

Типовые ошибки в защите сети

Денис Батранков, консультант по ИБ,
CISSP, PCNSE, MVP Security

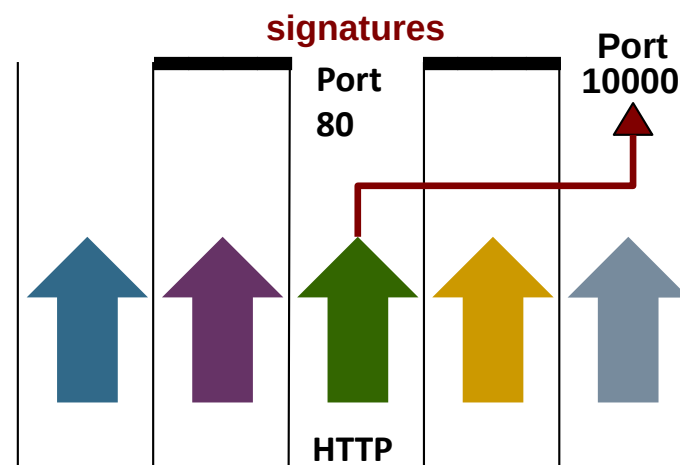
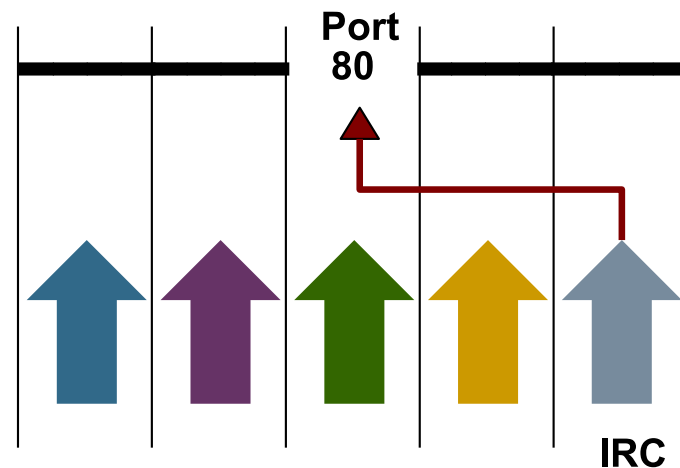
Palo Alto Networks Russia & CIS
Moscow-City
Russia@paloaltonetworks.com

Обход firewall – типовое явление



Ошибка: правила продолжают писать по портам

1. Распространение вредоносного ПО или нелегитимного трафика через открытые порты
 - нестандартное использование стандартных портов
 - создание новых специализированных протоколов для атаки
2. Использование стандартных протоколов на нестандартных портах – уклонение от сигнатурного сканирования



Пример обхода защиты: туннелирование поверх DNS

Примеры утилит

- tcp-over-dns
- dns2tcp
- Iodine
- Heyoka
- OzymanDNS
- NSTX

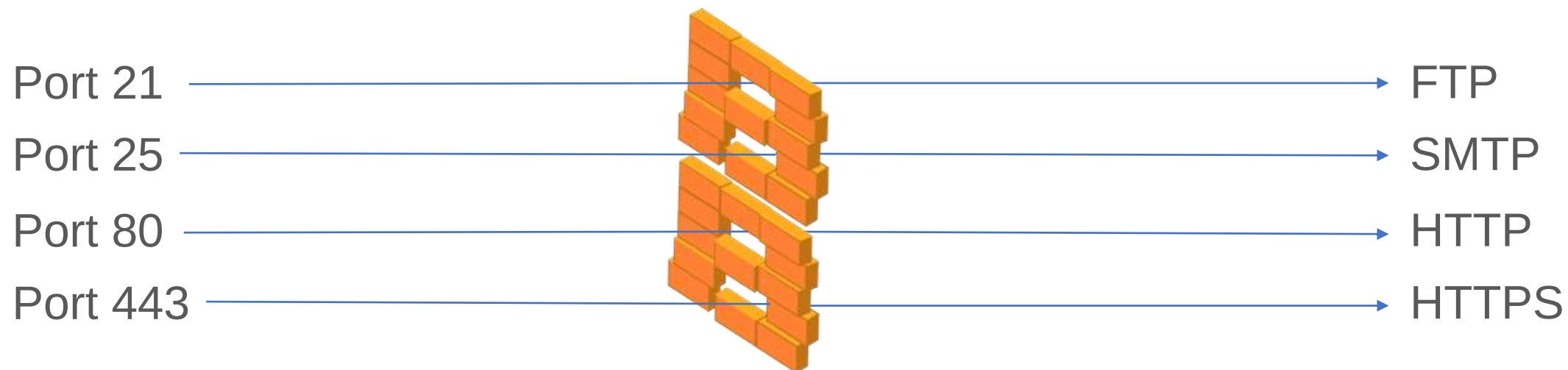
DNS	91	57916	53	Standard query TXT	AAAAAAh5AA.=auth.ec2.mui
DNS	213	53	57916	Standard query response TXT	
DNS	144	57916	53	Standard query TXT	2XKBgAABADFFNkQzMUNGOEE1
DNS	245	53	57916	Standard query response TXT	
DNS	98	57916	53	Standard query TXT	2XI7KiF1AHNzaA.=connect.
DNS	199	53	57916	Standard query response TXT	
DNS	85	57916	53	Standard query TXT	2XIAAAABBA.ec2.muides.co
DNS	240	53	57916	Standard query response TXT	
DNS	85	57916	53	Standard query TXT	2XIAAQACBA.ec2.muides.co
DNS	113	57916	53	Standard query TXT	2XIAAADCFNTSC0yLjAtT3Bl
DNS	85	57916	53	Standard query TXT	2XIAAAEBA.ec2.muides.co
DNS	253	57916	53	Standard query TXT	2XIAAAAFCAAAxQIFPLjhQeS
DNS	85	57916	53	Standard query TXT	2XIAAAAGBA.ec2.muides.co


```

Authority RRs: 1
Additional RRs: 1
  ▸ Queries
  ▾ Answers
    ▾ AAAAAAh5AA.=auth.ec2.muides.com: type TXT, class IN
      Name: AAAAAAh5AA.=auth.ec2.muides.com
      Type: TXT (Text strings)
      Class: IN (0x0001)
      Time to live: 3 seconds
      Data length: 34
      Text: A2XIAAAh5ADA5VzNLWkdJN0NLREwzREc
      Text:
    
```

Использование рекурсивных запросов для передачи инкапсулированных сообщений по TCP в запросах удаленному DNS серверу и ответах клиенту

80е годы



Один порт = 1 приложение

Теперь это не так

FTP

YUM

DELL-UPDATE

SMTP

Name	Tagged	Category	Subcategory	Risk	Technology	Standard Ports
 bbc-iplayer		media	photo-video	3	browser-based	tcp/80,554,1935
 bbcp		general-internet	internet-utility	2	client-server	tcp/5031-5039
 bbn-rcc-mon		networking	ip-protocol	1	network-protocol	
 beampro-telepresence		business-systems	general-business	1	peer-to-peer	udp/6868,6871
 beamyourscreen		collaboration	internet-conferencing	3	browser-based	tcp/443,80
 beats-music		media	audio-streaming	2	browser-based	tcp/80,443,1935
 bebo						
 bebo-base		collaboration	social-networking	3	browser-based	tcp/80,443
 bebo-mail		collaboration	email	3	browser-based	tcp/80
 bebo-posting		collaboration	social-networking	4	browser-based	tcp/80
 beinsync		networking	remote-access	2	client-server	tcp/443
 bet365		media	gaming	2	browser-based	tcp/80,443

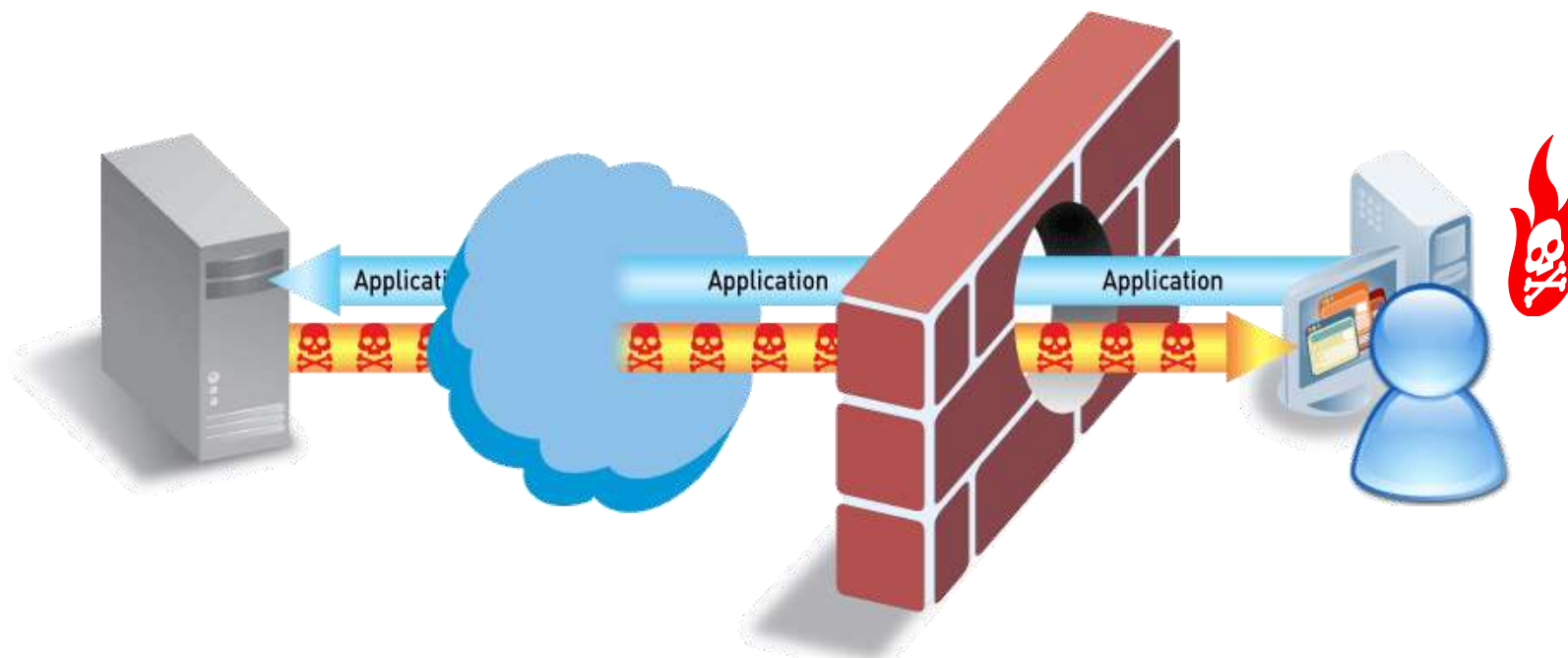
Ошибка: разрешаем небезопасные приложения

Приложения сами могут быть “угрозами”

- P2P file sharing, туннельные приложения, анонимайзеры, мультимедиа, TOR, Bitcoin

Приложения могут способствовать распространению угроз

- Основные угрозы – это угрозы уровня приложений



Приложения и угрозы уровня приложений создают бреши в системе безопасности

Какую часть сетевого трафика теперь надо проверять?

Пакет

Данные приложения	TCP Port 80	Source Address	Destination Address
-------------------	-------------	----------------	---------------------

Традиционно:

Приложение = номер порта (напр., HTTP = 80)

Пакет

Данные приложения	TCP Port 80	Source Address	Destination Address
-------------------	-------------	----------------	---------------------

Новое определение:

Приложение = Специфические передаваемые данные
flash = данные для анимации Adobe Player внутри браузера

Что Вы видите со старым firewall?

Много
трафика
по порту
80

Много
трафика
по порту
21

Много
трафика
по порту
53

Много
трафика
по порту
25

NGFW: Вашей сетью пользуется 200-300 приложений



Вам нужно разрешить программистам VNC.
Какие порты открывать?

Правила писать в L7 firewall удобнее, потому что не надо помнить порты

	Name	Source			Destination		Application	Service	Action	Profile
		Zone	Address	User	Zone	Address				
6	Allow VNC	any	any	 programmers	 Outside	any	 vnc	 application-default	 Allow	

L7 Firewall помнит стандартные порты каждого приложения

Name	Tagged	Category	Subcategory	Risk	Technology	Standard Ports
 pocketcloud		networking	remote-access		client-server	tcp/443,3389,5222,5228,udp/dynamic
 sina-uc (1 out of 5 shown)						
 sina-uc-remote-control		networking	remote-access		client-server	udp/8001,dynamic
 vnc						
 vnc-base		networking	remote-access		client-server	tcp/5500,tcp/5900,5901
 vnc-chat		collaboration	instant-messaging		client-server	tcp/5800,5900
 vnc-clipboard		networking	remote-access		client-server	tcp/5900,5901
 vnc-encrypted		networking	remote-access		client-server	tcp/5900,5901
 vnc-filetransfer		networking	remote-access		client-server	tcp/5900,5901
 vnc-print		networking	remote-access		client-server	tcp/5900,5901
 vnc-http		networking	remote-access		browser-based	tcp/5800



Разница между межсетевым экраном L4 и L7

slideshare-uploading		
application function		
PowerPoint	slideshare	"Confidential and Proprietary"
file type	application	content
marketing	HTTP	file-sharing
group	protocol	URL category
rivanov	SSL	canada
user	protocol	destination country
172.16.1.10	TCP/443	64.81.2.23
source IP	destination port	destination IP

T
R
A
N
S
P
O
R
T

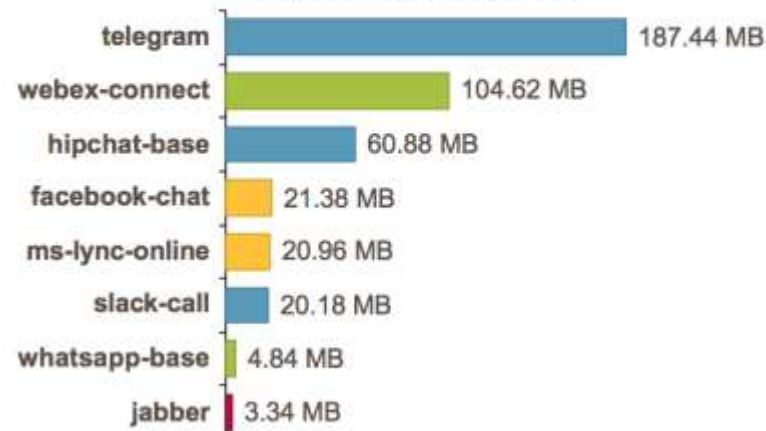
A
P
P
L
I
C
A
T
I
O
N

Instant-Messaging - 426.72MB

23 9

APPLICATION VARIANTS
VS INDUSTRY AVERAGE

TOP INSTANT-MESSAGING APPS

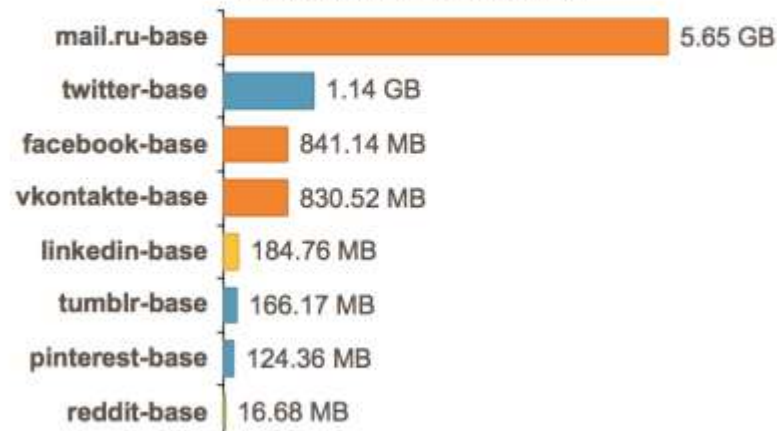


Social-Networking - 8.92GB

22 1

APPLICATION VARIANTS
VS INDUSTRY AVERAGE

TOP SOCIAL-NETWORKING APPS



Gaming - 342.5MB

14

APPLICATION VARIANTS
VS INDUSTRY AVERAGE

TOP GAMING APPS

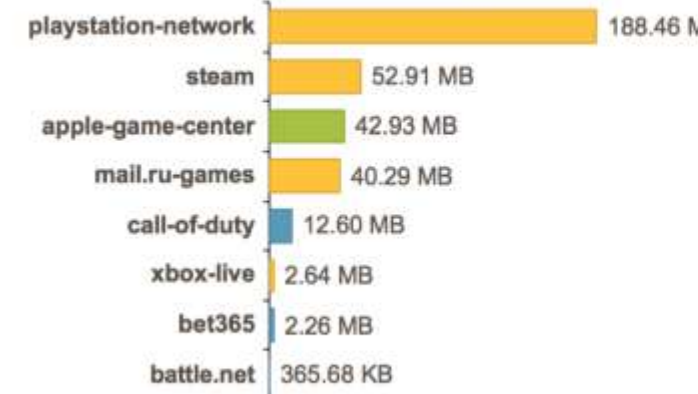
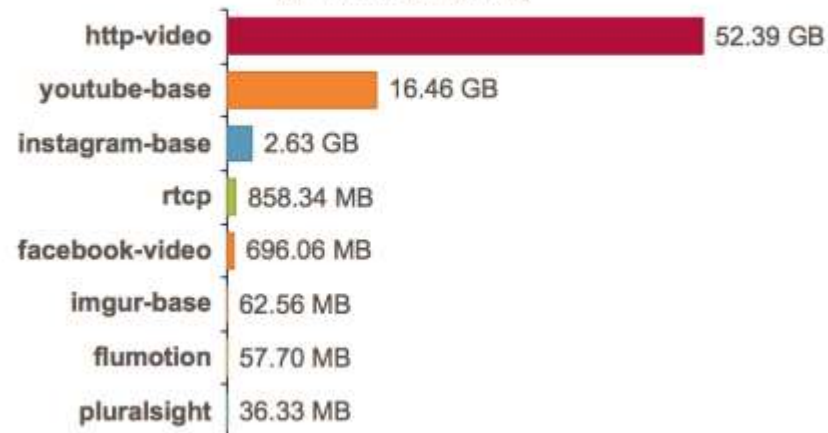


Photo-Video - 73.27GB

26 22

APPLICATION VARIANTS
VS INDUSTRY AVERAGE

TOP PHOTO-VIDEO APPS



Proxy - 698.5MB

1

APPLICATION VARIANTS
VS INDUSTRY AVERAGE

TOP PROXY APPS

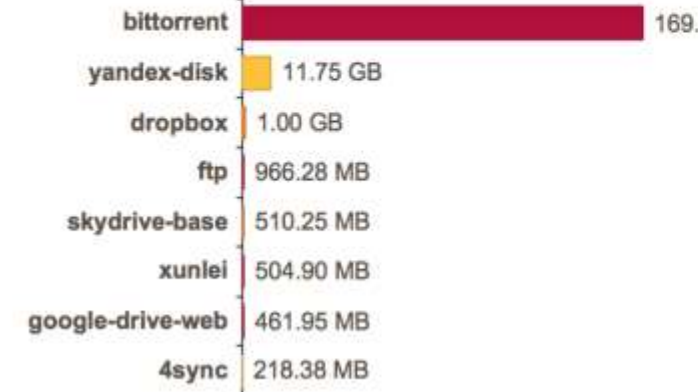


File-Sharing - 184.79GB

28

APPLICATION VARIANTS
VS INDUSTRY AVERAGE

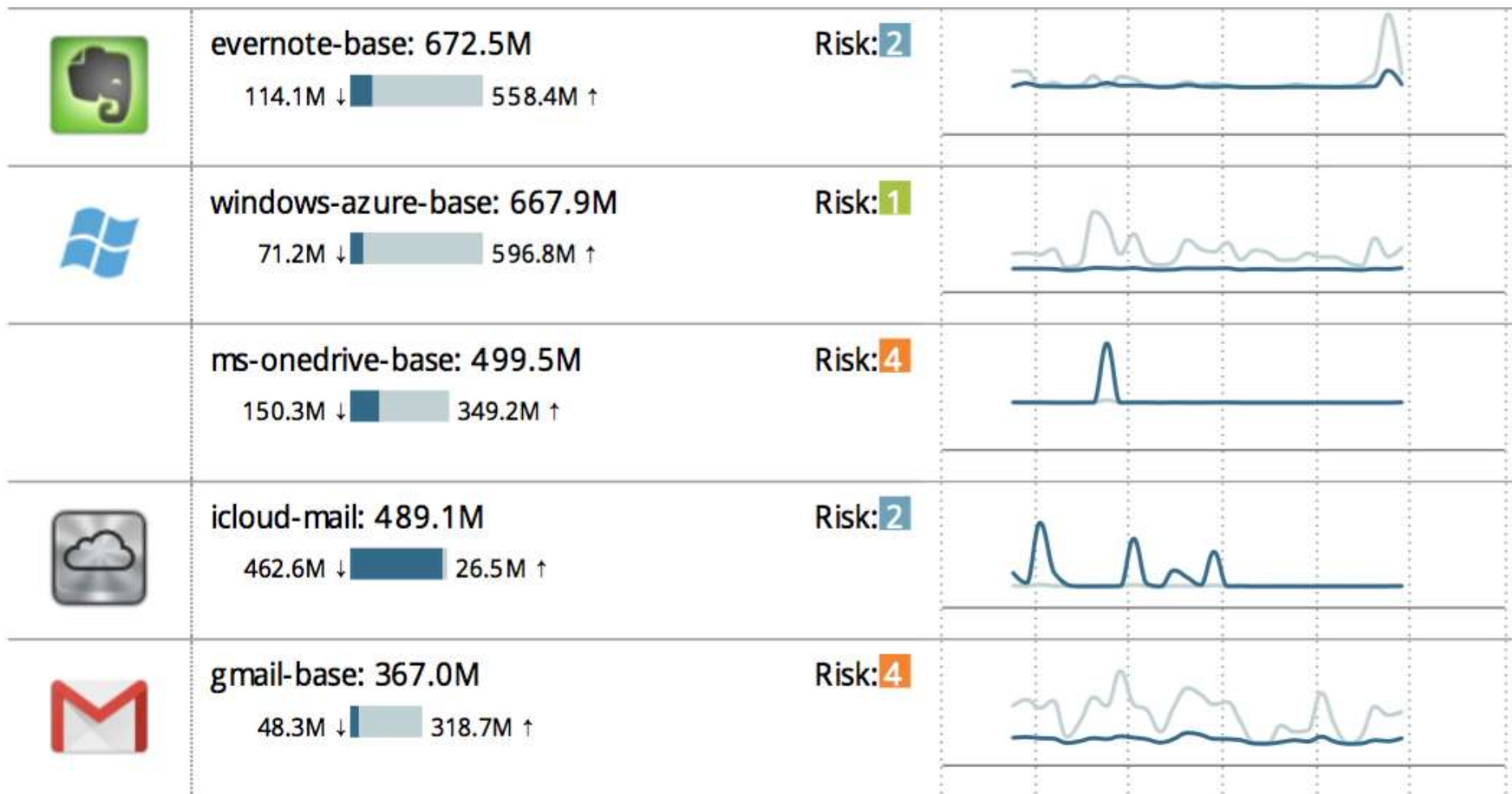
TOP FILE-SHARING APPS



Отчет SLR позволяет
показать приложения,
вирусы, атаки, бот-сети

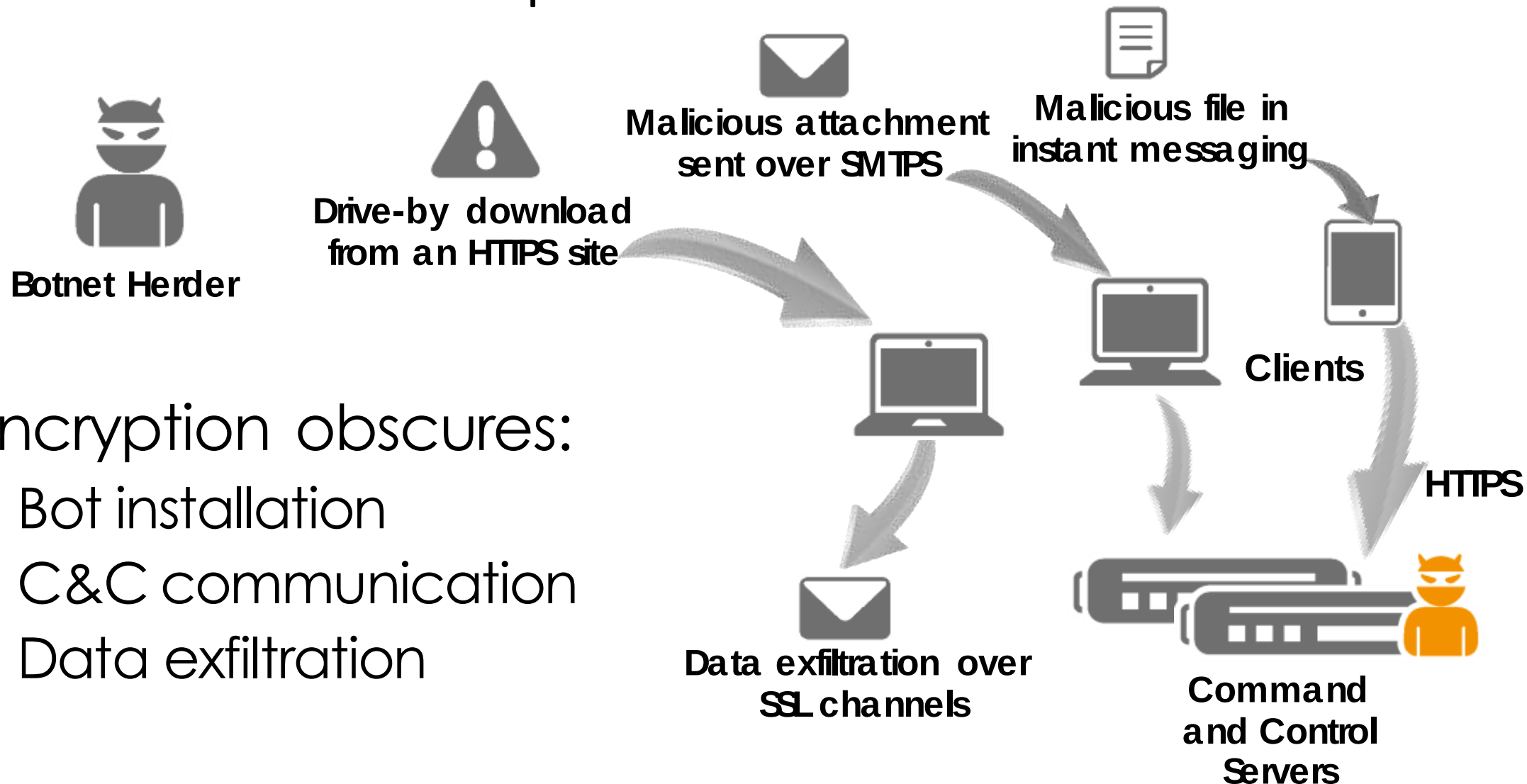
Отчет по приложениям и угрозам Security Lifecycle Report (SLR)

Ошибка: игнорируется использование SaaS



Используем компонент **Aperture** для защиты облачных ресурсов компании

Атаки через SSL



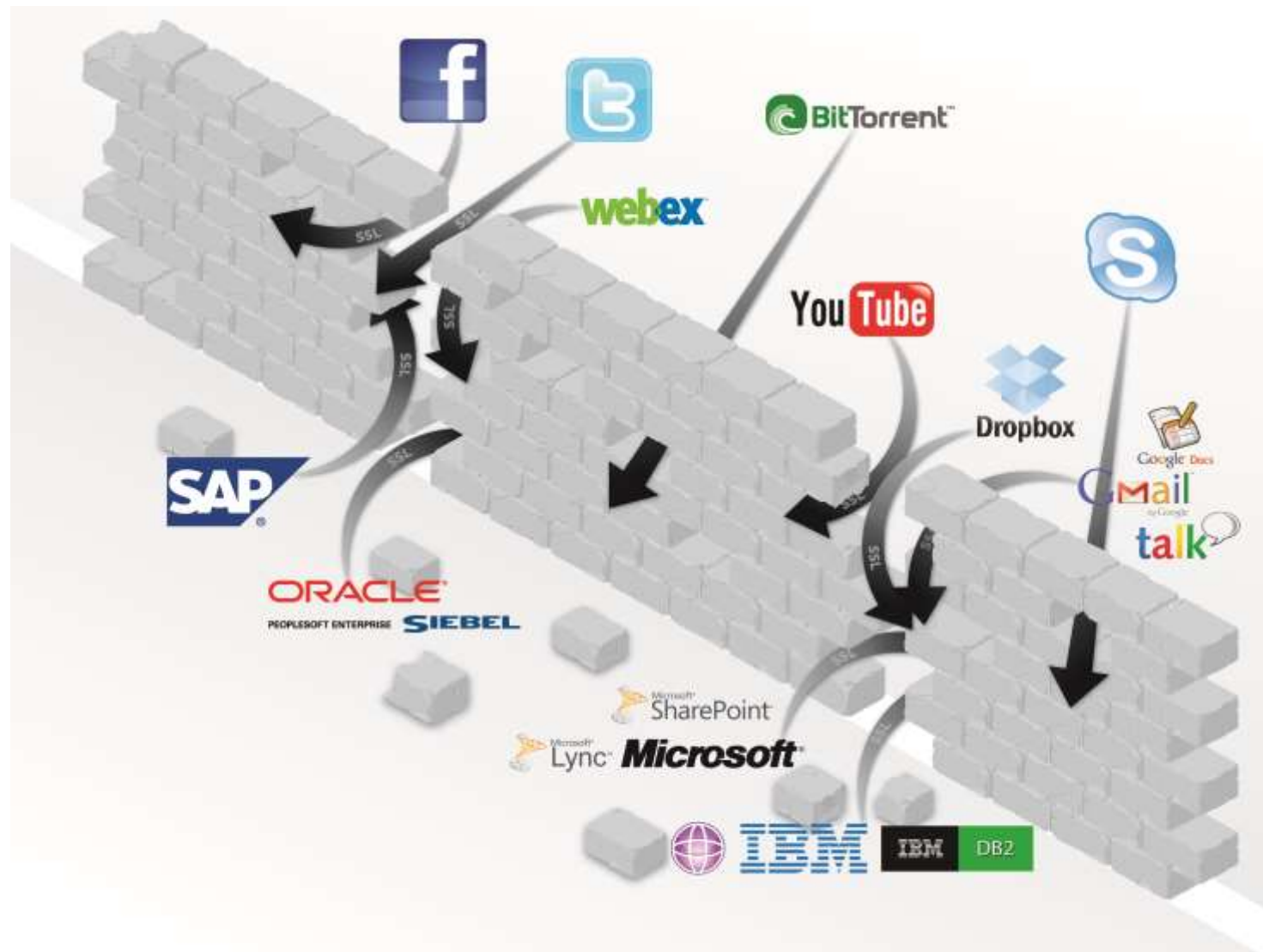
- Encryption obscures:
 - Bot installation
 - C&C communication
 - Data exfiltration

Ошибка: игнорируем зашифрованные каналы

Что сотрудники передают
через зашифрованные
каналы?

Применение шифрования:

- SSL
- Специальные протоколы шифрования



Статистика: SSL зашифрована треть трафика сети

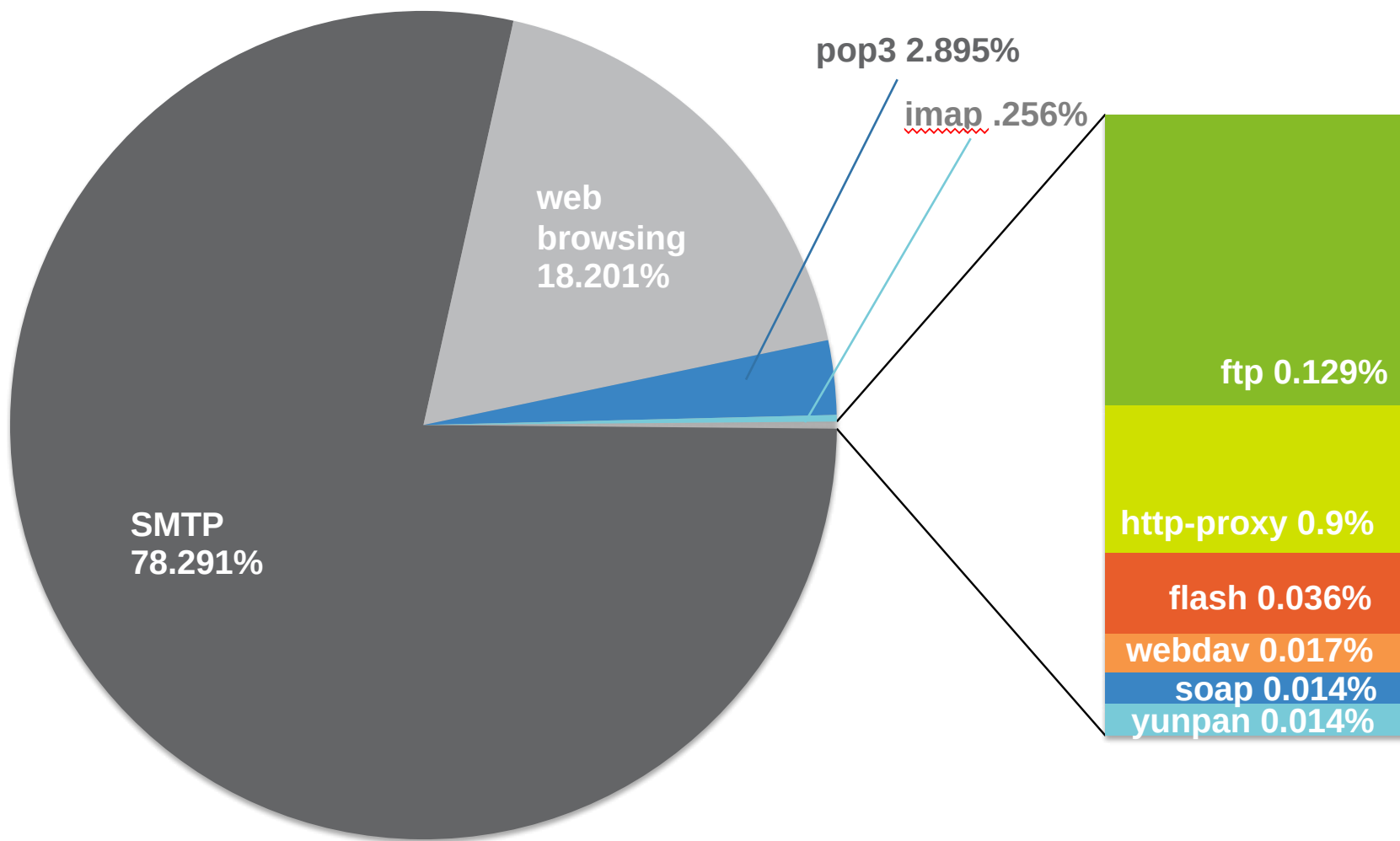


Доверяй, но проверяй!

Ошибка: ищем только известные плохие файлы антивирусом

неизвестные	Неизвестные хорошие	Неизвестные плохие
	Известные хорошие	Известные плохие (есть сигнатура)
хорошие		плохие

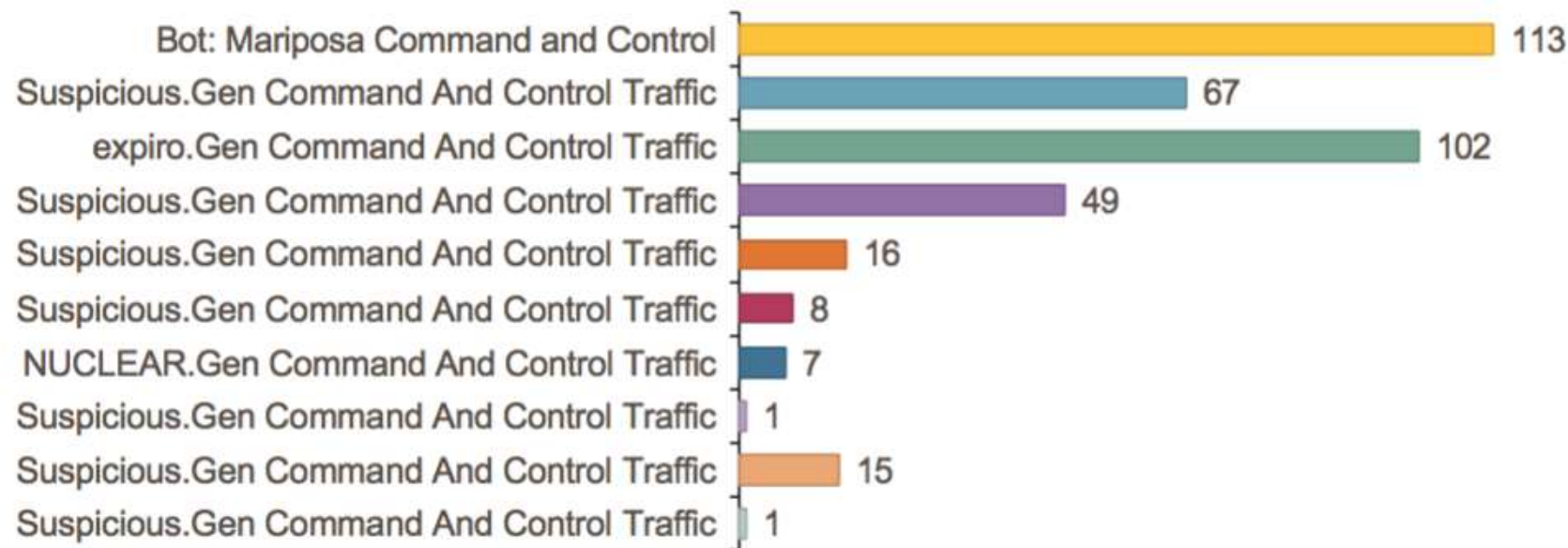
ТОР 10 приложений доставляющие неизвестное вредоносное ПО (статистика песочницы Wildfire по количеству сессий)



Сколько компьютеров в бот-сети?

Шпионское ПО, осуществляющее соединение с внешними узлами **2,606**

Рисунок ниже демонстрирует взломанные хосты, которые осуществляют попытки соединения с подозрительными внешними серверами.



Ошибка: неверный сайзинг устройства

- Требуется в T3 производительность при включенной одной функции
- Требуется в T3 включить подписки на весь функционал, например, IPS, антивирус, URL
- Оценивается число сессий L4 вместо L7
- Оценивается скорость Firewall, вместо скорости Firewall+IPS+антивирус+URL+песочница



2 НОЯБРЯ 2017 МОСКВЕ



ВОПРОСЫ

