СӘТБАЕВ УНИВЕРСИТЕТІ SATBAYEV UNIVERSITY

Дисциплина «Этичный хакинг и противодействие взлому»

Лекция 7

Атаки типа отказ в обслуживании (Denial-of-Services)

Преподаватель: **Батыргалиев Асхат Болатканович, PhD, ассоц.проф. кафедры «Кибербезопасность, обработка и хранение информации»**

askhat.b.b@gmail.com

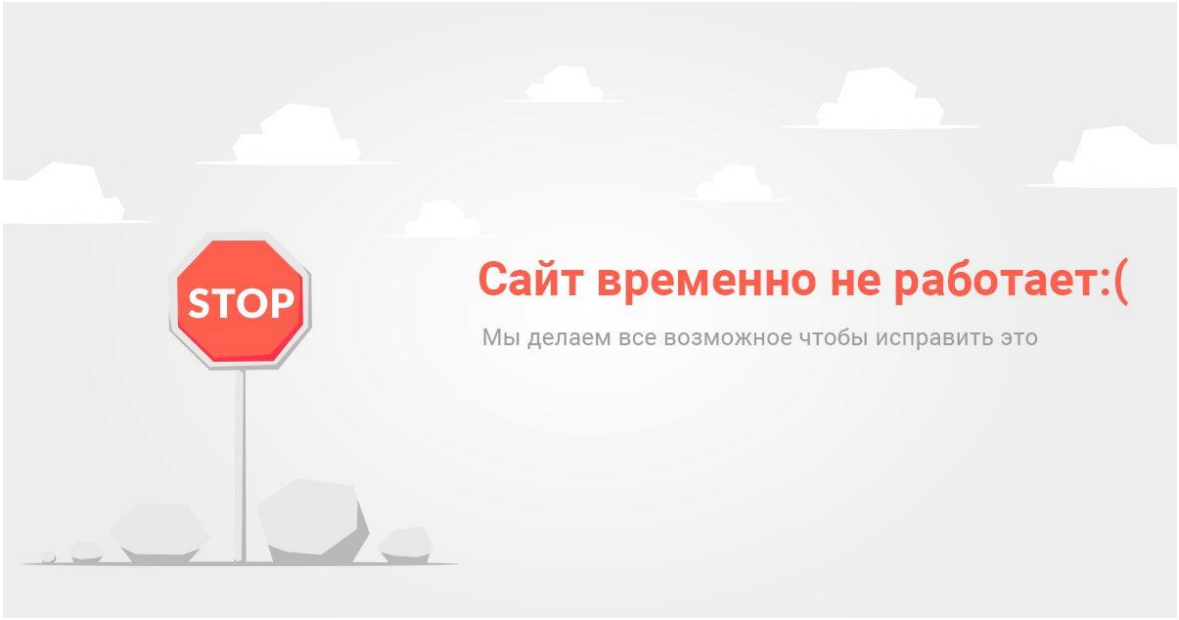
Содержание

По завершению урока Вы будете знать:

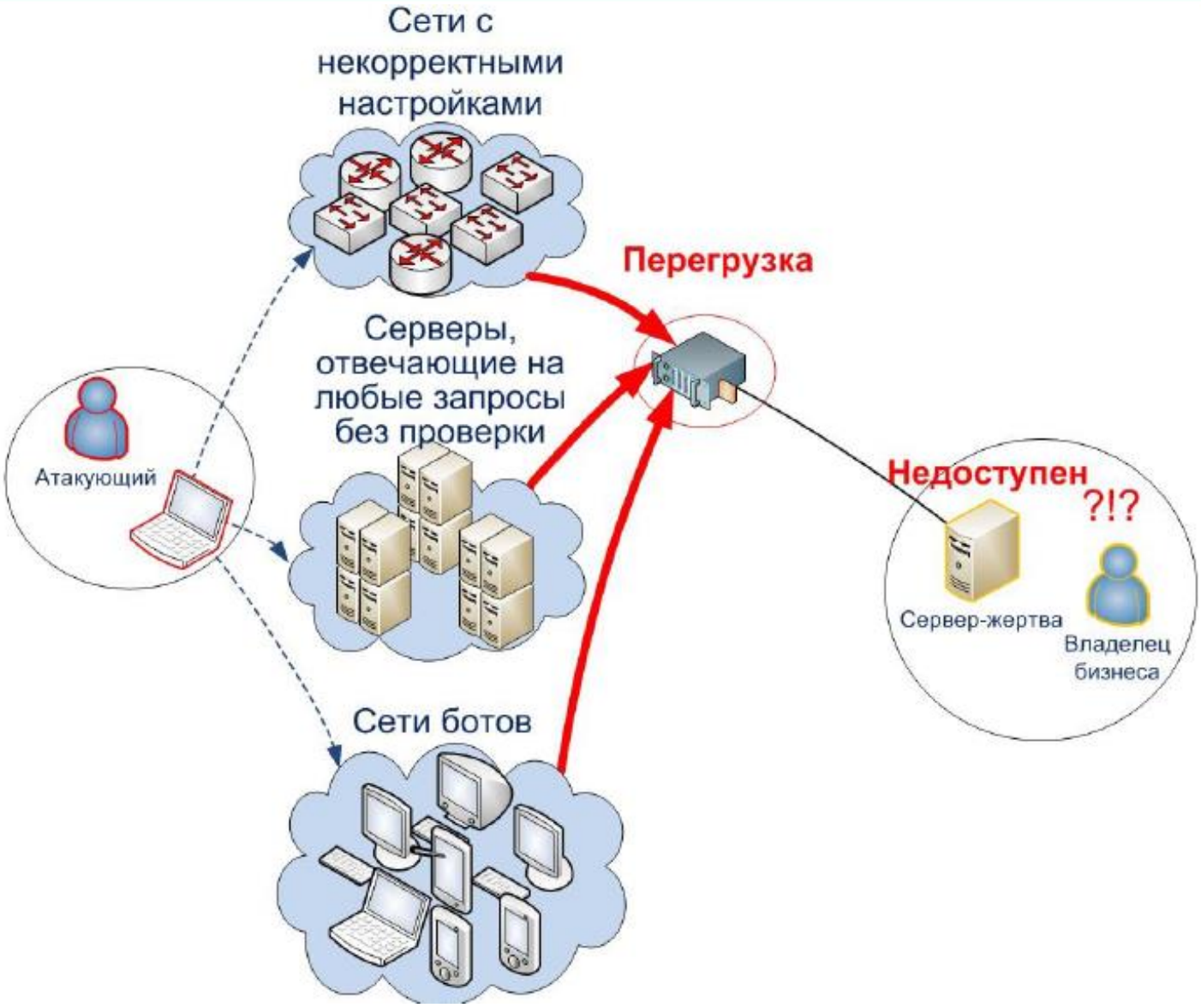
1. Общее понятие атаки отказа в обслуживании
2. Инструменты организации атак
3. Основные направления DDoS-атак
4. Типы атак по принципу действия
5. DDoS-атаки с усилением
6. Атаки с использованием ботнетов
7. Распространение вредоносных программ
8. Атаки на сети оператора
9. Статистика DDoS-атак
10. Динамика роста DDoS-атак
11. Пример DDoS-атак при наличии защиты

Введение в атаки отказа в обслуживании

DoS (*Denial of Service*, «отказ в обслуживании») - хакерская атака на вычислительную систему с целью довести её до отказа, то есть создание таких условий, при которых добросовестные пользователи системы не смогут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ будет затруднён.



Инструменты организации атак



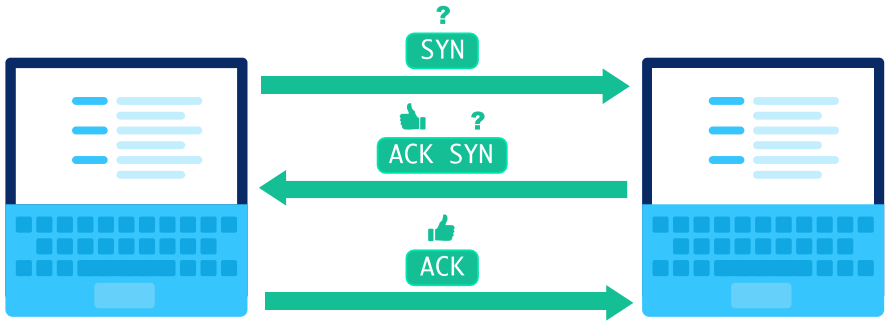
Основные направления DDoS-атак

На сегодняшний день существует огромное количество типов DDoS-атак.

Можно выделить около 40 типов атак, комбинации которых так или иначе используются для реализации 99% всех DDoS-атак в мире.

Основные направления DDoS-атак:

1. Канальная емкость
(уровни 2-3 эталонной модели OSI)



2. Уязвимости стека протоколов
(уровни 3-4 эталонной модели OSI)

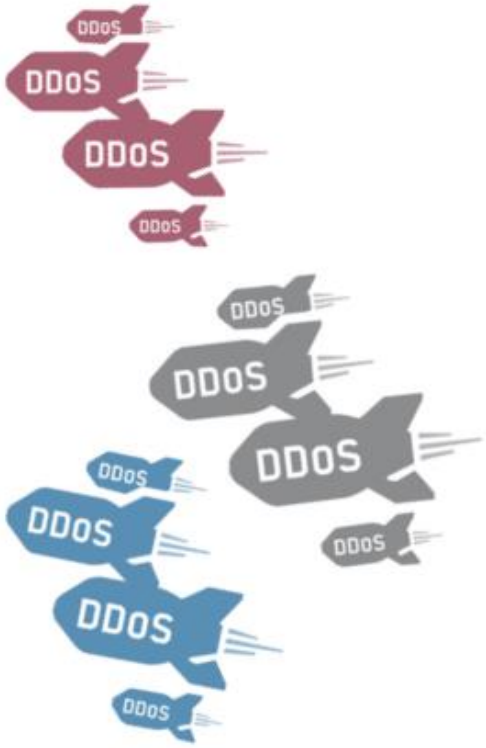
3. Уязвимости приложений
(уровень 7 эталонной модели OSI)

Основные направления DDoS-атак

ТИПЫ АТАК

L7 атаки скрыты и трудны для выявления в силу их сходства с полезным веб-трафиком

7	Прикладной
6	Представления
5	Сеансовый
4	Транспортный
3	Сетевой
2	Канальный
1	Физический



- **TCP SYN+ACK**
- TCP FIN
- TCP RESET
- TCP ACK
- TCP ACK+PSH
- TCP Fragment
- **UDP Flood**
- Slowloris
- Spoofing
- **ICMP Flood**
- IGMP Flood
- HTTP(s) Flood
- Brute Force
- Connection Flood
- DNS Flood
- NXDomain
- **SYN + UDP Flood**
- **ICMP + UDP Flood**
- Ping of Death
- Smurf
- Reflected ICMP & UDP
- Боты !

Типы атак по принципу действия

Атаки, направленные на переполнение канала	Атаки, использующие уязвимости стека сетевых протоколов	Атаки на уровень приложений
DNS амплификация (DNS Amplification)	IP null атака (IP null Attack)	HTTP флуд (HTTP Flood, Excessive VERB)
DNS флуд (DNS Flood)	TCP null атака (TCP null Attack)	HTTP флуд одиночными запросами (Single Request HTTP Flood, Multiple VERB Single Request)
ICMP флуд (ICMP Flood)	Атаки с модификацией поля TOS (Type of Service (TOS) flood)	HTTP флуд одиночными сессиями (Single Session HTTP Flood, Excessive VERB Single Session)
NTP амплификация (NTP amplification)	ACK / PUSH ACK флуд (ACK & PUSH ACK Flood)	Атака с целью отказа приложения (Faulty Application Attack)
NTP флуд (NTP Flood)	RST/FIN флуд (RST/FIN Flood)	Атака фрагментированными HTTP пакетами (Fragmented HTTP Flood, HTTP Fragmentation)
Ping флуд (Ping Flood)	SYN-ACK флуд (SYN-ACK Flood)	Сессионная атака. Атака медленными сессиями (Session Attack, SlowLoris)
UDP флуд (UDP Flood)	SYN-флуд (SYN Flood)	DDoS атаки "нулевого" дня (Zero Day DDoS attack)
UDP-флуд с помощью ботнета (Non-Spoofed UDP Flood)	TCP null/ IP null атака	
Фрагментированный UDP флуд (UDP Fragmentation Flood, UDP Framentation)	Атака поддельными TCP сессиями с несколькими ACK (Multiple ACK Fake Session Attack)	
VoIP флуд (VoIP Flood)	Атака поддельными TCP сессиями с несколькими SYN-ACK (Multiple SYN-ACK Fake Session Attack)	
Флуд медиа-данными (Media Data Flood)	Атака с подменой адреса отправителя адресом получателя (Synonymous IP атака; Same Source/Dest Flood; LAND Attack)	
Атака широковещательными ICMP ECHO пакетами (Smurf Attack)	Атака с помощью перенаправления трафика высоконагруженных сервисов (Misused Application Attack)	
Атака широковещательными UDP пакетами (Fraggle Attack)	Атака поддельными TCP сессиями (Fake Session Attack)	
Фрагментированный ACK флуд (Fragmented ACK Flood)	Ping смерти (Ping Of Death)	
Фрагментированный ICMP-флуд (ICMP Fragmentation Flood)		
Другие атаки с амплификацией (Another amplification attacks)		

DDoS-атаки с усилением

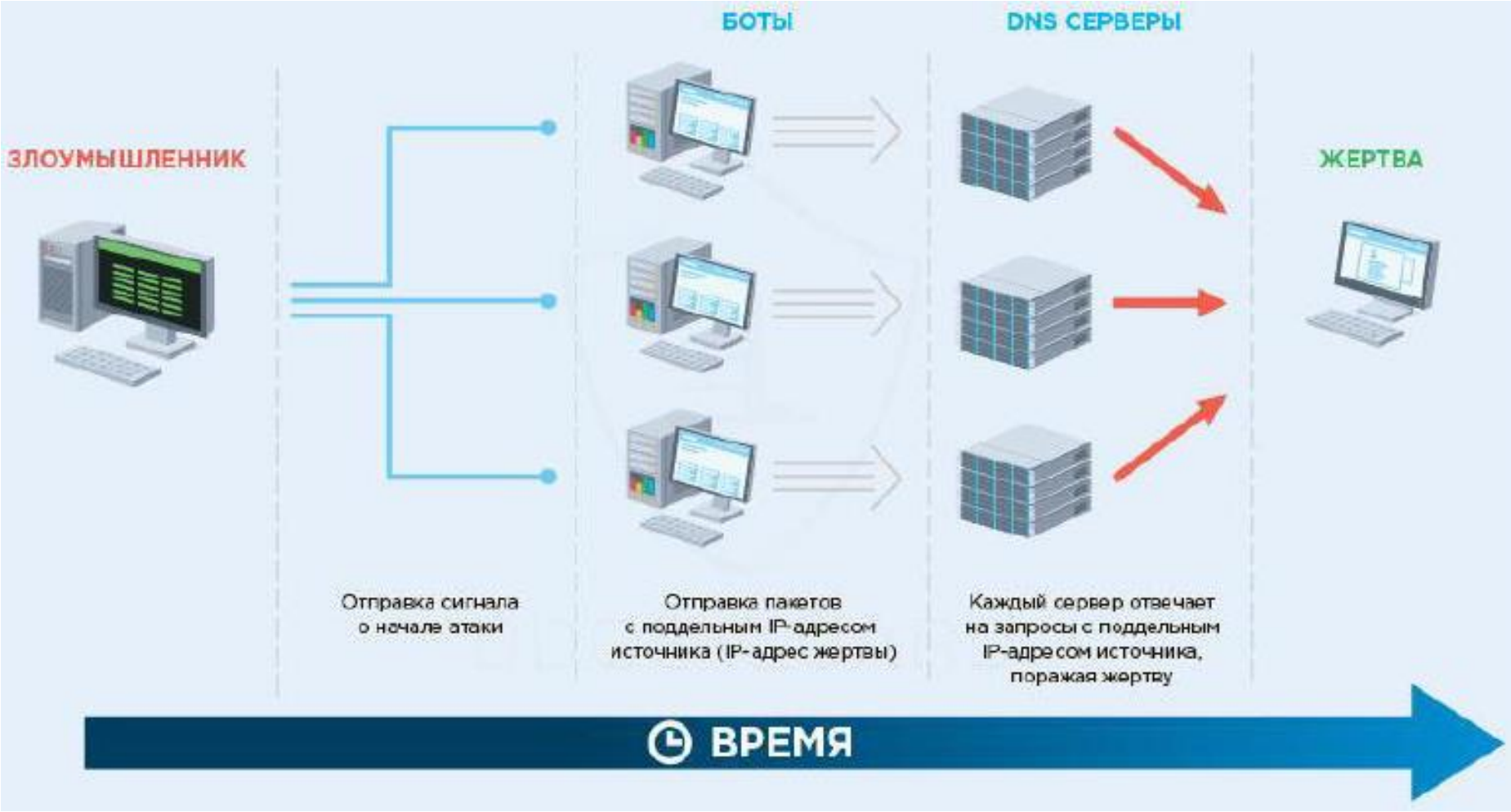


Схема воздействия: заполнить все каналы дата-центра и добиться недоступности сервера-жертвы из сети Интернет

Атаки с использованием ботнетов

Ботнет – компьютерная сеть, состоящая из некоторого количества хостов (ботов) – идеальный инструмент для организации самых сложных атак.

Атаки с использованием ботнетов

Злоумышленники могут применить различные способы для выявления и получения доступа к машинам-жертвам. Наиболее важными из них являются:

- *Случайное сканирование*. В этом подходе машина, зараженная вредоносным кодом (это может быть машина атакера или другая взломанная им ранее ЭВМ), сканирует определенную IP-область, выбирая адреса случайным образом, и пытается выявить уязвимую машину. Если такая обнаружена, делается попытка ее взлома и, в случае успеха, размещает там свой вредоносный код. Этот метод создает достаточно большой трафик, так как одни и те же адреса сканируются помногу раз. Преимуществом такого способа является достаточно быстрое заражение большого числа машин и создание впечатления, что сканирование происходит отовсюду. Однако высокий уровень трафика препятствует длительному продолжению атаки.
- *Сканирование по списку*. Задолго до начала сканирования атакер подготавливает достаточно обширный список потенциально уязвимых машин. Такой список может готовиться достаточно долгое время, чтобы не привлечь к этому внимания служб безопасности. Сканирование производится только для машин их этого списка. Когда обнаружена уязвимая машина, на нее устанавливается соответствующая программа, а список сканирования делится пополам. Вновь взломанной машине поручается сканирование машин одной из частей списка. Каждая из машин продолжает сканирование пока не сможет найти уязвимую ЭВМ. После этого список снова делится и процедура продолжается. Таким образом, число машин, участвующих во взломах, лавинообразно увеличивается.

Атаки с использованием ботнетов

- *Топологическое сканирование*. При топологическом сканировании используется информация, содержащаяся в машине жертвы, для поиска новых потенциальных жертв. При этом на диске взломанной машины ищутся URL, которые можно попробовать атаковать. Этот метод может оказаться даже несколько более эффективным, чем сканирование по списку.
- *Сканирование локальной субсети*. Этот вид сканирования работает за firewall. Взломанная машина ищет потенциальные жертвы в своей собственной локальной сети. Эта техника может использоваться в сочетании с другими способами атак, например, взломанная машина может начать сканирование локальной сети, а когда список таких машин будет исчерпан, переключиться на сканирование других сетевых объектов.
- *Перестановочное сканирование*. При этом типе сканирования все машины совместно используют общий псевдослучайный перестановочный список IP-адресов. Такой список может быть сформирован с помощью блочного 32-битного шифра с заранее заданным ключом. Если взломанная машина была инфицирована при сканировании по списку или из локальной сети, она начинает сканирование, начиная со своей позиции в списке перестановок. Если же она оказалась скомпрометирована в процессе перестановочного сканирования, она начинает сканирование с псевдослучайной позиции списка. В случае если она встретит уже инфицированную машину, она выбирает новую псевдослучайную позицию в списке перестановок и продолжает работу с этой точки. Распознавание инфицированных машин происходит за счет того, что их отклики отличаются от откликов невзломанных ЭВМ. Сканирование прекращается, если машина встретит заданное число инфицированных машин. После этого выбирается новый ключ перекодировок и начинается новая фаза сканирования. Факт такого сканирования труднее детектировать.

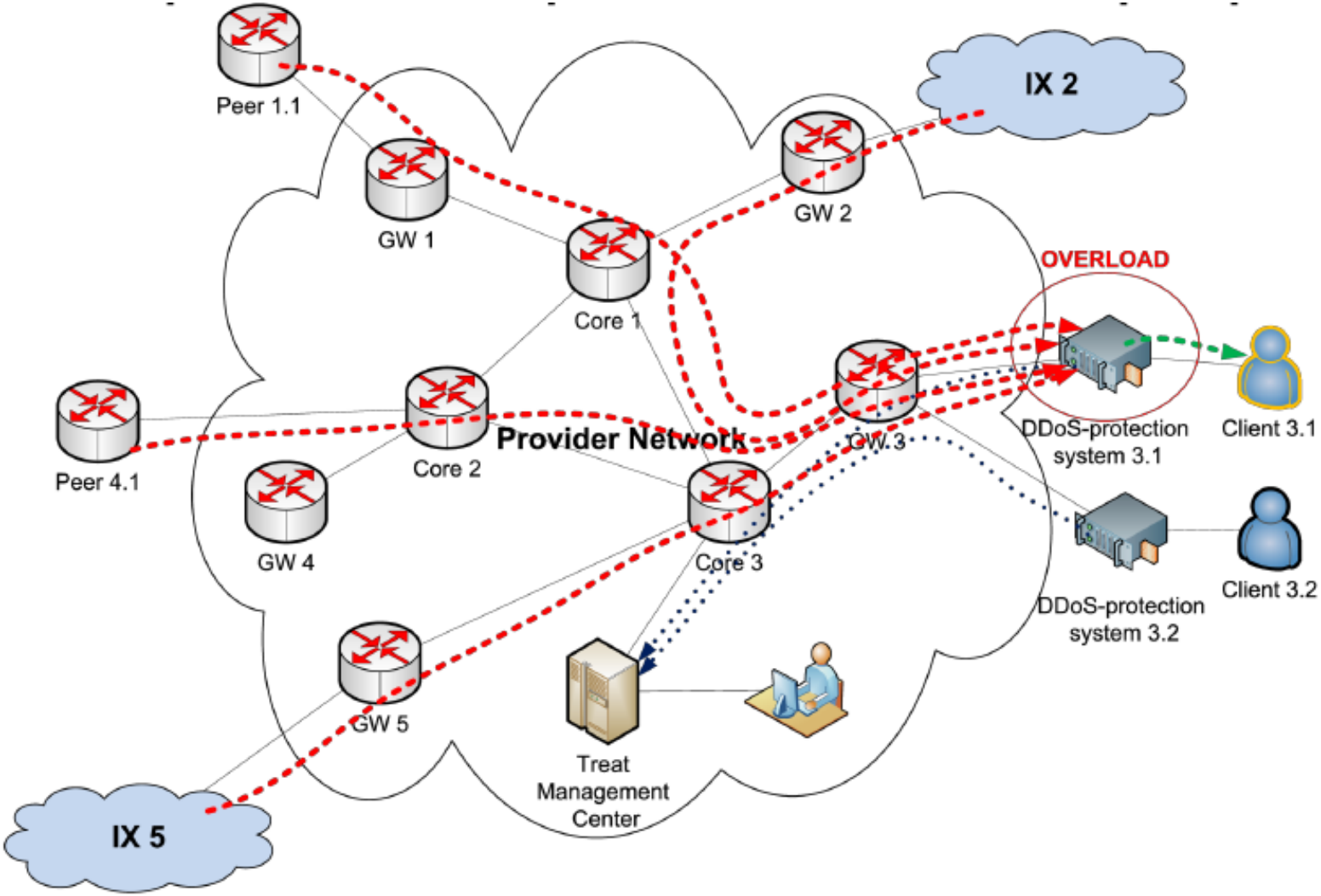
Распространение вредоносных программ

Можно выделить три механизма рассылки вредоносных кодов и построения сетей для атак:

- *Централизованная рассылка*. В этой схеме после выявления уязвимой системы, которая должна стать зомби, выдается команда в центр рассылки для копирования вредоносного кода (toolkit) во взломанную машину. После копирования этого кода осуществляется инсталляция вредоносной программы на машине жертвы. После инсталляции запускается новый цикл атак с уже захваченной машины. Для передачи кодов программ могут использоваться протоколы HTTP, FTP и RPC.
- *Доставка от атакера (Back-chaining)*. В этой схеме все вредоносные коды доставляются в захваченную машину из ЭВМ атакера. В частности, средства атаки, установленные у атакера, включают в себя программы доставки вредоносных кодов жертве. Для этой цели на машине-жертве может использоваться протокол TFTP.
- *Автономная рассылка*. В этой схеме атакующая машина пересылает вредоносный код в машину-жертву в момент взлома.

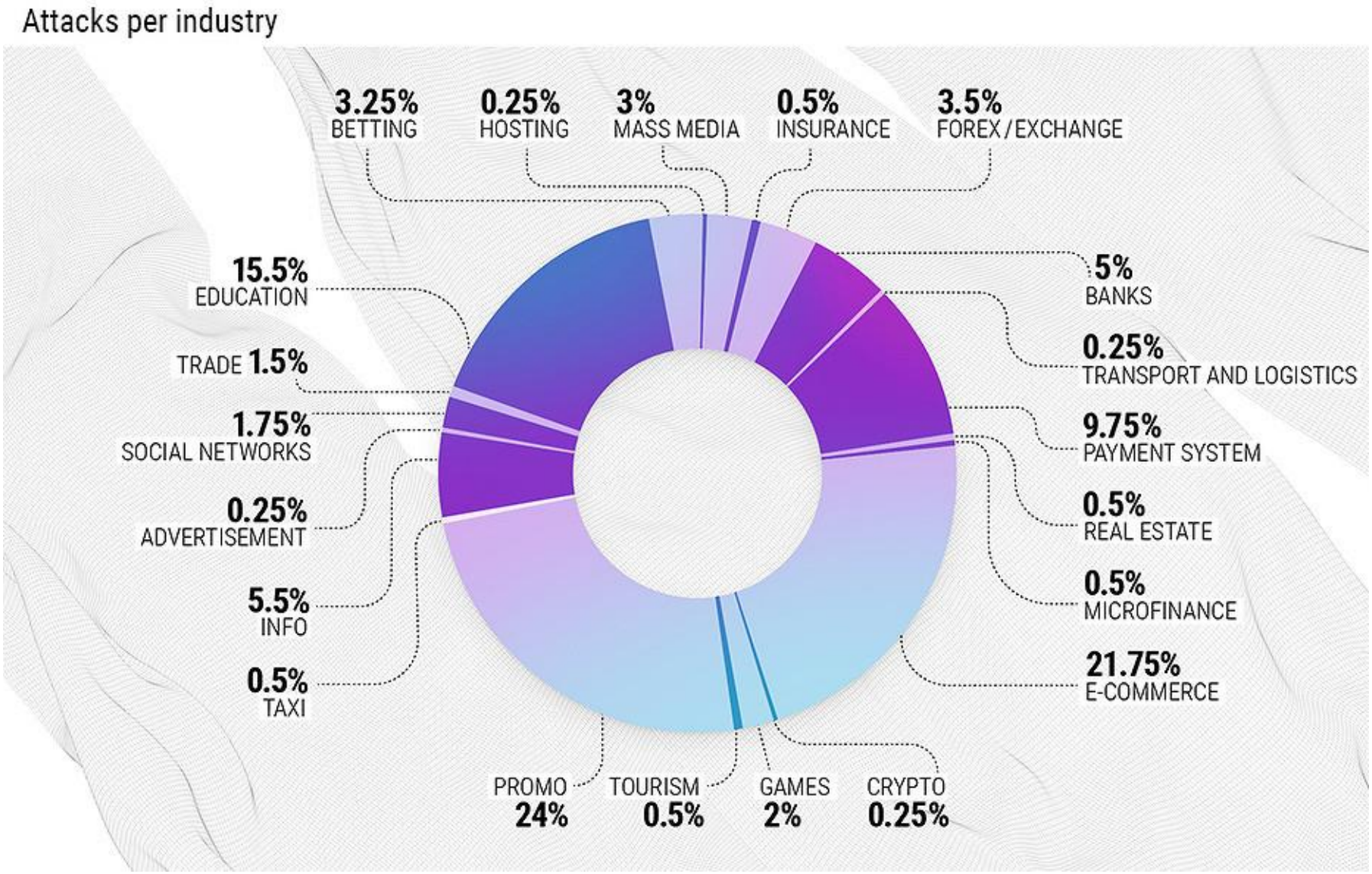
После того как армия атакующих машин сформирована, атакер определяет вид и объект атаки и ждет удобного момента времени. После начала атаки все машины этой армии начинают слать пакеты по адресу машины-жертвы. Объем трафика при этом может быть столь велик, что может быть заблокирован даже шлюз сети, где расположена машина-жертва. Сейчас в Интернет имеется около дюжины программ автоматизации процесса на всех фазах атаки. Причем для пользования ими не требуется лицензии.

Атаки на сети оператора

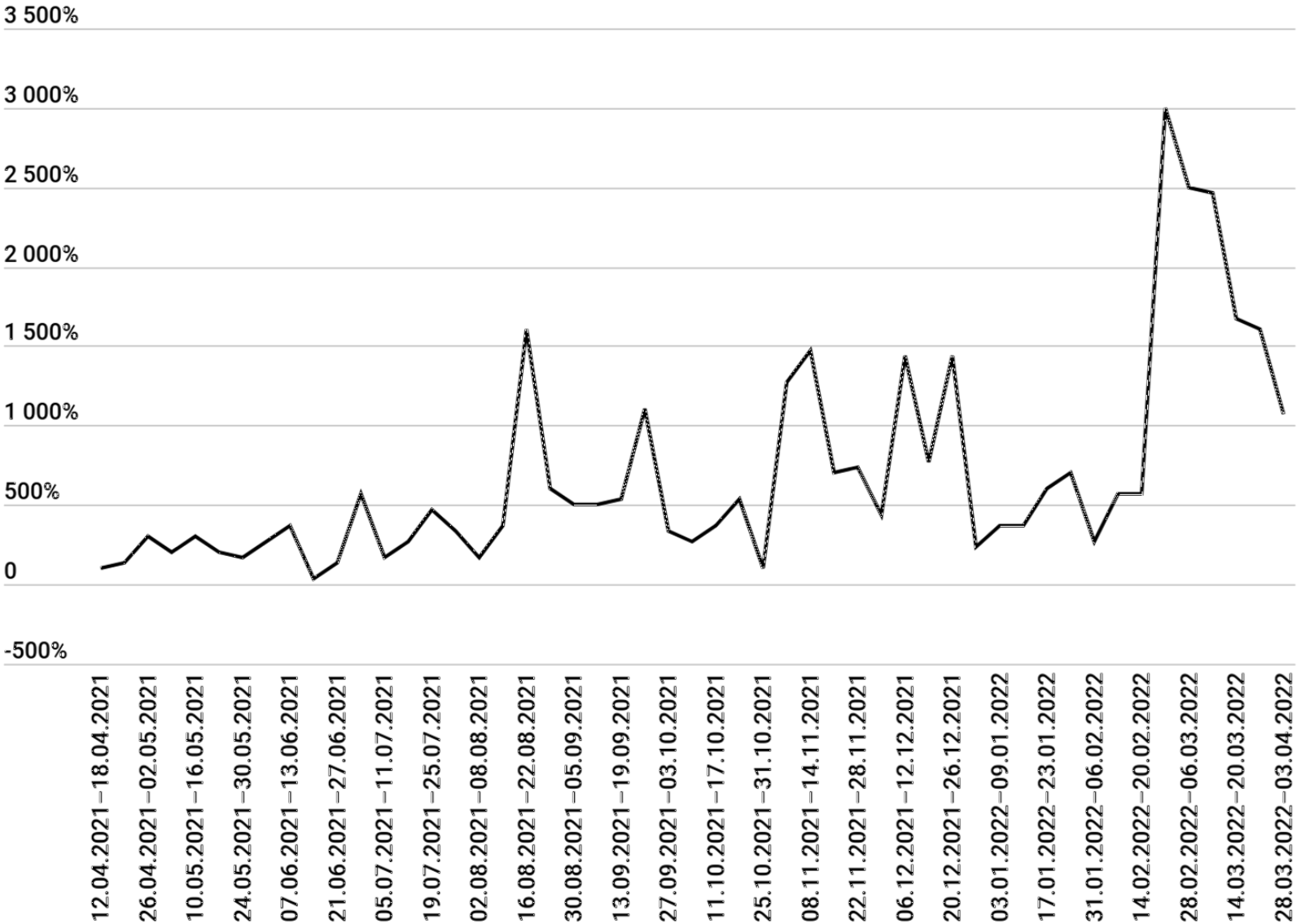


Со всех направлений начинает прибывать трафик, адресованный одному хосту, на котором возникает перегрузка и, как следствие, его недоступность.

Статистика DDoS-атак

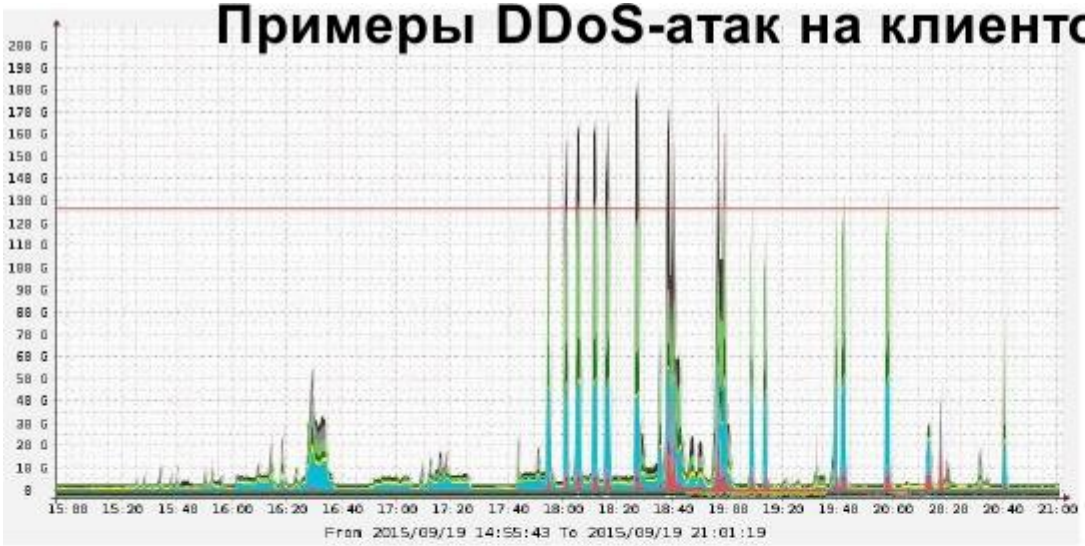


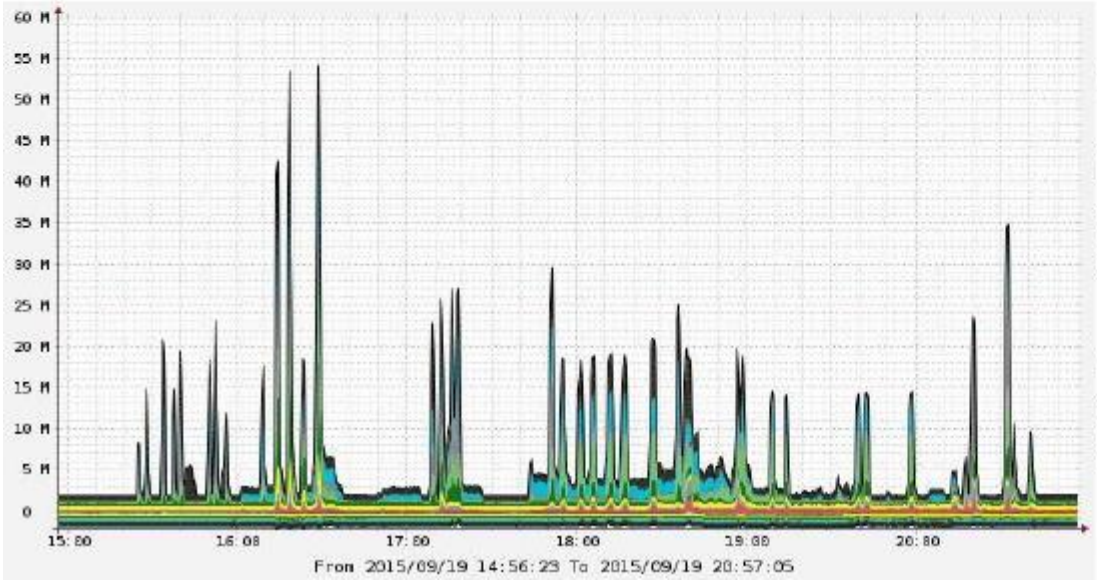
Динамика роста DDoS-атак



Пример DDoS-атак при наличии защиты

Примеры DDoS-атак на клиентов DDoS-GUARD





Хронология профессиональной атаки:

1.Начать с распределенной атаки (на подсеть) фрагментированными пакетами 20 млн. пакетов в секунду *(с 15:20 до 16:00)*

2. Добавить TCP SYN-flood +35 млн. пакетов в секунду *(с 16:00 до 18:00)*

3.Добавить амплификационных атак +180-190 Гбит/с *(с 18:00 до 20:50)*

4.Вернуть деньги заказчику, т.к. ресурс остался доступным благодаря нашей защите :-)