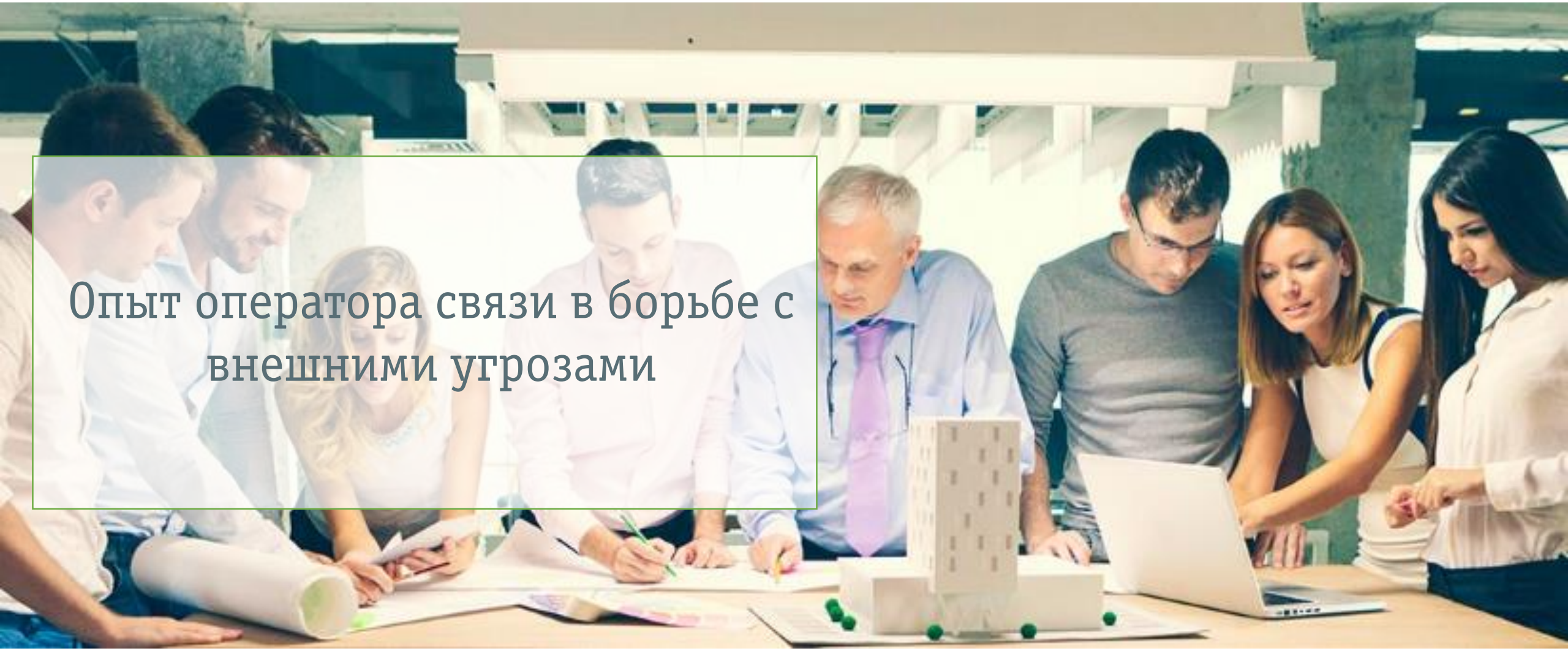


Опыт оператора связи в борьбе с внешними угрозами

Содержание

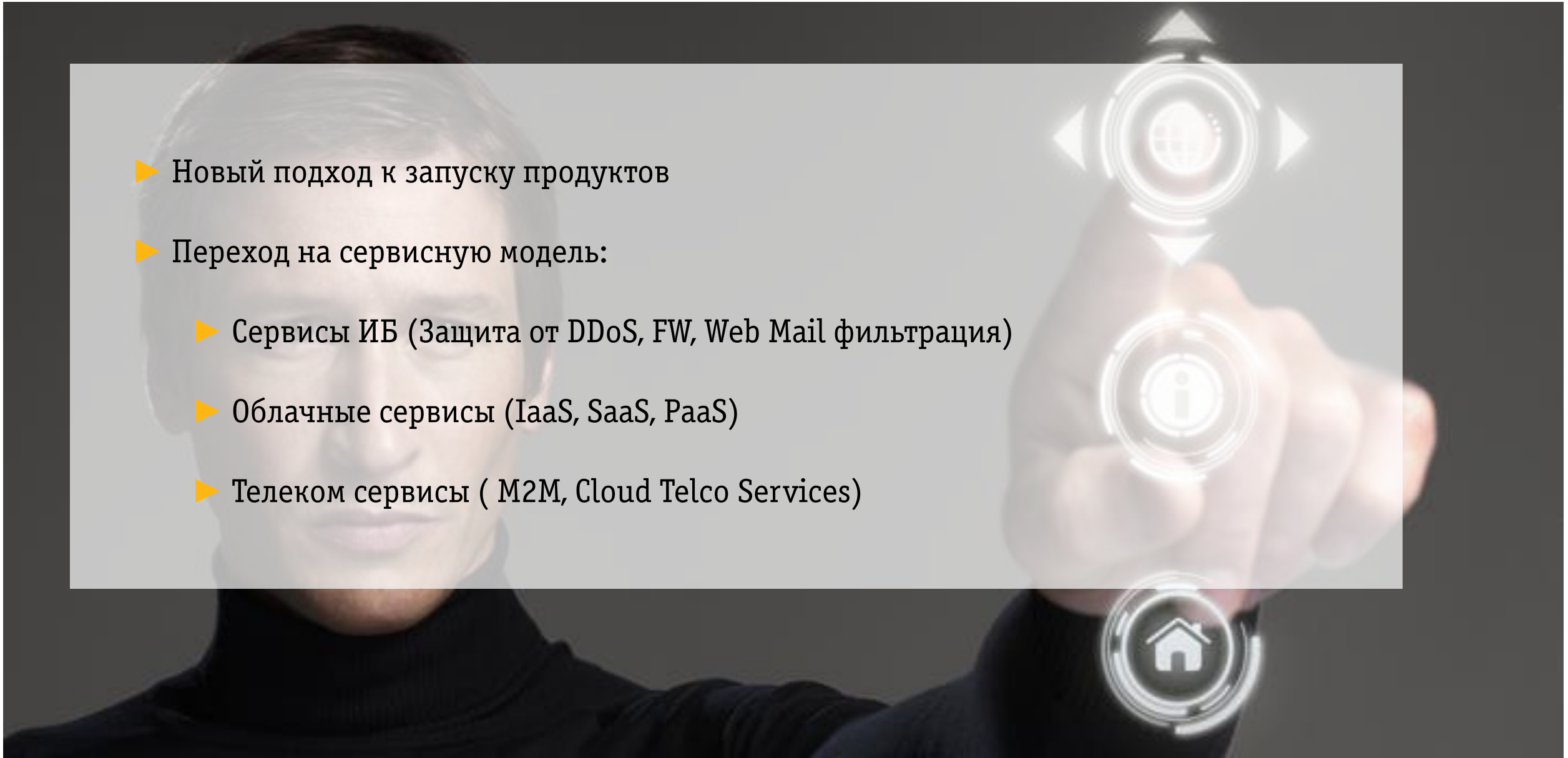
Тренды

- Digitalизация бизнеса
- Мобилизация сотрудников
- Проникновение облаков в бизнес

- **Размывание границ сети**
- Стремительный **рост числа угроз**, в том числе и для малого бизнеса

Оператор связи раньше

Мы меняемся



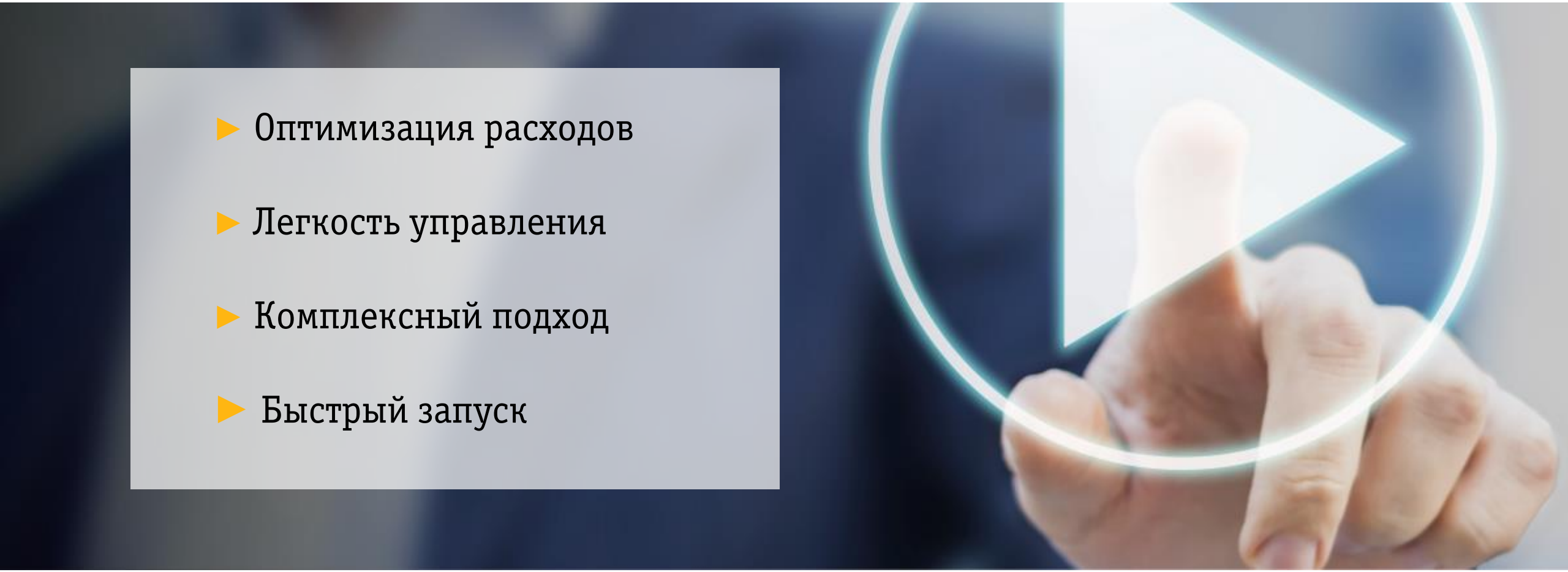
- Новый подход к запуску продуктов
- Переход на сервисную модель:
  - Сервисы ИБ (Защита от DDoS, FW, Web Mail фильтрация)
  - Облачные сервисы (IaaS, SaaS, PaaS)
  - Телеком сервисы (M2M, Cloud Telco Services)

Новый подход к запуску сервисов

- Изучение потребностей клиентов
- Внутренняя экспертиза
- Тестирование
- Запуск в эксплуатацию

- Сокращение time-to-market
- Кастомизация сервисов в соответствии с потребностями бизнеса

Облачные сервисы ИБ



- Оптимизация расходов
- Легкость управления
- Комплексный подход
- Быстрый запуск

Часть II

Защита от DDoS. История, статистика, кейсы.

Защита от DDoS

2011	Установлено оборудование для защиты ИТ ресурсов Билайн.
2012–2013	Изучение потребностей клиентов в услуге защиты от DDoS.
2013	Построение центра отчистки интернет трафика. Подключение первых клиентов.
2014–2015	Построение локальных региональных центров отчистки. Расширение вариантов предоставления услуги.

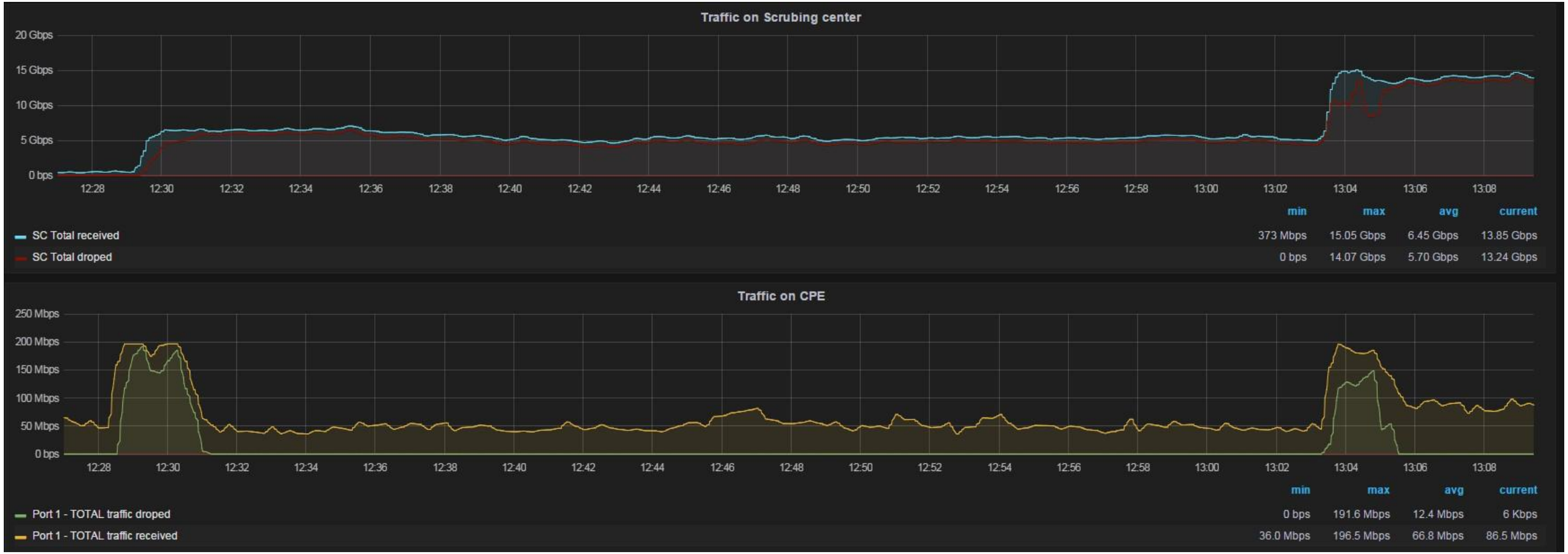
Немного статистики

- Среднее число различных атак на клиента ~15 000 +15% Y2Y
- Увеличение длительности атак. 30% атак длятся более 1 часа +12% Y2Y
- Рост числа Amplification атак
- В среднем 9 атак превышающих емкость канала связи +30% Y2Y
- Максимальная емкость отраженной атаки ~38Gbps -15% Y2Y

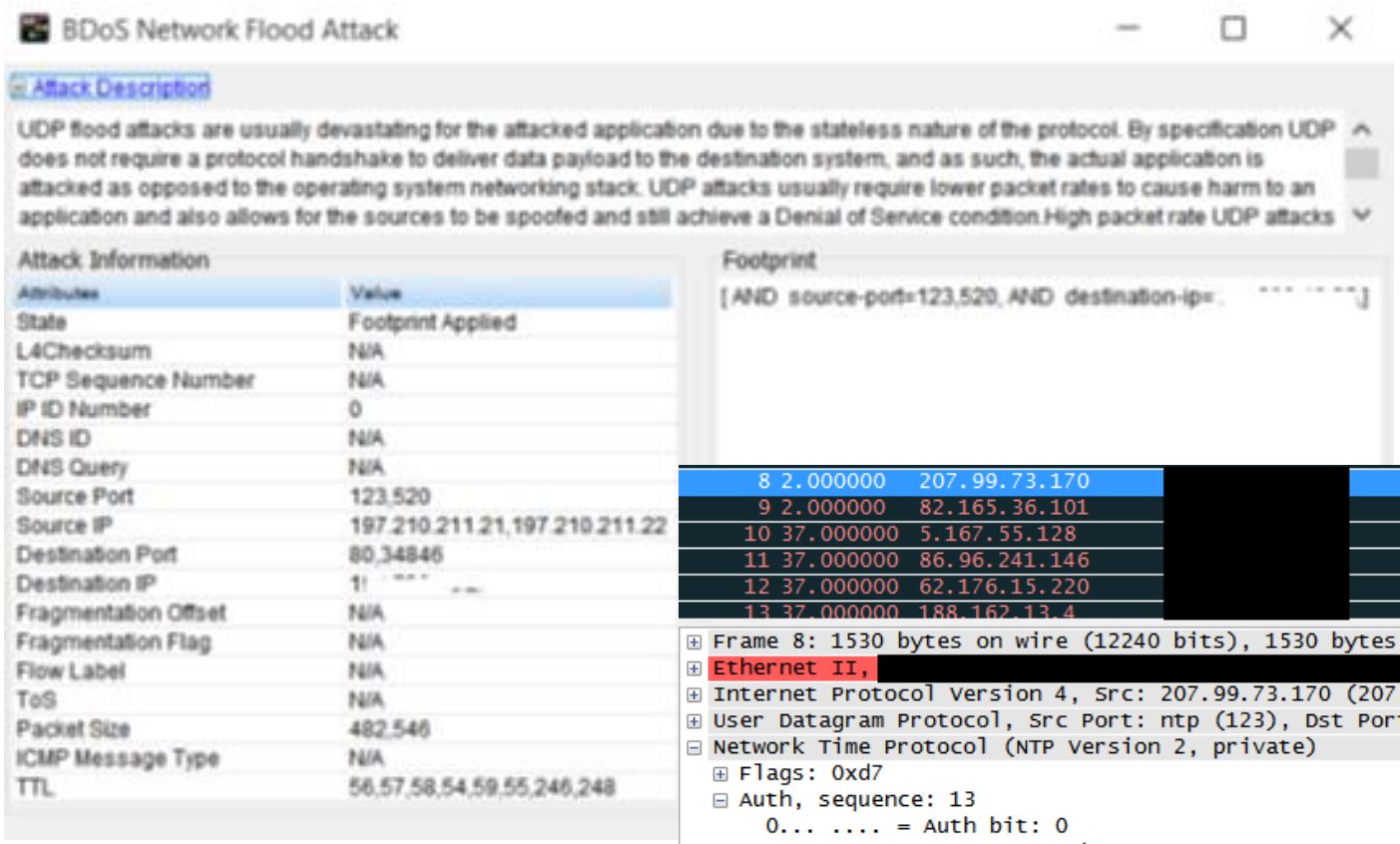
Цели и причины атак

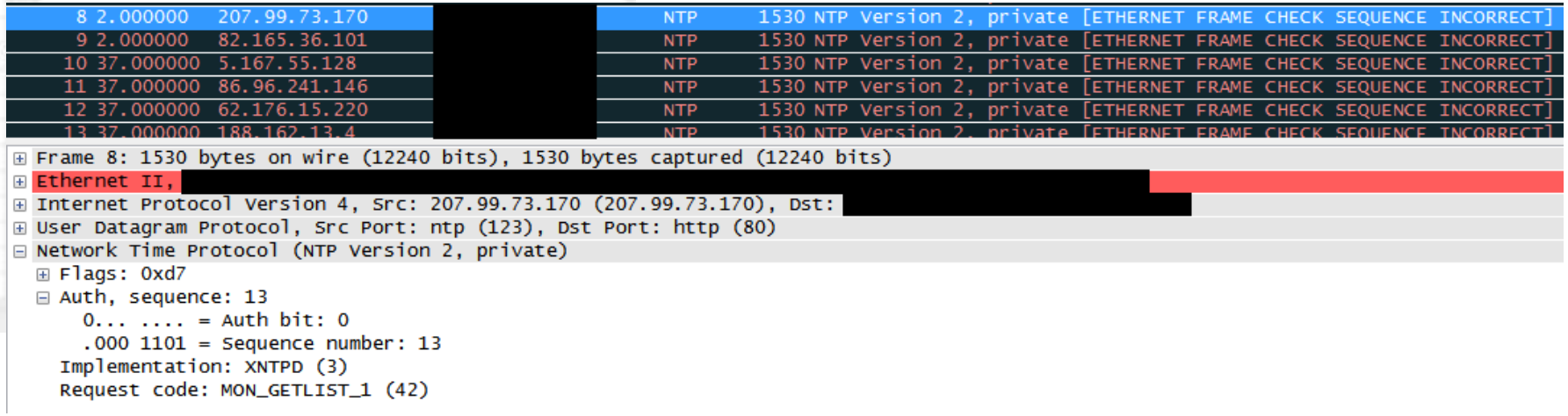
- Финансовые - вымогательство
- Политические
- Конкуренты
- Месть - Обиженные сотрудники
- Развлечение - школьники

История одной атаки

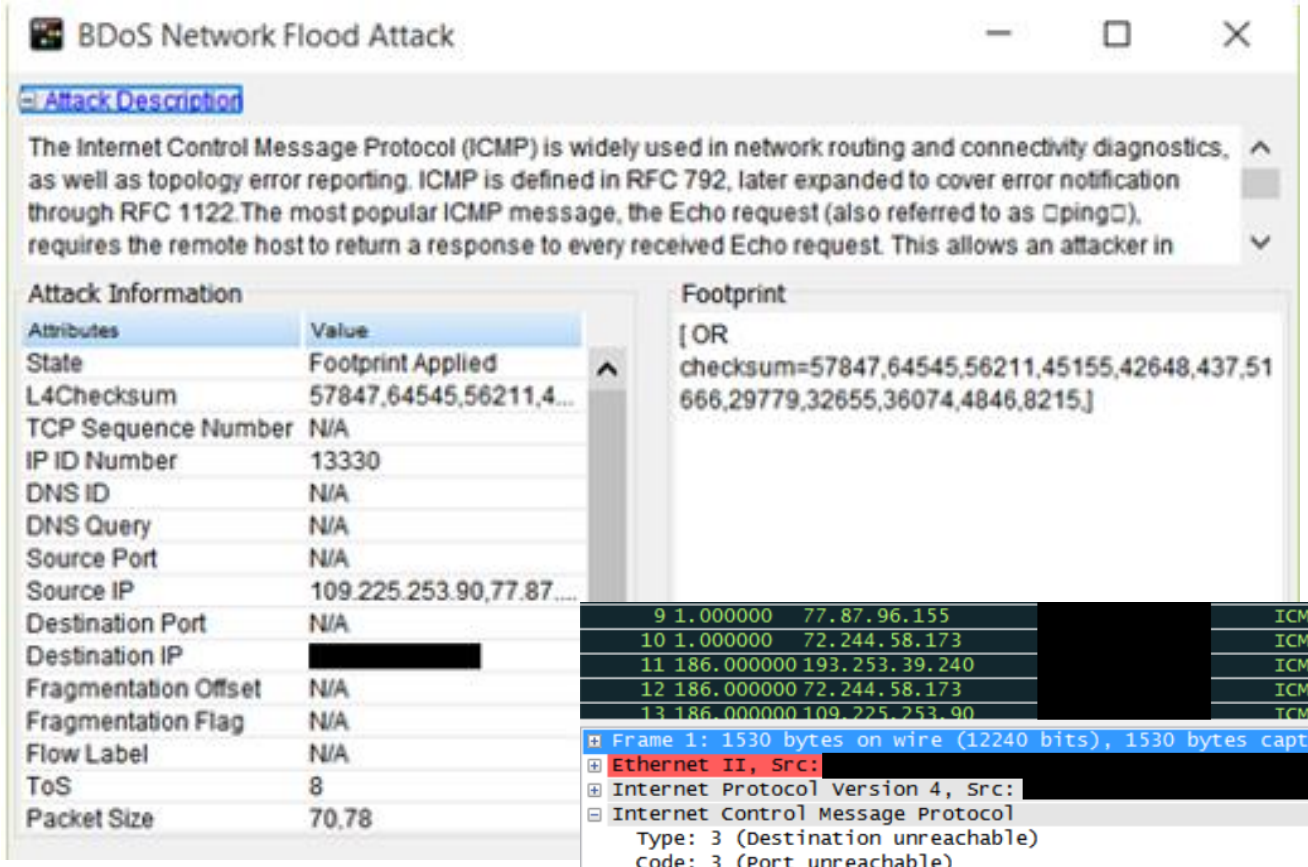


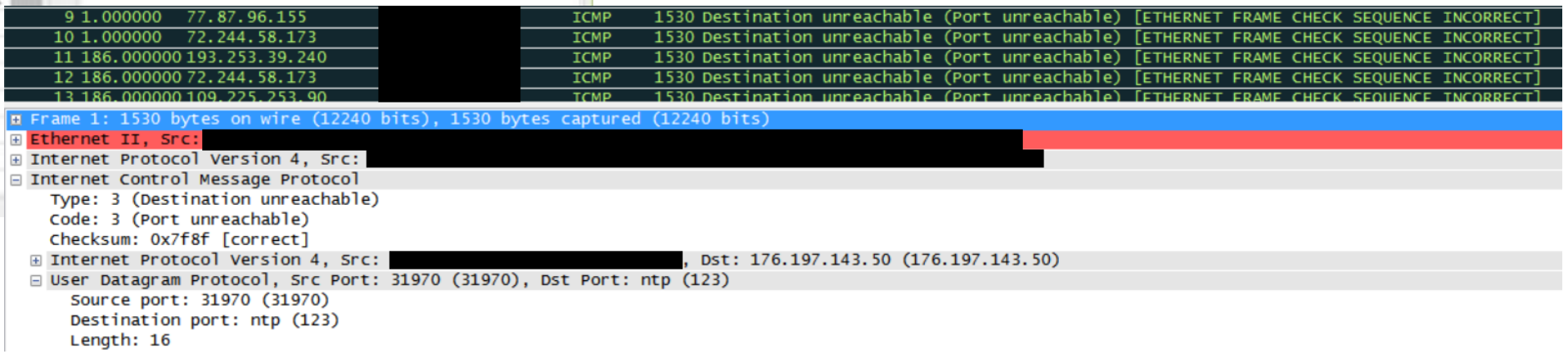
Подробнее


BDoS Network Flood Attack
Attack Description
UDP flood attacks are usually devastating for the attacked application due to the stateless nature of the protocol. By specification UDP does not require a protocol handshake to deliver data payload to the destination system, and as such, the actual application is attacked as opposed to the operating system networking stack. UDP attacks usually require lower packet rates to cause harm to an application and also allows for the sources to be spoofed and still achieve a Denial of Service condition.High packet rate UDP attacks
Attack Information
Attributes
Value
State
Footprint Applied
L4Checksum
N/A
TCP Sequence Number
N/A
IP ID Number
0
DNS ID
N/A
DNS Query
N/A
Source Port
123,520
Source IP
197.210.211.21,197.210.211.22
Destination Port
80,34846
Destination IP
Fragmentation Offset
N/A
Fragmentation Flag
N/A
Flow Label
N/A
ToS
N/A
Packet Size
482,546
ICMP Message Type
N/A
TTL
56,57,58,54,59,55,246,248
Footprint
[AND source-port=123,520, AND destination-ip=


8 2.000000 207.99.73.170 NTP 1530 NTP Version 2, private [ETHERNET FRAME CHECK SEQUENCE INCORRECT]
9 2.000000 82.165.36.101 NTP 1530 NTP Version 2, private [ETHERNET FRAME CHECK SEQUENCE INCORRECT]
10 37.000000 5.167.55.128 NTP 1530 NTP Version 2, private [ETHERNET FRAME CHECK SEQUENCE INCORRECT]
11 37.000000 86.96.241.146 NTP 1530 NTP Version 2, private [ETHERNET FRAME CHECK SEQUENCE INCORRECT]
12 37.000000 62.176.15.220 NTP 1530 NTP Version 2, private [ETHERNET FRAME CHECK SEQUENCE INCORRECT]
Frame 8: 1530 bytes on wire (12240 bits), 1530 bytes captured (12240 bits)
Ethernet II,
Internet Protocol Version 4, Src: 207.99.73.170 (207.99.73.170), Dst:
User Datagram Protocol, Src Port: ntp (123), Dst Port: http (80)
Network Time Protocol (NTP Version 2, private)
Flags: 0xd7
Auth, sequence: 13
0... .... = Auth bit: 0
.000 1101 = Sequence number: 13
Implementation: XNTPD (3)
Request code: MON_GETLIST_1 (42)

И еще немого подробнее





Ботнет? Нет!

vpnguy / ntpdos

Watch

Code | Issues 1 | Pull requests 0 | Pulse | Graphs

Branch: master ▾ ntpdos / ntpdos.py

outime Removed redundant str() calls

2 contributors

Executable File | 79 lines (65 sloc) | 2.02 KB | Raw

```
#!/usr/bin/env python
from scapy.all import *
import sys
import threading
import time
#NTP Amp DOS attack
#by DaRkReD
#usage ntpdos.py <target ip> <ntpserver list> <number of threads> ex: ntpdos.py 1.2.3.4 file.txt 10
#FOR USE ON YOUR OWN NETWORK ONLY


#packet sender
def deny():
        #Import globals to function
        global ntplist
        global currentserver
        global data
        global target
```

```
74    print "Sending..
75
76    #Keep alive so c
77    while True:
78            time.sle
```

rickarivesa / DNSampAttack

Code | Issues 0 | Pull requests 0 | Pulse | Graphs

No description or website provided.

7 commits | 1 branch

Branch: master ▾ | New pull request | New file | Find file | HT

rickarivesa Create test.py

README.md	Initial commit
attack.pl	Create attack.pl
dnsamp.py	Create dnsamp.py
dnsdrdos.c	Create dnsdrdos.c
find_open_resolvers.pl	Create find_open_resolvers.pl
test.py	Create test.py
whateveryouwant.c	Create whateveryouwant.c

README.md

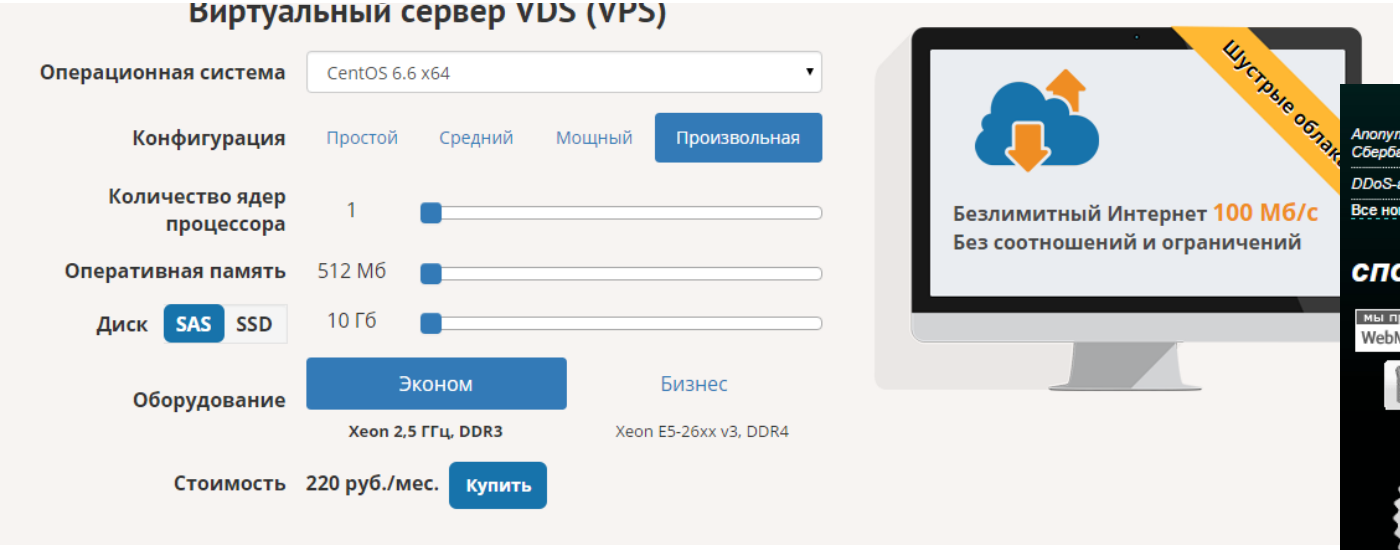
DNSampAttack

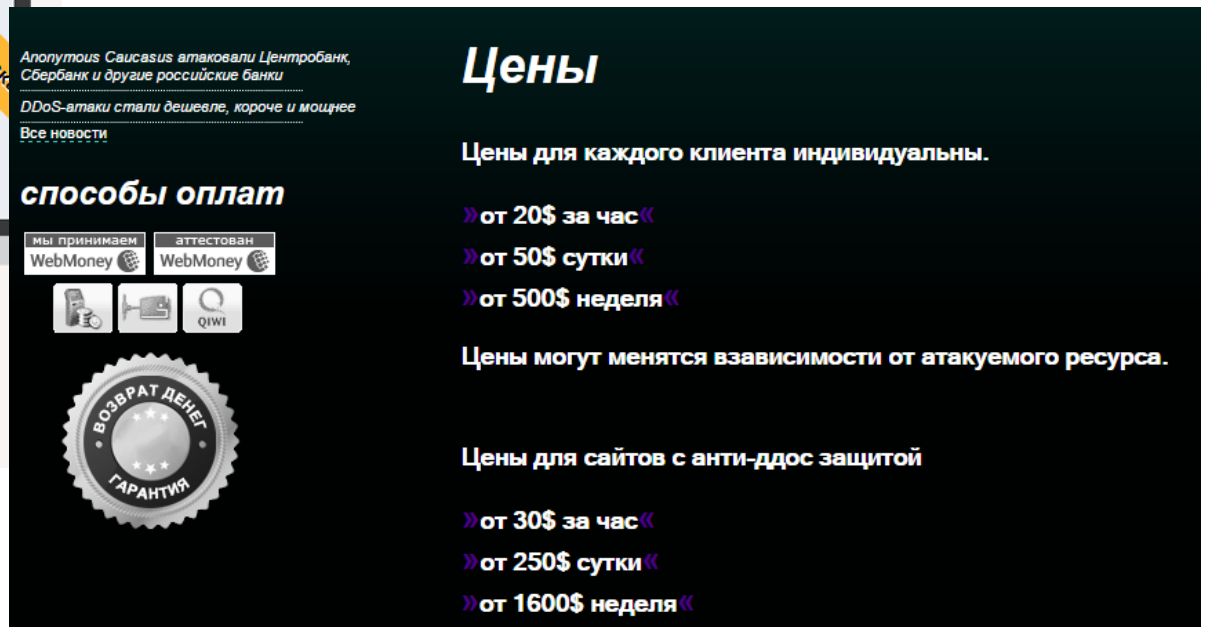
```
18            print "[+] Sent spoo
19        except:
20            print "[-] Could not
```

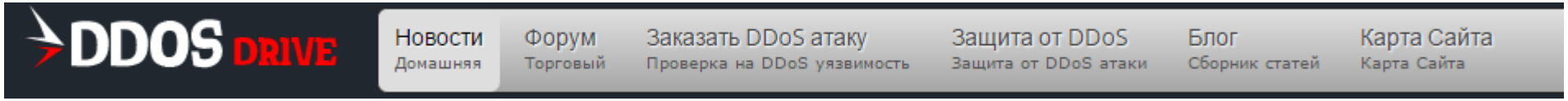
nmap –sU –pU:123 –Pn –n –script=ntp-monlist x.x.x.x/x

Билайн Бизнес

Дорого? Нет!







3. Цену на сайт определяем мы сами, конечная цена формируется исходя из следующих критериев ресурса на который Вы решили заказать ддос, а именно тематика, посещаемость, где расположен: на shared хостинге, VPS, VDS и конечно наличие анти-ддос защиты. При длительных заказах предусмотрены скидки (по договоренности).

4. За сайт расположенный на Shared хостинге цена от 50 WMZ.

5. За сайт расположенный на VPS сервере цена от 100 WMZ.

6. За сайт расположенный на VDS сервере цена от 150 WMZ.

7. За сайт пользующийся услугами анти-ддос компаний (перечислять не буду, потому что их сейчас много) цена от 400 WMZ.

Билайн Бизнес

Текущая ситуация

- DDoS атаки – серьезный бизнес
  - Уменьшение числа сверх объемных атак
  - Цель сделать атакуемый ресурс недоступным
- Организовать атаку можно не имея опыта
  - Готовые инструменты в Интернете
  - Множество злоумышленников готовых «помочь»
- Новые цели для атаки. Нет гарантий, что вас не атакуют завтра

Чего ждать?

- Лучше не будет
- Многовекторность – комбинация атак сетевого и уровня приложения
- Новые цели атаки
- Целевые DDoS атаки на клиентов

Билайн Бизнес

Спасибо за внимание!

Сабылин Владимир
e-mail Vsabylin@Beeline.ru
Mob +7 966 194 84 81