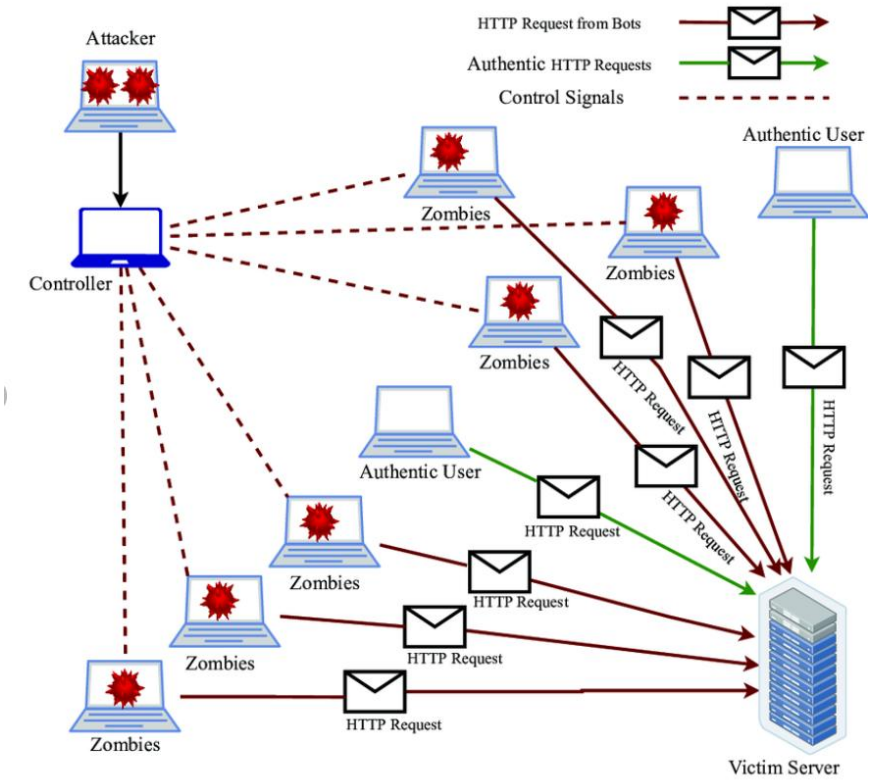


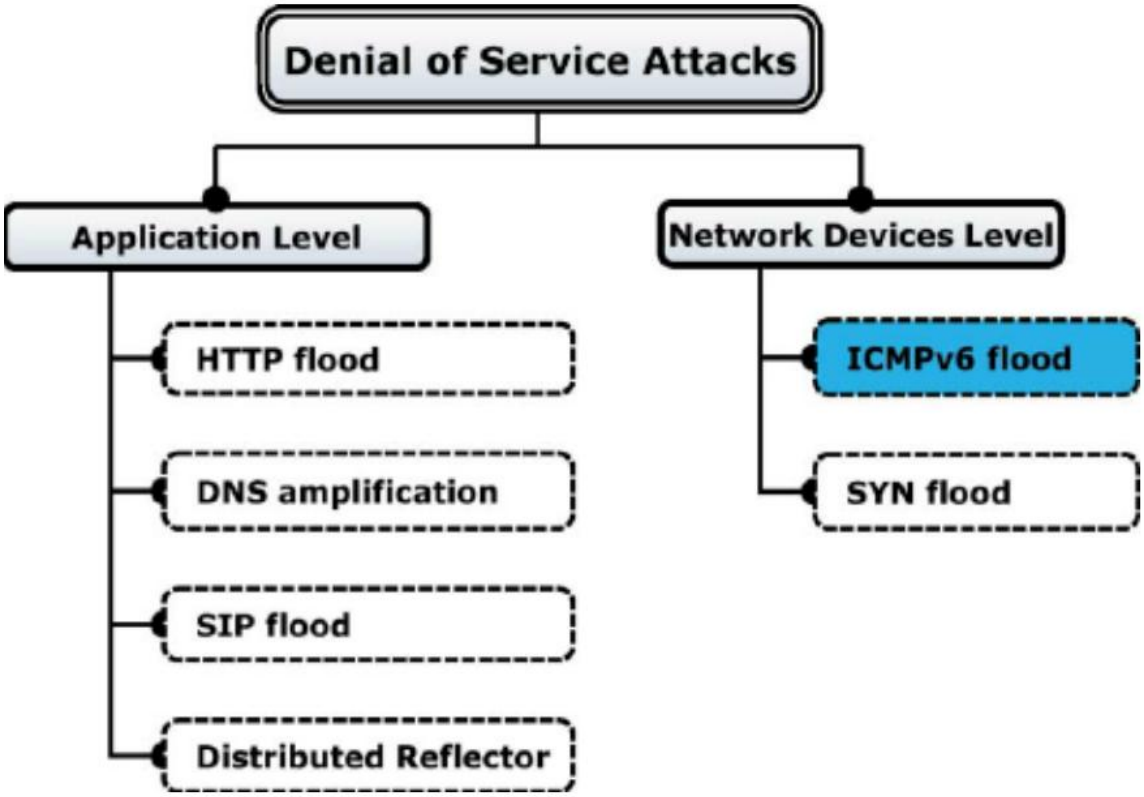

**DDoS** атаката означава Разпределена атака за отказ на услуга.

Това е вид кибератака, при която нападателите използват голям брой устройства (обикновено компрометирани компютри, наречени "ботове" или "ботнети") за да затруднят или напълно блокират достъпа до онлайн услуги или уебсайтове.




*Семантична диаграма на ДДОС атака*

*Източник:* Schematic diagram of a DDoS attack. | Download Scientific Diagram




*Класификация на ДДОС атака*

*Източник:* Classi fi cation of DDoS attacks. | Download Scientific Diagram

## I. Класифициране на ДДОС атаките

Дистрибутираните откази на услуга са атаки, които целят да направят онлайн услуги недостъпни, като ги претоварват с трафик от множество източници. Професионално класифицирането на ДДОС атаките може да се извърши въз основа на различни критерии като методи на атаките, цели, и техния тип на изпълнение. Ето как може да се подходи към тяхната класификация:

### 1. Според методите на атака

- **Обемни атаки (Volume-Based Attacks)**: Тези атаки се характеризират с изпращане на голямо количество трафик към целевата система, за да се изчерпа нейната пропускателна способност и да се прекрати нормалното й функциониране.

**Примери**:

**UDP Flood**: Изпращане на голямо количество пакети UDP (User Datagram Protocol), което претоварва целевата мрежа.

**ICMP Flood (Ping Flood)**: Изпращане на огромен брой ICMP пакети (ping), за да се претовари мрежовото устройство или да се блокират ресурсите му.

- **Протоколни атаки (Protocol-Based Attacks)**: Атаки, които използват уязвимости в мрежовите протоколи, като TCP/IP.

**Примери:**

**SYN Flood**: Атака, при която се изпращат множество SYN заявки, но никога не се изпращат ACK отговори, което изчерпва съществуващите ресурси на сървъра.

**Smurf Attack**: Атака, която използва ICMP пакети, насочени към широки мрежови адреси (broadcast), така че да генерира трафик от множество устройства към целта.

- **Атаки на ниво приложение (Application Layer Attacks)**: Тези атаки целят да претоварят целевия сървър, като изискват обработка на сложни заявки. Те обикновено са по-трудни за откриване.

**Примери:**

**HTTP Flood**: Атака, която изпраща множество HTTP заявки към уебсайта с цел да изчерпа ресурси на сървъра.

**Slowloris**: Атака, при която се изпращат непълни HTTP заявки, така че сървърът да изчерпа всички свои конекции, преди да може да обработи нови заявки.

### 2. Според начините на изпълнение

- **Ботнети (Botnet-Based Attacks)**: Използват се компрометирани устройства (ботове), които извършват атаките координирано. Те могат да бъдат компютри, IoT устройства и други уязвими системи.

Пример: **Mirai Botnet** - ботнет, който използва уязвимости в IoT устройства (като камери и рутери), за да генерира огромен трафик.

- **Атаки от единични източници (Single-Source Attacks)**: Тези атаки идват от един единствен източник. Обикновено те са лесни за откриване и блокиране, но могат да бъдат опасни, ако се използват методи като amplification (умножаване на трафика).

Пример: **DNS Amplification** - атаката използва DNS сървъри, за да генерира трафик, който да бъде изпратен към целта.

### 3. Според целите

- **Нарушаване на достъпа до услуги (Availability Attacks)**: Основната цел е да се прекъсне достъпът на потребителите до дадената онлайн услуга или ресурс. Това е най-често срещаната цел при ДДОС атаките.
- **Целенасочено унищожаване на репутацията (Reputation Attacks)**: В някои случаи, атаката цели не само да направи сайта недостъпен, но и да нанесе щета на репутацията на компанията или организацията.
- **Натиск за изпълнение на изисквания (Extortion DDoS Attacks)**: Извършват се с цел изнудване на организациите да платят определена сума пари, за да избегнат атаката или за да спрат нападението, ако то вече е започнало.

### 4. Според обема на атаката

- **Малки и средни атаки**: Обикновено целят малки или средни бизнеси с ограничен капацитет за защита, като при тези атаки обемът на трафика не е толкова голям.
- **Големи атаки (Large-Scale DDoS Attacks)**: Атаките могат да изискват стотици гигабити на секунда трафик и да претоварят големи глобални мрежи или услуги, като например облачни инфраструктури.

### 5. Според целевата инфраструктура

- **Атаки срещу уеб сървъри и уеб приложения**: Това включва атаки към уебсайтове и онлайн услуги, които използват HTTP/S, както и изпълнението на сложни заявки към сървъри.
- **Атаки срещу мрежова инфраструктура (Network Infrastructure Attacks)**: Целта е да се атакува инфраструктурата на доставчиците на интернет услуги, като рутери, DNS сървъри и шлюзове.

Класифицирането на ДДОС атаките се базира на различни аспекти като тип на атаката, метод на изпълнение, цели и обхват. Това помага на специалистите по киберсигурност да идентифицират и противодействат на заплахите по-ефективно, използвайки правилните техники за защита.

## II. Примери за ДДОС атака:

ДДОС атаките са били използвани в различни случаи и са причинили значителни репутационни и финансови загуби на компании и организации. Ето някои известни примери за ДДОС атаки и какви са били последствията:

### 1. Атаката срещу GitHub (2018)

- **Описание**: През февруари 2018 година GitHub, платформата за хостване на код, стана обект на една от най-големите публично известни ДДОС атаки. Нападателите използваха техника за атака с "Memcached amplification" (усилване чрез Memcached сървъри), при която трафикът се увеличава многократно чрез уязвими сървъри, които отговарят на заявки с големи количества данни.
- **Мащаб**: Трафикът надвишаваше 1.35 Tbps (терабита в секунда), което прави тази атака една от най-големите по размер в историята.
- **Финансови загуби**: Макар GitHub бързо да се възстанови от атаката благодарение на използването на облачни анти-ДДОС услуги, самата атака показва колко скъпо може да стане защитата от такива атаки и какви разходи могат да възникнат за компаниите при опит за възстановяване на услугите.

### 2. Атаката срещу Dyn (2016)

- **Описание**: Dyn, компания за DNS услуги, беше атакувана през октомври 2016 г. Отново се използваха хиляди компрометирани устройства, част от "IoT" мрежа (Интернет на нещата), като IP камери и домашни маршрутизатори. Атаката прекъсна достъпа до популярни сайтове като Twitter, Spotify, Reddit и Netflix.
- **Мащаб**: Атаката засегна десетки милиони потребители в САЩ и по света.
- **Финансови загуби**: Въпреки че не бяха публично оповестени точни финансови загуби, компанията Dyn обяви значителни приходи от клиенти заради прекъсванията на услугата. За компаниите, чиито уебсайтове бяха засегнати, имаше потенциални загуби поради прекъсвания на операциите, намалена продажба или повредена репутация.

### 3. Атаката срещу Cloudflare (2017)

- **Описание**: Cloudflare, доставчик на услуги за защита срещу ДДОС атаки и CDN (Content Delivery Network), беше подложен на огромна атака през 2017

година. Атаката, при която се използва "HTTP flood", също беше извършена с помощта на компрометирани IoT устройства.

- **Мащаб**: Трафикът достигна 2.3 Tbps, което беше рекорден размер по това време.
- **Финансови загуби**: Cloudflare успя да се справи с атаката, но самата атака демонстрира колко тежки могат да бъдат последиците за компаниите, които предлагат услуги за защита от ДДОС, и какви инвестиции в инфраструктура са необходими, за да могат да се справят с такъв мащаб на трафик.

### 4. Атаката срещу Skype (2007)

- **Описание**: През 2007 година Skype беше атакуван чрез серия от ДДОС атаки, които създадоха сериозни проблеми с достъпността на услугата за потребителите. Повечето потребители на Skype не можеха да осъществяват разговори или да влизат в акаунтите си.
- **Мащаб**: Атаката беше ограничена, но имахме огромен брой неуспешни опити за достъп до сървърите на Skype.
- **Финансови загуби**: Skype понесе сериозни щети поради прекъсванията на услугата. Прекъснатите разговори и услуги доведоха до намаляване на приходите от платени абонаменти и реклами.

## III. Финансови загуби и последствия от ДДОС атаките:

1. **Загуба на приходи**: Когато уебсайтът или онлайн услугата стане недостъпна, това може да доведе до загуба на приходи, особено ако компанията разчита на онлайн транзакции или абонаментни услуги.
2. **Повредена репутация**: Често публично обявените атаки могат да навредят на имиджа на компанията, което води до загуба на доверие сред клиентите и партньорите.
3. **Допълнителни разходи за защита и възстановяване**: За да се справят с атаките, компаниите често трябва да инвестират в специализирани услуги за защита, като облачни анти-ДДОС платформи, и да наемат специалисти, които да реагират бързо.

4. **Юридически и регулаторни санкции**: Ако атаките водят до нарушаване на регулации за защита на данни (като GDPR в Европейския съюз), могат да бъдат наложени значителни финансови санкции.

ДДОС атаките се утвърдиха като сериозен риск за бизнеса и могат да имат значителни икономически последствия, ако не се управляват правилно.

## Примери за модерна ДДОС атака

Модерните DDoS (Distributed Denial of Service) атаки често използват сложни и разнообразни методи за създаване на натоварване върху целевия сървър или мрежа. Един от най-разпространените примери за съвременна DDoS атака е **атака с използване на IoT устройства** (Интернет на нещата), като част от **ботнет мрежа**. Тези атаки стават все по-чести поради масовото използване на устройства като камери за наблюдение, рутери и други свързани устройства, които често имат слаба сигурност.

**Пример за модерна DDoS атака:**

### Атака с използване на IoT устройства (ботнет атака)

1. **Компрометиране на IoT устройства**: Хакерите използват уязвимости в устройства като IP камери, рутери или умни домашни устройства, за да ги инфектират с малуер. Тези устройства обикновено не са добре защитени, тъй като не получават редовни актуализации на сигурността.

2. **Създаване на ботнет**: След като устройствата бъдат компрометирани, те се свързват в т.нар. "ботнет" — мрежа от хиляди или дори милиони устройства, които могат да бъдат използвани за атака.

3. **Извършване на атака**: Хакерите командват ботнет мрежата да започне масово изпращане на трафик към целевия сървър. Трафикът може да бъде:

   **CYN flood атака** — изпращане на голямо количество SYN пакети (неполни TCP връзки), които изчерпват ресурсите на сървъра и го правят недостъпен за легитимни потребители.

   **HTTP flood атака** — изпращане на голямо количество HTTP заявки към уеб сървър, което води до изтощаване на ресурсите му.

4. **Дестабилизация на услугата**: Заради огромния обем трафик целевият сървър или мрежа не може да обработва всички входящи заявки и става недостъпен за потребителите, които се опитват да използват услугите му. Това може да доведе до значителни загуби за бизнеса, като например спиране на онлайн магазини, уебсайтове или финансови услуги.

Пример за такава атака е атаката върху **Dyn (DNS доставчик)** през 2016 година, която използва ботнет от компрометирани IoT устройства като камери и рутери, за да срине DNS услугите и да направи недостъпни големи уебсайтове като Twitter, Netflix и Reddit. (Вече я разгледахме по-горе.)

**Основни характеристики на модерните DDoS атаки:**

- Използване на IoT устройства и ботнети.
- Атаки с много канали (multi-vector), комбиниращи различни типове трафик, за да се увеличи ефективността на атаката.
- Използване на техники за прикриване на истинския източник на атаката, като проксита и ботнет мрежи.

Такива атаки могат да бъдат особено разрушителни, ако целят критична инфраструктура или големи корпоративни мрежи.

## III. Как да се предпазим от ДДОС атака:

Предпазването от ДДОС хакерски атаки е критично за защита на онлайн услуги и инфраструктури, особено за организации с важни цифрови ресурси. Професионалният подход за защита включва комбинация от технологии, стратегии и съвременни методи, които могат да осигурят ефективна защита срещу различните видове ДДОС атаки. Ето някои ключови стъпки и практики за защита:

### 1. Използване на специализирани DDoS защити и услуги

- **Cloud-based DDoS защита**: Един от най-ефективните начини да се предпазите от ДДОС атаки е да използвате облачни защитни услуги като **Cloudflare**, **Akamai**, **AWS Shield** или **Google Cloud Armor**. Тези платформи разполагат с мащабируеми механизми за откриване и филтриране на трафик, които могат да погълнат и обработват голямо количество трафик, преди той да достигне до вашите сървъри.

• **Content Delivery Networks (CDNs)**: Използването на CDN услуги като **Cloudflare** или **Amazon Cloud Front** помага за разпределянето на трафика и намаляването на натоварването върху оригиналния сървър, като същевременно предотвратява прекомерното натоварване на един единствен източник.

*Това са методи, които насърчават към ползването на облачни услуги и техните физически ресурси и начини на защита. Това не е реклама и насърчаване за ползване на облачните услуги, а начин за малки фирми и организации.*

## 2. Мрежова сегментация и балансиране на натоварването

• **Балансиране на натоварването**: Използването на балансиране на натоварването (Load Balancer) може да помогне да се разпределят атаките върху различни сървъри, така че един сървър да не бъде претоварен. Тези системи могат да разпределят трафика между различни географски разположени сървъри или дата центрове, намалявайки натоварването върху отделни точки.

• **Сегментация на мрежата**: Разделянето на инфраструктурата на различни сегменти позволява по-голяма гъвкавост в защитата и по-бързо локализиране на проблеми. Така ако един сегмент бъде компрометиран, другите могат да продължат да функционират.

## 3. Идентифициране и филтриране на зловреден трафик

• **IP филтриране и блокиране**: Определени инструменти за сигурност могат да блокират IP адреси, които изпращат аномален трафик. Много платформи и мрежови устройства могат да използват списъци с IP адреси за да блокират подозрителен трафик.

• **Rate limiting (Ограничаване на скоростта)**: Ограничаване на броя на заявките към сървъра за определен период от време (например 100 заявки на минута) може да помогне да се предотвратят атаки, които се опитват да претоварят приложението чрез прекалено много заявки за кратко време.

• **Captcha и challenge-response механизми**: За уеб приложения е полезно да се използват CAPTCHA механизми за проверка на човешки потребители при взаимодействие с онлайн ресурси. Това може да помогне да се блокират бот мрежи, които са основен източник на атаки.

### 4. Използване на firewall и intrusion detection системи (IDS)

• **Web Application Firewall (WAF)**: Използването на **WAF** може да блокира зловредни заявки, като например SQL инжекции, скриптинг атаки или други зловредни заявки, които обикновено се използват при ДДОС атаки. Модерни WAF решения могат да блокират аномален трафик или атаки на ниво приложение.

• **Intrusion Detection Systems (IDS)**: Системи за откриване на проникванията като **Snort** или **Suricata** могат да засичат и алармират за подозрителен трафик или необичайни модели на поведение в мрежата. Те могат да помогнат за ранно откритие на атаки и за навременно предприемане на мерки.

### 5. Анализ на трафика и мониторинг в реално време

• **Мониторинг на трафика**: Програми като **Nagios**, **Zabbix**, или **Prometheus** могат да бъдат използвани за наблюдение на мрежовия трафик в реално време и за автоматично откриване на необичайни натоварвания или аномалии, които могат да предшестват ДДОС атака.

• **Traffic Analytics**: Анализ на трафика и поведение на потребителите позволява навременна идентификация на моделите на атака и бързо предприемане на защита. Технологии за машинно обучение могат да бъдат интегрирани за автоматично идентифициране на необичайни пикове в трафика.

### 6. Наличност на резервни ресурси и мащабируемост

• **Автоматична мащабируемост**: Използването на облачни инфраструктури с автоматична мащабируемост (например **AWS Auto Scaling**, **Azure Scale Sets**) позволява динамично увеличаване на ресурсите при атака, като по този начин се предотвратява претоварването на инфраструктурата.

• **Изграждане на резервни системи**: Важно е да има стратегия за възстановяване на услугата при прекъсвания. Ако основният дата център е подложен на атака, може да се прехвърли трафика към вторични локации или ресурси.

### 7. Честото обновяване на софтуера и правилата за уязвимости

• **Актуализация на софтуерни компоненти**: Редовното обновяване на софтуерни компоненти, уеб приложения, операционни системи и мрежови

устройства е критично за предотвратяване на използването на известни уязвимости от страна на атакуващите.

- **Заключване на IoT устройства**: Често ботнетите използват компрометирани IoT устройства (като камери или рутери), които могат да се използват за стартиране на атаки. Тези устройства трябва да бъдат правилно конфигурирани и да получават редовни актуализации.

### 8. Обучение на служителите

- **Обучение за киберсигурност**: Служителите трябва да бъдат информирани за най-добрите практики за киберсигурност и да разпознават подозрителни дейности или аномалии, които могат да предшестват атака. Те също така трябва да са запознати с протоколите за реакция при инциденти, ако са създадени такива в организацията.

Предпазването от ДДОС атаки изисква интегриран подход с използване на технологии за защита на мрежата, филтриране на трафика, съвременни стратегии за управление на натоварването, мониторинг на трафика в реално време и подготовка на резервни ресурси. Възможността да се открият и реагират на такива атаки бързо е от съществено значение за минимизиране на щетите и запазване на бизнес процесите в безопасност.


Yordanka Dimitrova Zhecheva
Digitally signed by Yordanka Dimitrova Zhecheva
Date: 2025.03.27 12:00:33 +02'00'