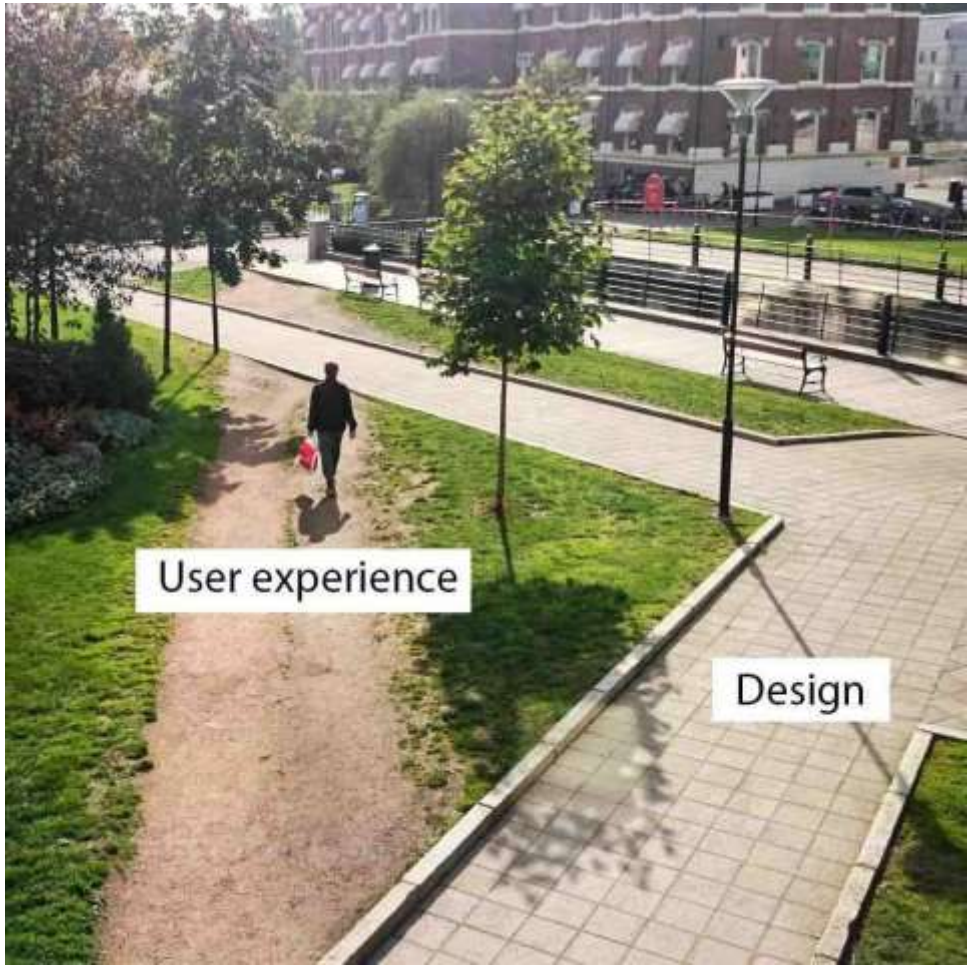
# Типовые ошибки в защите сети

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

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

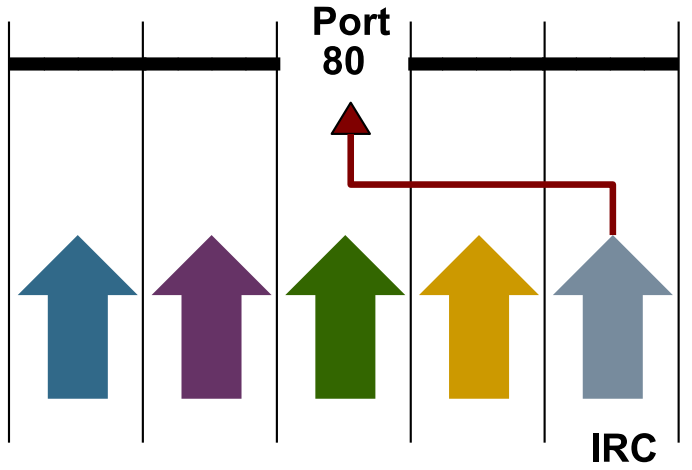
# Обход firewall – типовое явление

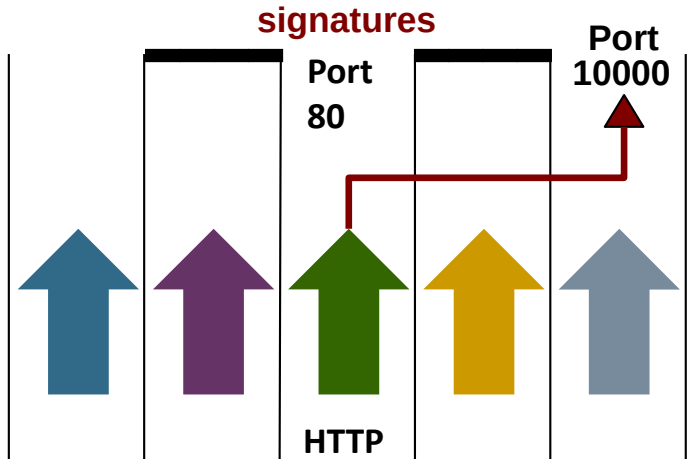


# Ошибка: правила продолжают писать по портам

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

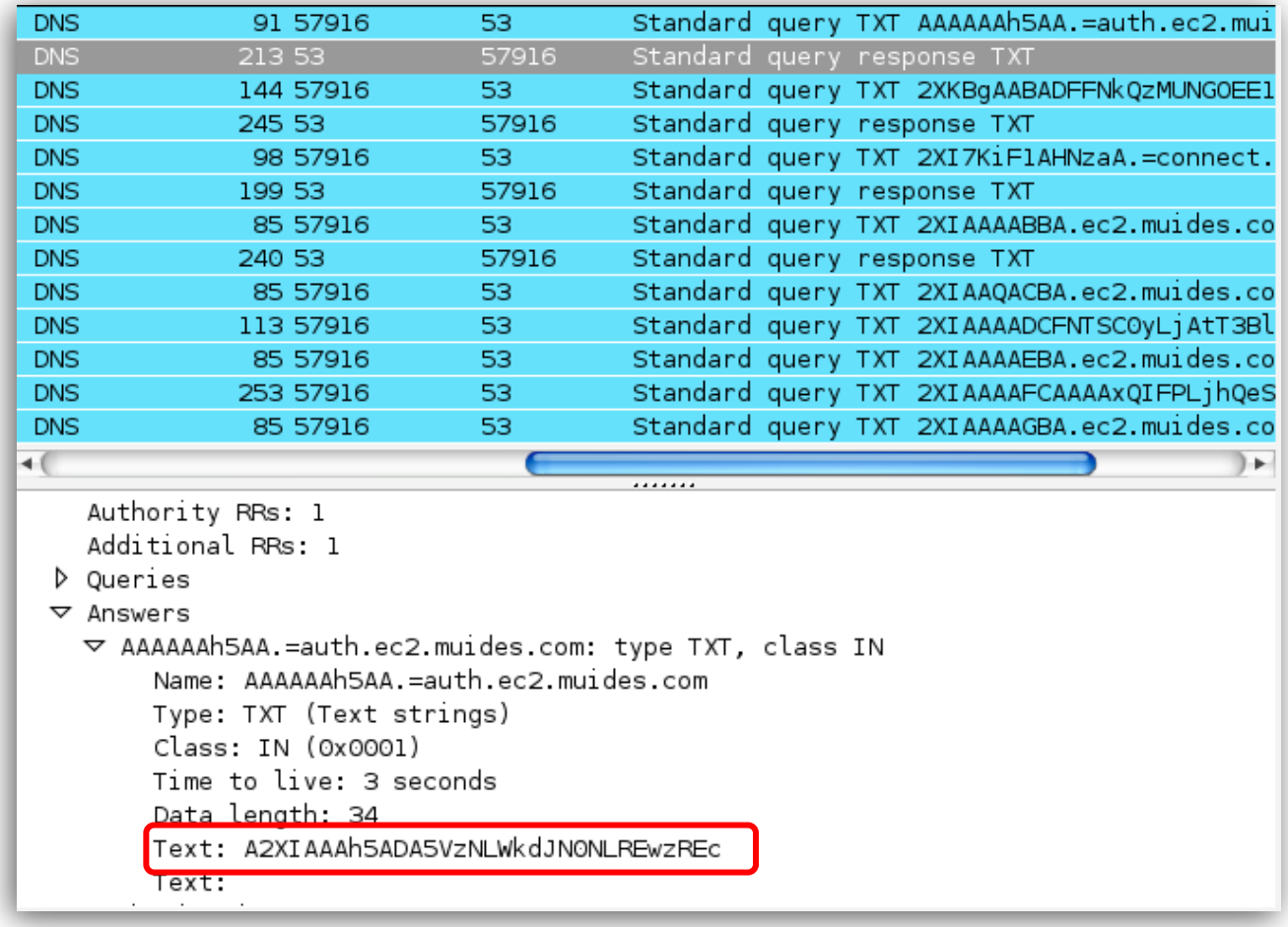


# Пример обхода защиты: туннелирование поверх DNS

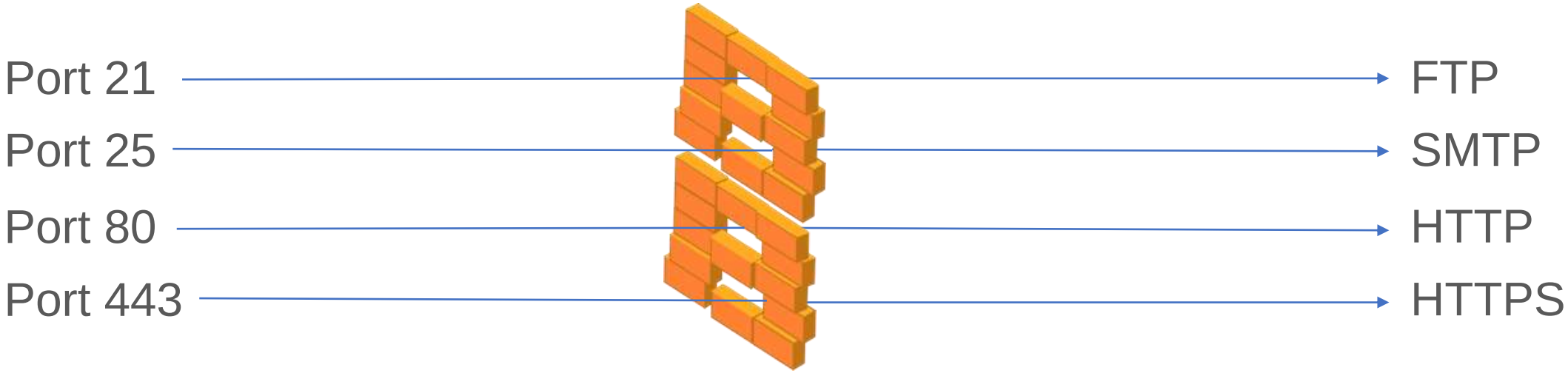
## Примеры утилит

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




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

## 80е годы




**Один порт = 1 приложение**

FTP

YUM

DELL-UPDATE

SMTP

## Теперь это не так

| 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 |

https://applipedia.paloaltonetworks.com/

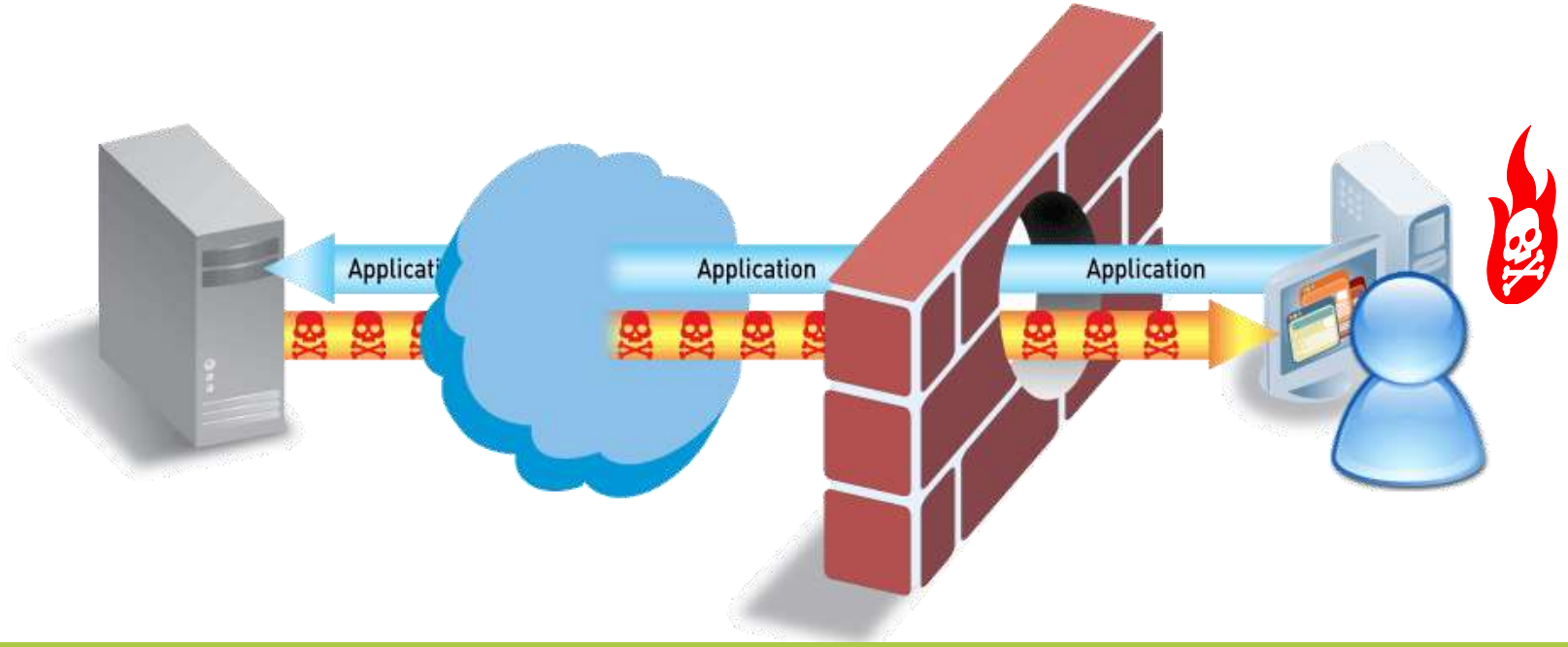
# Ошибка: разрешаем небезопасные приложения

## Приложения сами могут быть “угрозами”

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

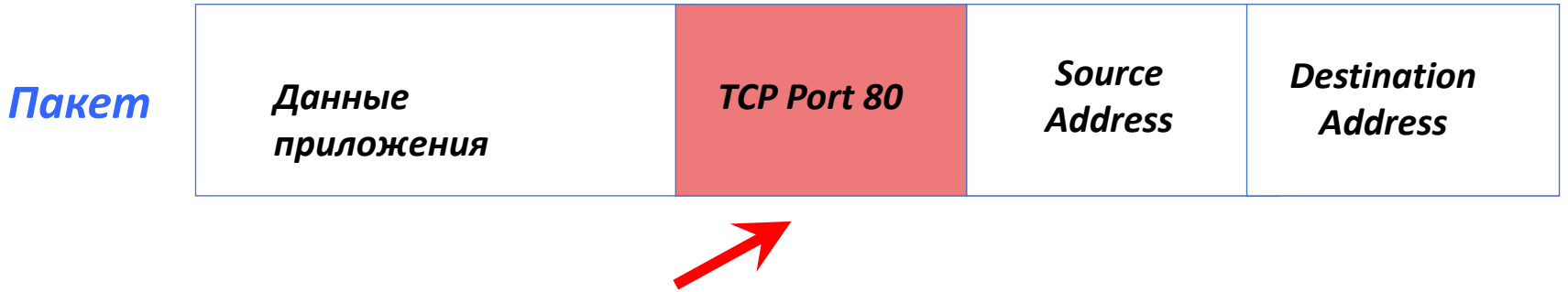
## Приложения могут способствовать распространению угроз

- Основные угрозы – это угрозы уровня приложений




Приложения и угрозы уровня приложений создают бреши в системе безопасности

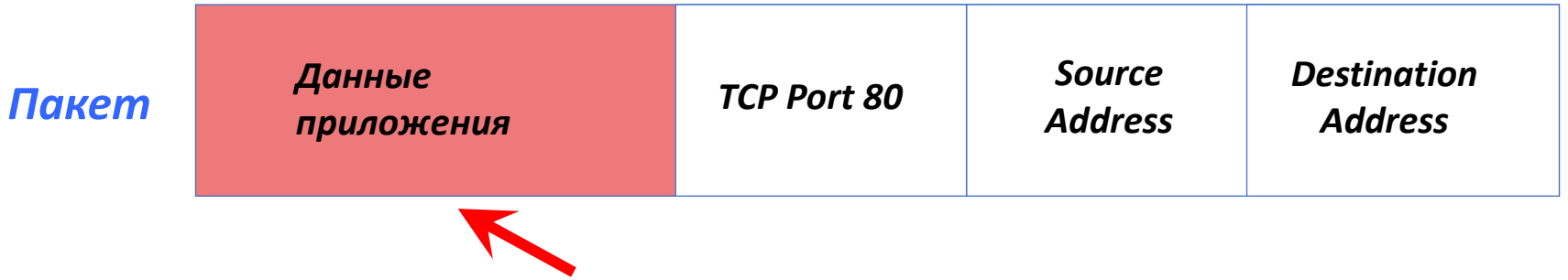
# Какую часть сетевого трафика теперь надо проверять?




***Традиционно:***

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

---




***Новое определение:***

***Приложение = Специфические передаваемые данные***

***flash = данные для анимации Adobe Player внутри браузера***

# Что Вы видите со старым firewall?

# 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 | 1 | client-server | tcp/443,3389,5222,5228,udp/dynamic |
| sina-uc (1 out of 5 shown) | | | | | | |
| sina-uc-remote-control | | networking | remote-access | 2 | client-server | udp/8001,dynamic |
| vnc | | | | | | |
| vnc-base | | networking | remote-access | 5 | client-server | tcp/5500,tcp/5900,5901 |
| vnc-chat | | collaboration | instant-messaging | 1 | client-server | tcp/5800,5900 |
| vnc-clipboard | | networking | remote-access | 2 | client-server | tcp/5900,5901 |
| vnc-encrypted | | networking | remote-access | 2 | client-server | tcp/5900,5901 |
| vnc-filetransfer | | networking | remote-access | 3 | client-server | tcp/5900,5901 |
| vnc-print | | networking | remote-access | 2 | client-server | tcp/5900,5901 |
| vnc-http | | networking | remote-access | 5 | browser-based | tcp/5800 |

# Разница между межсетевым экраном L4 и L7

slideshare-uploading
application function

PowerPoint
file type

slideshare
application

“Confidential and Proprietary”
content

marketing
group

HTTP
protocol

file-sharing
URL category

rivanov
user

SSL
protocol

canada
destination country

172.16.1.10
source IP

TCP/443
destination port

64.81.2.23
destination IP

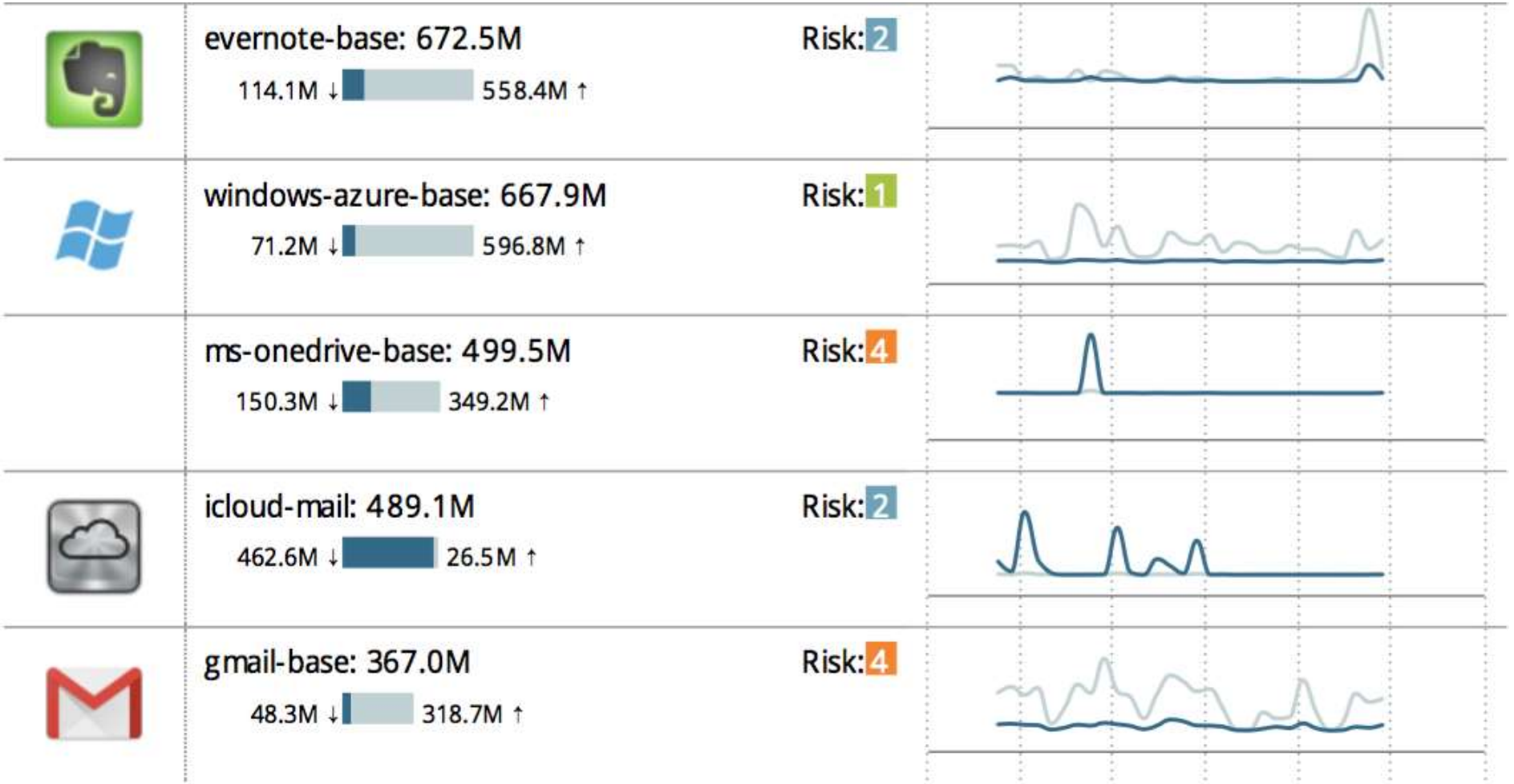
TRANSPORT

APPLICATION


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

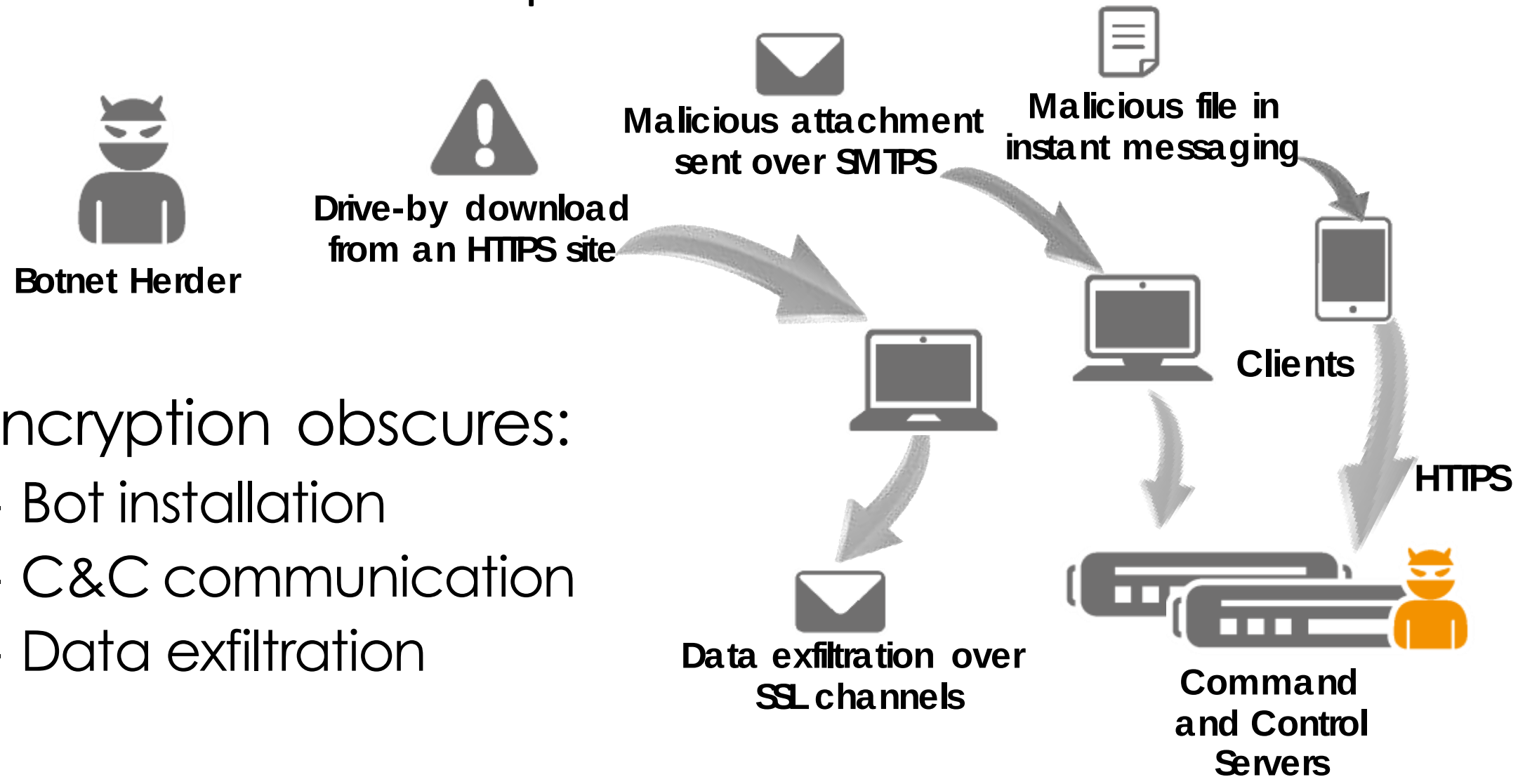
# Отчет по приложениям и угрозам Security Lifecycle Report (SLR)

# Ошибка: игнорируется использование SaaS




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

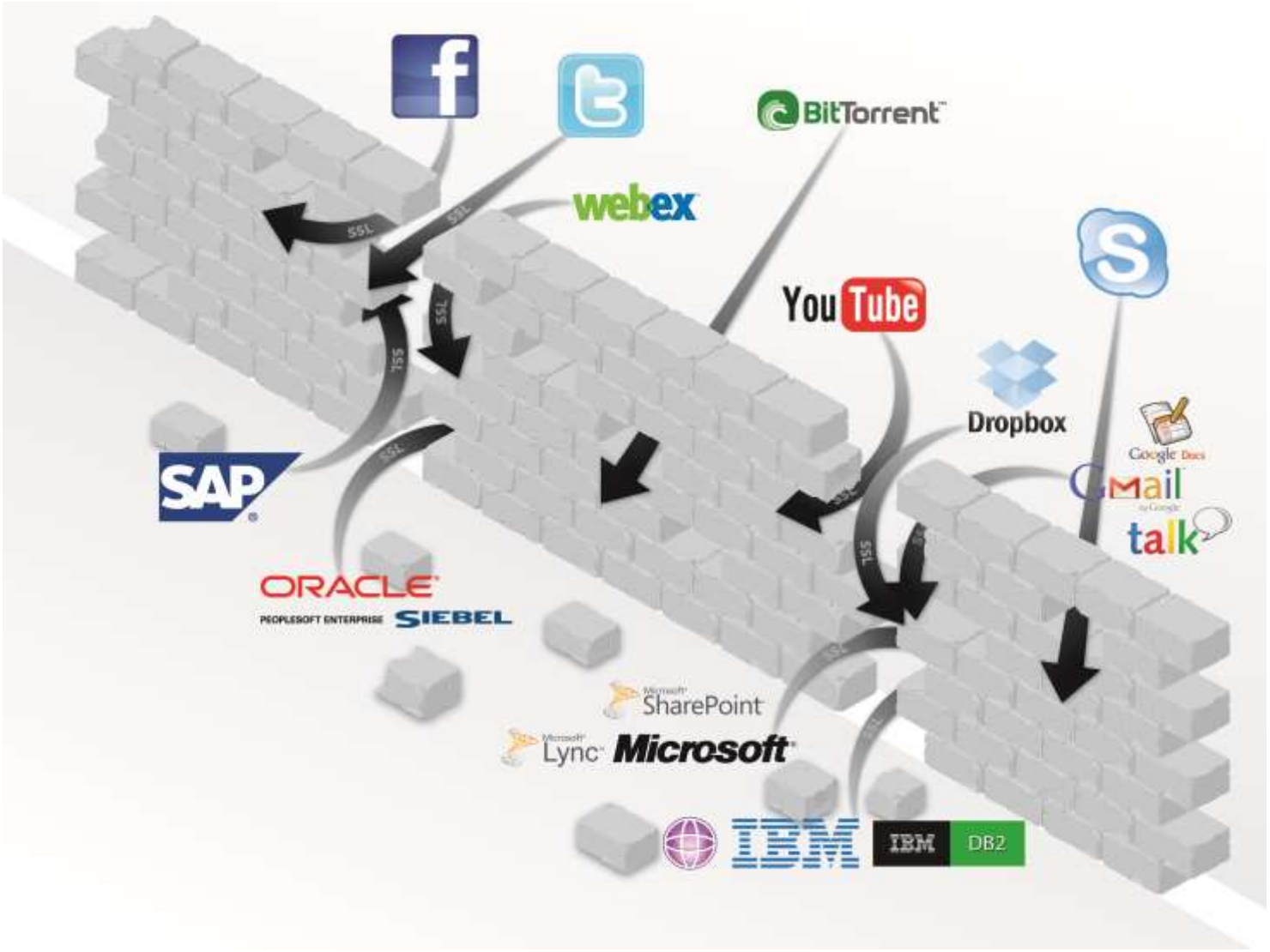
# Атаки через SSL




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

# Ошибка: игнорируем зашифрованные каналы

Что сотрудники передают через зашифрованные каналы?



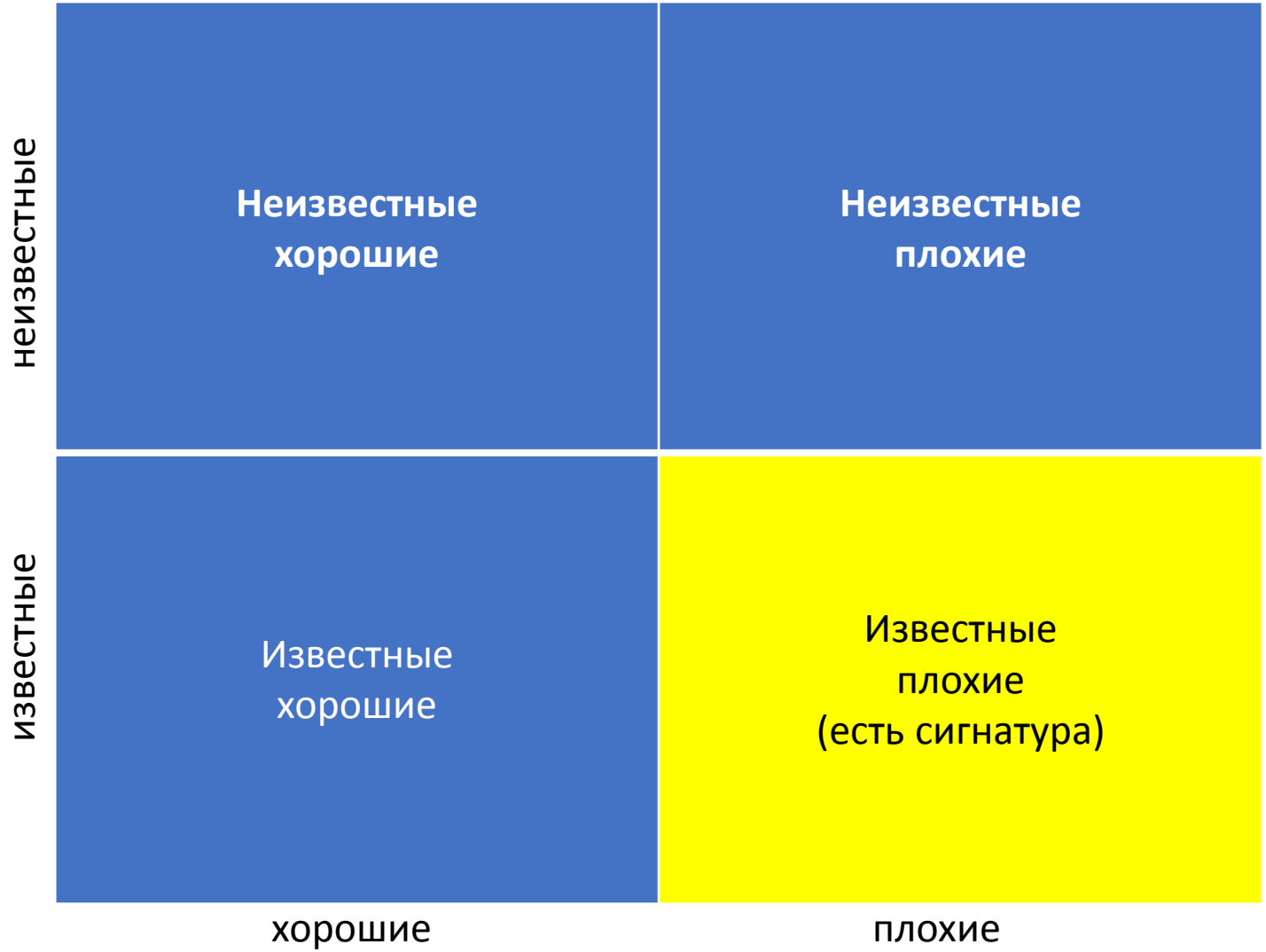

**Применение шифрования:**

- **SSL**
- **Специальные протоколы шифрования**

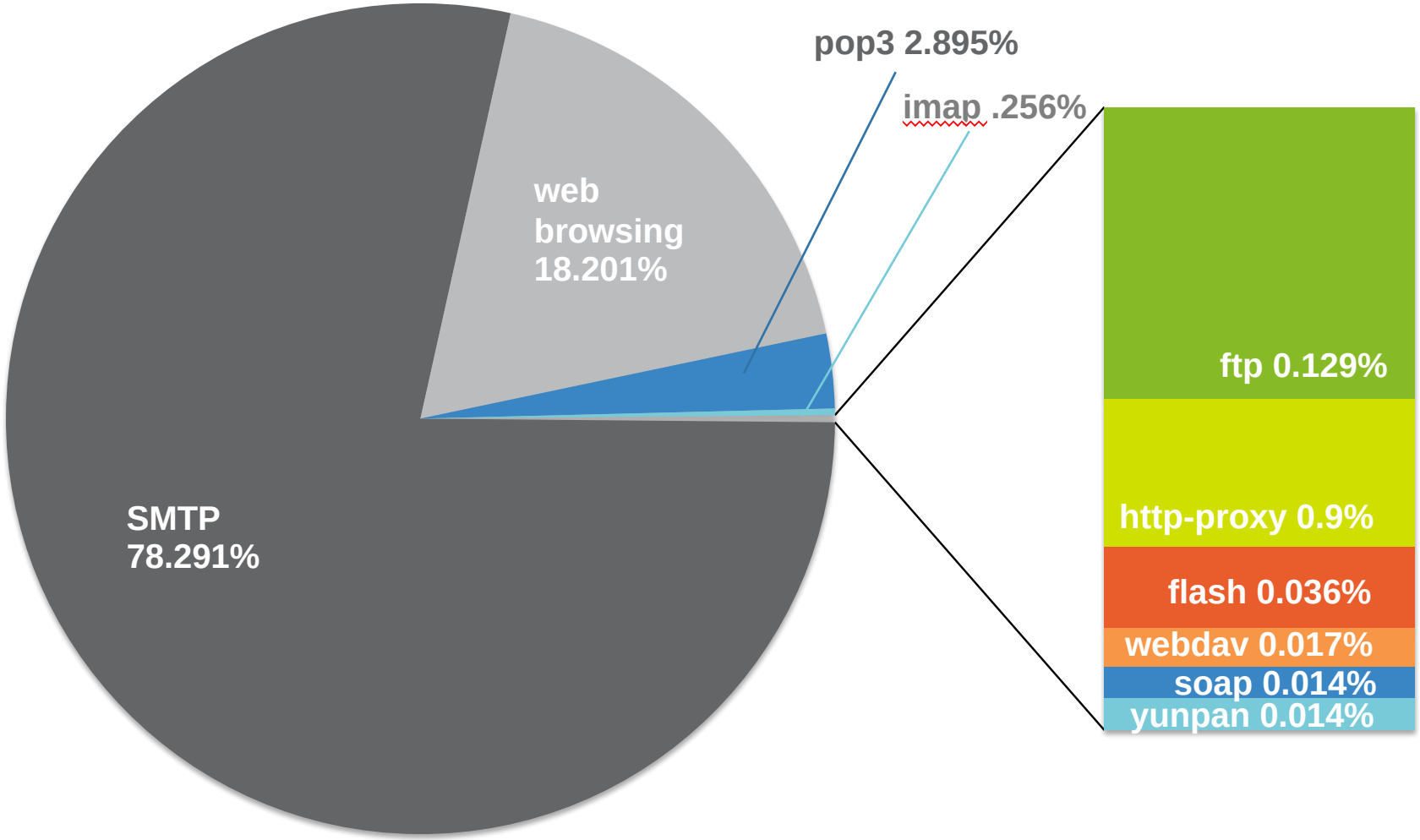
# Статистика:
# SSL зашифрована треть трафика сети

**Доверяй, но проверяй!**

# Ошибка: ищем только известные плохие файлы антивирусом



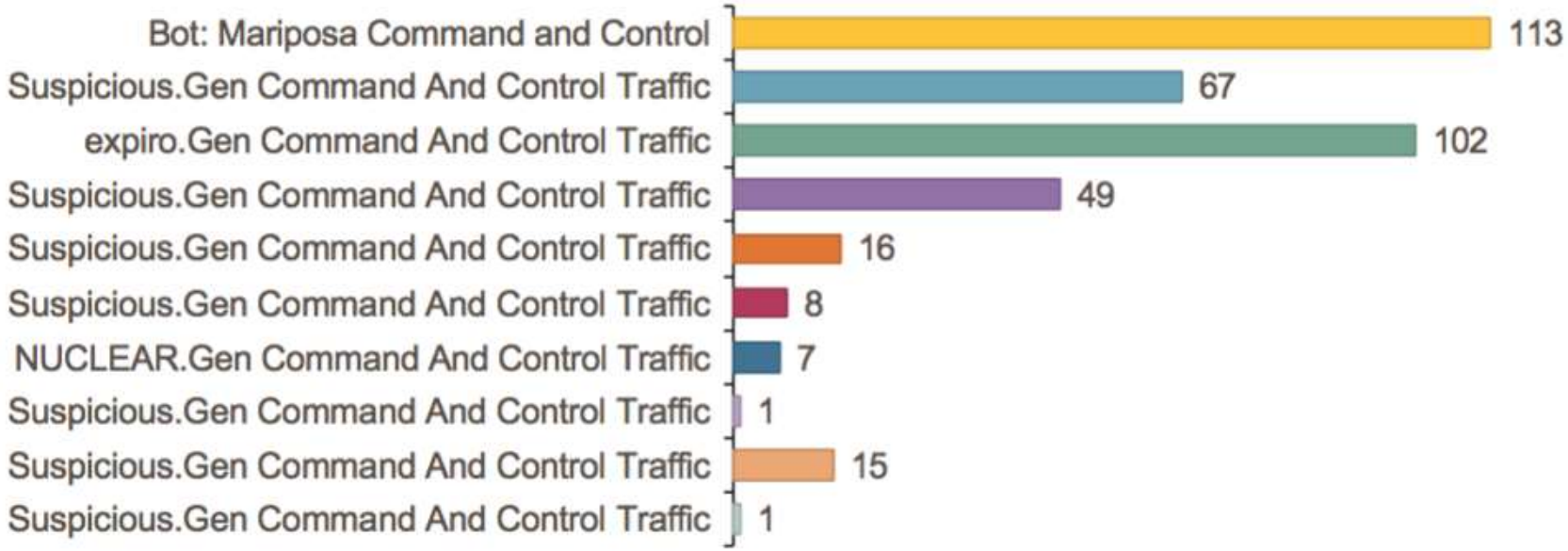
# TOP 10 приложений доставляющие неизвестное вредоносное ПО (статистика песочницы Wildfire по количеству сессий)



# 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 ТЗ производительность при включенной одной функции
- Требуется в ТЗ 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

# ВОПРОСЫ