



Опыт оператора связи в борьбе с
внешними угрозами

Содержание

I. Взгляд оператора

II. Защита от DDoS. История, статистика, кейсы.

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



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**

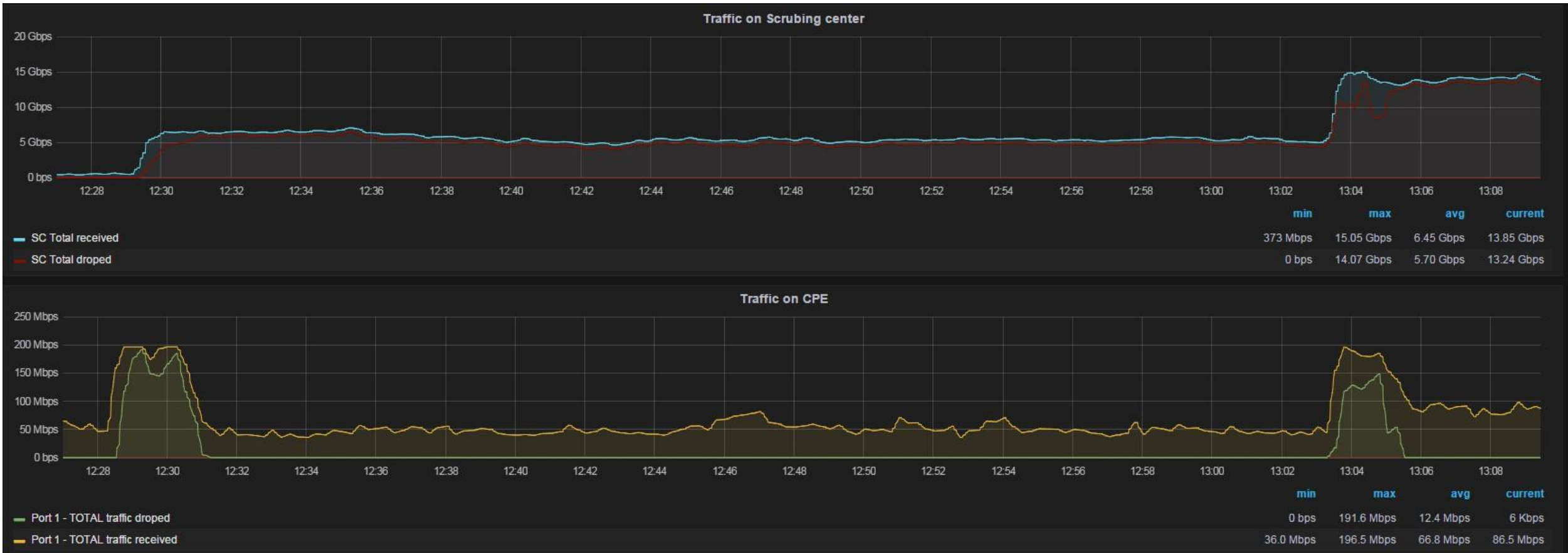


Цели и причины атак

- ▶ 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	1!
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]
13	37.000000	188.162.13.4	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, [REDACTED]
- Internet Protocol Version 4, Src: 207.99.73.170 (207.99.73.170), Dst: [REDACTED]
- 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 немного подробнее

BDoS Network Flood Attack

Attack Description

The Internet Control Message Protocol (ICMP) is widely used in network routing and connectivity diagnostics, as well as topology error reporting. ICMP is defined in RFC 792, later expanded to cover error notification through RFC 1122. The most popular ICMP message, the Echo request (also referred to as ping), requires the remote host to return a response to every received Echo request. This allows an attacker in

Attack Information

Attributes	Value
State	Footprint Applied
L4Checksum	57847,64545,56211,4...
TCP Sequence Number	N/A
IP ID Number	13330
DNS ID	N/A
DNS Query	N/A
Source Port	N/A
Source IP	109.225.253.90,77.87....
Destination Port	N/A
Destination IP	[REDACTED]
Fragmentation Offset	N/A
Fragmentation Flag	N/A
Flow Label	N/A
ToS	8
Packet Size	70,78

Footprint

[OR
checksum=57847,64545,56211,45155,42648,437,51
666,29779,32655,36074,4846,8215.]

Offset	Length	Protocol	Details
9	1.000000	ICMP	1530 Destination unreachable (Port unreachable) [ETHERNET FRAME CHECK SEQUENCE INCORRECT]
10	1.000000	ICMP	1530 Destination unreachable (Port unreachable) [ETHERNET FRAME CHECK SEQUENCE INCORRECT]
11	186.000000	ICMP	1530 Destination unreachable (Port unreachable) [ETHERNET FRAME CHECK SEQUENCE INCORRECT]
12	186.000000	ICMP	1530 Destination unreachable (Port unreachable) [ETHERNET FRAME CHECK SEQUENCE INCORRECT]
13	186.000000	ICMP	1530 Destination unreachable (Port unreachable) [ETHERNET FRAME CHECK SEQUENCE INCORRECT]

Frame 1: 1530 bytes on wire (12240 bits), 1530 bytes captured (12240 bits)

- Ethernet II, Src:** [REDACTED]
- Internet Protocol Version 4, Src: [REDACTED]
- Internet Control Message Protocol
 - Type: 3 (Destination unreachable)
 - Code: 3 (Port unreachable)
 - Checksum: 0x7f8f [correct]
- Internet Protocol Version 4, Src: [REDACTED], Dst: 176.197.143.50 (176.197.143.50)
- User Datagram Protocol, Src Port: 31970 (31970), Dst Port: ntp (123)
 - Source port: 31970 (31970)
 - Destination port: ntp (123)
 - Length: 16

Ботнет? Нет!

vpnguy / ntpdos

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

```
1 #!/usr/bin/env python
2 from scapy.all import *
3 import sys
4 import threading
5 import time
6 #NTP Amp DOS attack
7 #by DaRkReD
8 #usage ntpdos.py <target ip> <ntpserver list> <number of threads> ex: ntpdos.py 1.2.3.4 file.txt 10
9 #FOR USE ON YOUR OWN NETWORK ONLY
10
11
12 #packet sender
13 def deny():
14     #Import globals to function
15     global ntplist
16     global currentserver
17     global data
18     global target
```

```
74 print "Sending.."
```

```
75
```

```
76 #Keep alive so c
```

```
77 while True:
```

```
78     time.sleep
```

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

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 spoof
```

```
19
```

```
except:
```

```
20
```

```
print "[-] Could not
```

Дорого? Нет!

Виртуальный сервер VDS (VPS)

Операционная система

Конфигурация

Количество ядер процессора

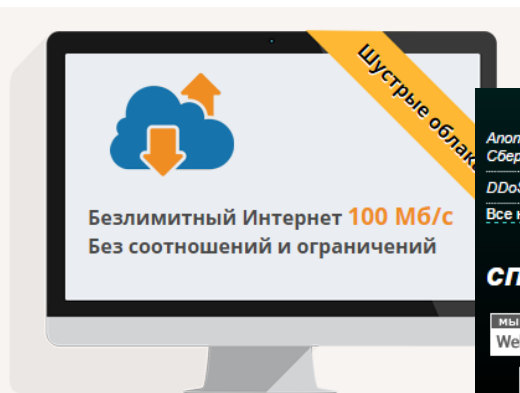
Оперативная память

Диск

Оборудование

Хеон 2,5 ГГц, DDR3 Хеон E5-26xx v3, DDR4

Стоимость 220 руб./мес.



Аполунтос Caucasus атаковали Центробанк, Сбербанк и другие российские банки
DDoS-атаки стали дешевле, короче и мощнее
Все новости

Цены

Цены для каждого клиента индивидуальны.

» от 20\$ за час «
» от 50\$ сутки «
» от 500\$ неделя «

Цены могут меняться в зависимости от атакуемого ресурса.

способы оплат

мы принимаем WebMoney аттестован WebMoney

Цены для сайтов с анти-ддос защитой

» от 30\$ за час «
» от 250\$ сутки «
» от 1600\$ неделя «

DDOS DRIVE [Новости Домашняя](#) [Форум Торговый](#) [Заказать DDoS атаку](#) Проверка на DDoS уязвимость [Защита от DDoS](#) Защита от DDoS атаки [Блог](#) Сборник статей [Карта Сайта](#) Карта Сайта

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.

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

Спасибо за внимание!



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