DDoS-атаки и электронная коммерция

Типичные угрозы и современные подходы

Артём Гавриченков <ag@qrator.net>

Мишени

- L2
- L3
- L4
- L7

Мишени

- L2
  «Забивание» канала: ICMP Flood, * Amp… 500 Gbps
- L3
- L4
- L7

Мишени

- L2
  «Забивание» канала: ICMP Flood, * Amp… 500 Gbps
- L3
  Нарушение функционирования сетевой инфраструктуры
- L4
- L7

Мишени

- L2
  «Забивание» канала: ICMP Flood, * Amp… 500 Gbps
- L3
  Нарушение функционирования сетевой инфраструктуры
- L4
  Эксплуатация слабых мест TCP-драйвера
- L7

Мишени

- L2
  «Забивание» канала: ICMP Flood, * Amp… 500 Gbps

- L3
  Нарушение функционирования сетевой инфраструктуры

- L4
  Эксплуатация слабых мест TCP-драйвера

- L7
  Деградация Web-приложения

Противомеры

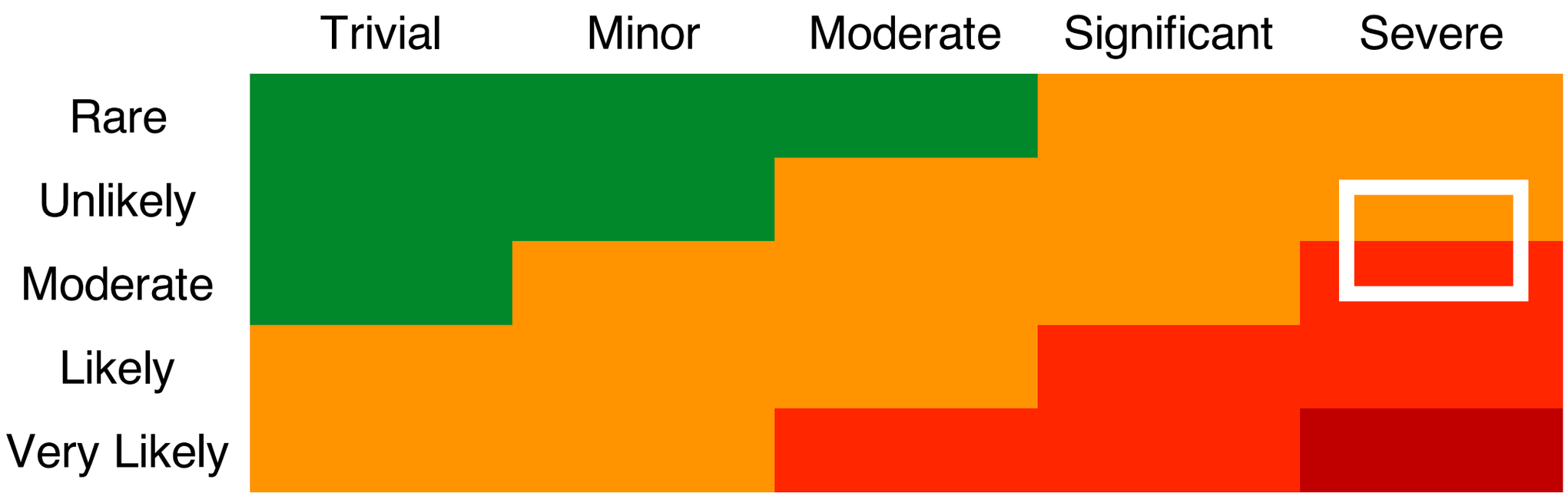
- L2
  Полоса!
- L3
  Аналитика
- L4
  Анализ поведения и эвристика
- L7
  Поведенческий, корреляционный анализ, мониторинг

Сетевая архитектура

- «Земной» хостинг
- «Облачный» хостинг
- CDN

Оценка рисков

Probability/Impact Matrix



Probability:
Moderate/Unlikely

Impact:
Severe

Оценка рисков

	Хостинг	Облако	CDN
L2			
L3			
L4			
L7			

Оценка рисков

	Хостинг	Облако	CDN
L2	High		
L3	Low		
L4	High		
L7	High		

Оценка рисков

	Хостинг	Облако	CDN
L2	High	Moderate	
L3	Low	Low	
L4	High	Low	
L7	High	High	

Оценка рисков

	Хостинг	Облако	CDN
L2	High	Moderate	Moderate
L3	Low	Low	High
L4	High	Low	Low
L7	High	High	Low

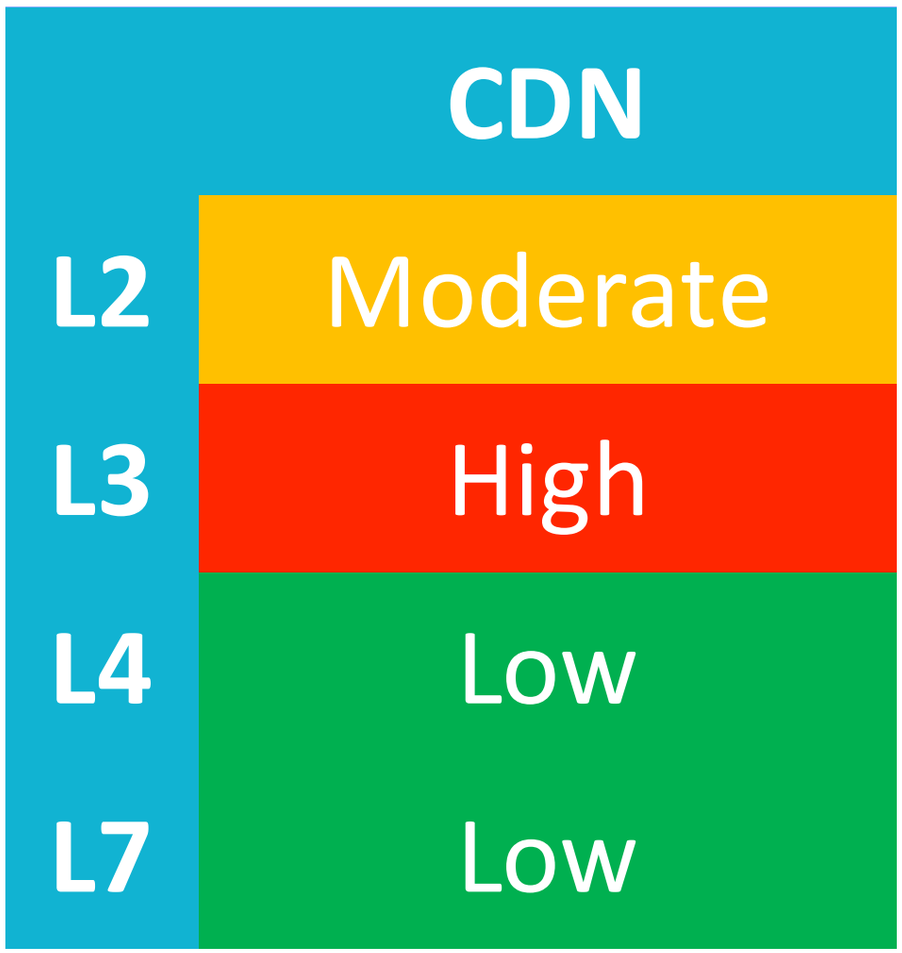
Оценка рисков

- Что ни размещай, в т.ч. специализированное оборудование
- У приложения должен быть запас производительности (2x)
- INSTANT RELOCATION

Оценка рисков

- BGP Anycast!
- 500 Гбит/с – не шутки
- У приложения должен быть запас производительности (2x)
- «DoS via billing»

Оценка рисков



- BGP Anycast
- Защищённый DNS-сервер

Сетевая архитектура

- Anycast-адрес – это вообще полезно!
  - IPv4, кстати, заканчивается
  - IPv6 плохо внедряется
  - Anycast можно арендовать

Сетевая архитектура

- Приложение, отвязанное от платформы
- Docker?
- Документация

Сетевая архитектура

- Обращайтесь к вендорам!
  - Атакующие тратят меньше сил
  - Придётся работать 24/7
  - Успешная атака не заканчивается быстро
  - Платить вымогателям нельзя!

Спасибо за внимание!

Artyom Gavrichenkov
<ag@qrator.net>

QRATOR