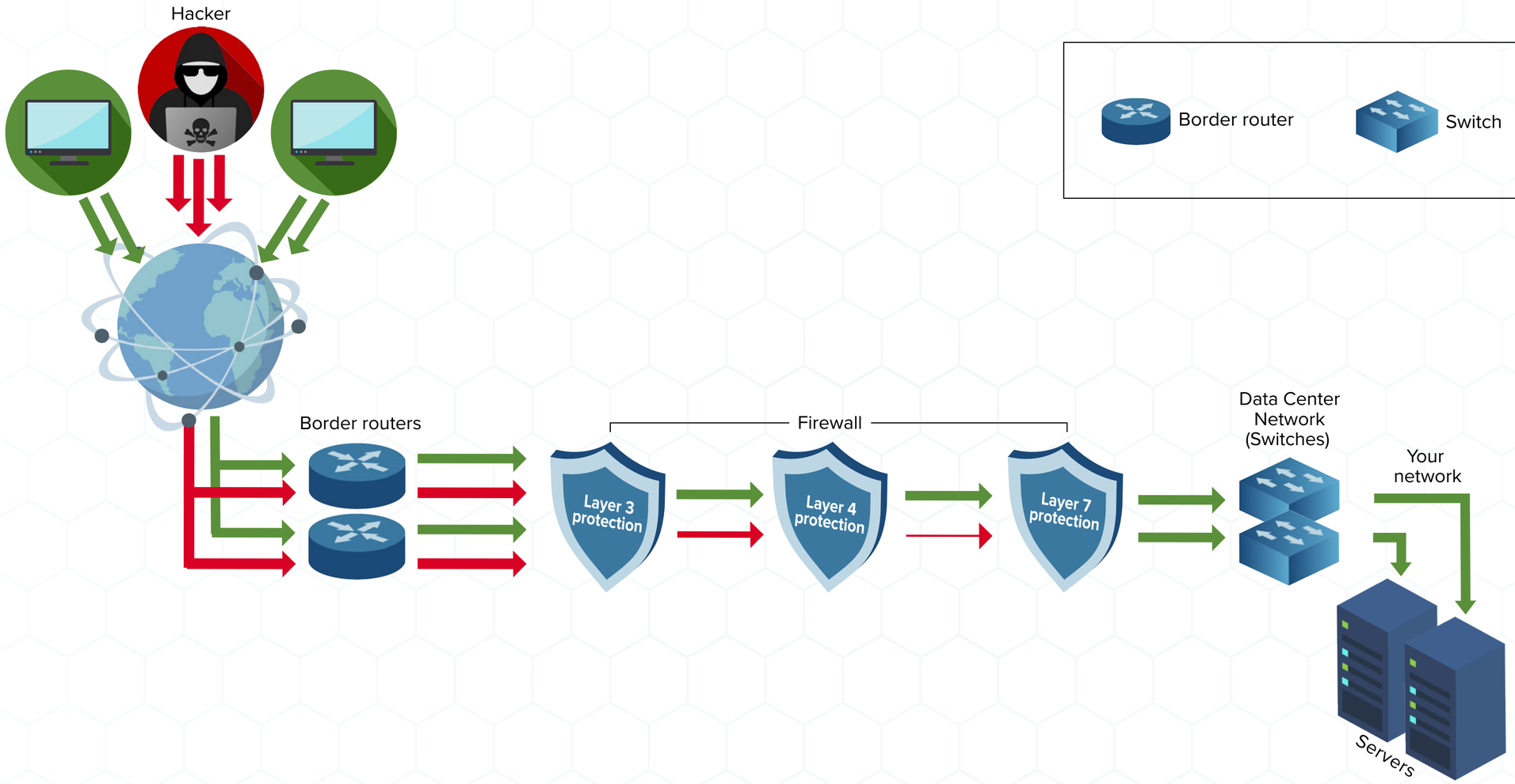
Защо да изберете **S3C**?

- **Собствена система за DDoS защита**
- Познаваме DDoS атаките от самото им зараждане
- Интуитивен клиентски Web портал
- Лесна активация
- Известявания по email/sms, графики и детайлна справка за спрените атаки
- 24/7 екип от специалисти по поддръжка на услугата

S3 COMPANY
NEXT GENERATION DATA CENTER

www.s3c.bg

Как работи нашата система?



S3 COMPANY
NEXT GENERATION DATA CENTER

www.s3c.bg

Част от **DDoS атаките,** които спираме успешно

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

При всеки нов тип DDoS атака към IP адрес на наш клиент, различна от познатите досега, прилагаме филтриране, което да спре зловредния трафик. Нововъведението бива инсталирано автоматично за всички съществуващи клиенти. Така цялата мрежа и инфраструктура е защитена от всякакъв вид нови типове DDoS атаки, веднага след като са засечени за пръв път.

Предимства

- Лесна активация, без нужда от преконфигуриране на наличното ви оборудване
- Консултация и пълна поддръжка преди и след активация на DDoS защитата
- Вашият трафик никога няма да бъде blackhole-нат!
- Безкрайно скалиране чрез клъстър технология
- Възможност за работа на устройствата на Layer 2 (bridge) и Layer 3 (routing)
- Възможност за 10G / 40G / 100G портове
- Резервираност - High Availability, тип Master-Master, с пълна синхронизация между устройствата
- Интерактивен Web панел за клиенти, с възможност за промени по конфигурацията на защитата

S3 COMPANY
NEXT GENERATION DATA CENTER

www.s3c.bg

Технически характеристики

- Linux базирани системи с разработен от нас network stack
- Мрежови адаптери с хардуерно ускорение за raw filterting
- Възможност за двупосочно и еднопосочно анализиране и филтриране на трафика
- Напълно съвместим с RFC дизайна и параметрите
- Спира атаки с капацитет до 500 Gbps

S3 COMPANY
NEXT GENERATION DATA CENTER

www.s3c.bg

S3 COMPANY

NEXT GENERATION DATA CENTER

Контакти:

sales@s3c.bg

+359 886 618 006

www.s3c.bg