SolidеX

Некоторые «модные» темы информационной безопасности

13 июля 2012 г.

Содержание

Solidex

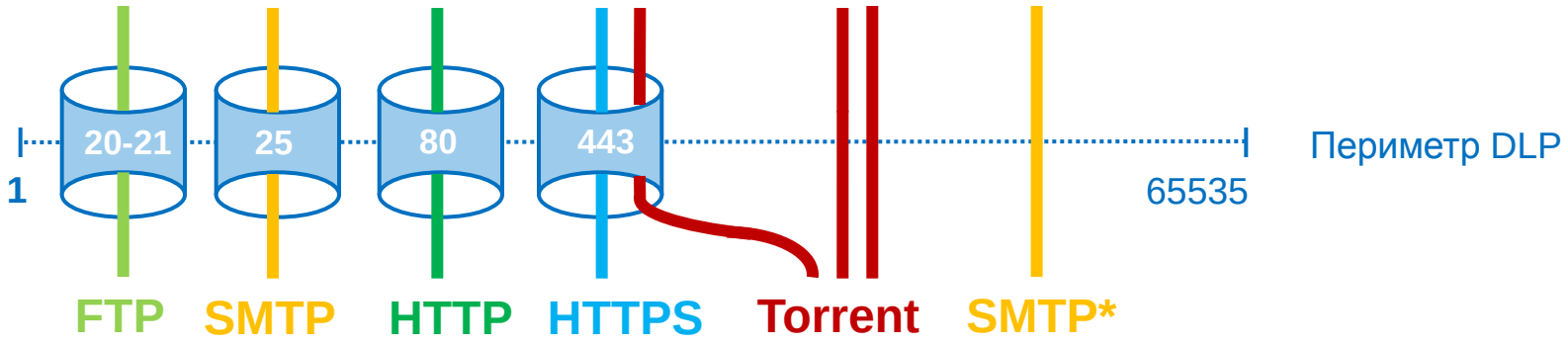
- Data Loss Prevention (DLP)
- Advanced Persistent Threat (APT)
- Vulnerability Management (VM)
- Бонус

Ожидания от DLP

Solidex

- Предотвращение утечек данных по «хорошо известным» каналам
- Перлюстрация канала Skype
- Проверка содержимого SSL/TLS-туннелей

Каналы утечки данных



* - протокол вне стандартного порта

- Контролируется узкий перечень портов по принципу proxy
- Неконтролируемый трафик:
  - «Маскируется» в разрешенных каналах
  - Обходит proxy-порты

Этот подход используется некоторыми продуктами на рынке DLP

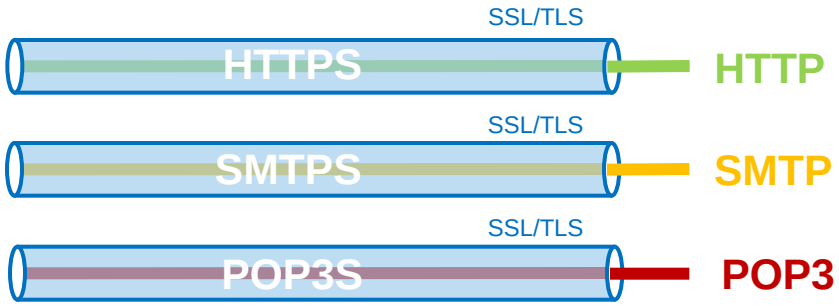
Как перлюстрировать Skype?

- Шифрованный канал Skype = только агент (plugin)
- Но: агента можно отключить
- Если подход «агентский»:
  - Дополнительные каналы (к примеру, Torrent) потребуют установки других агентов
  - Важно удостоверится, что агент не конфликтует с другим ПО (например, AV) и не влияет на производительность рабочей станции

Контроль Skype

- Стоит ли перлюстрировать Skype, если механизмы инспекции не надежны?
- От перлюстрации к контролю: определить политикой ИБ использование приложений таких как Skype и категорий приложений File Sharing, IM, Social Networking

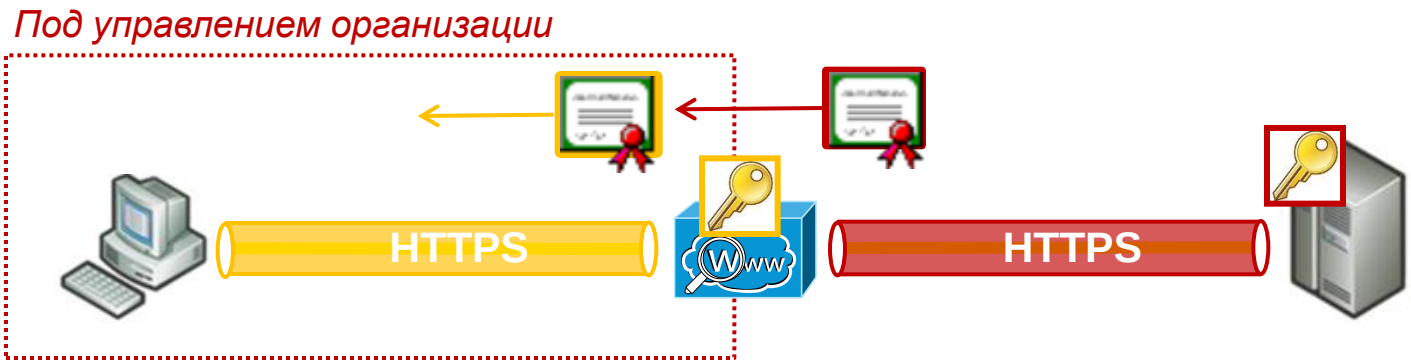
Контроль SSL/TLS-туннелей



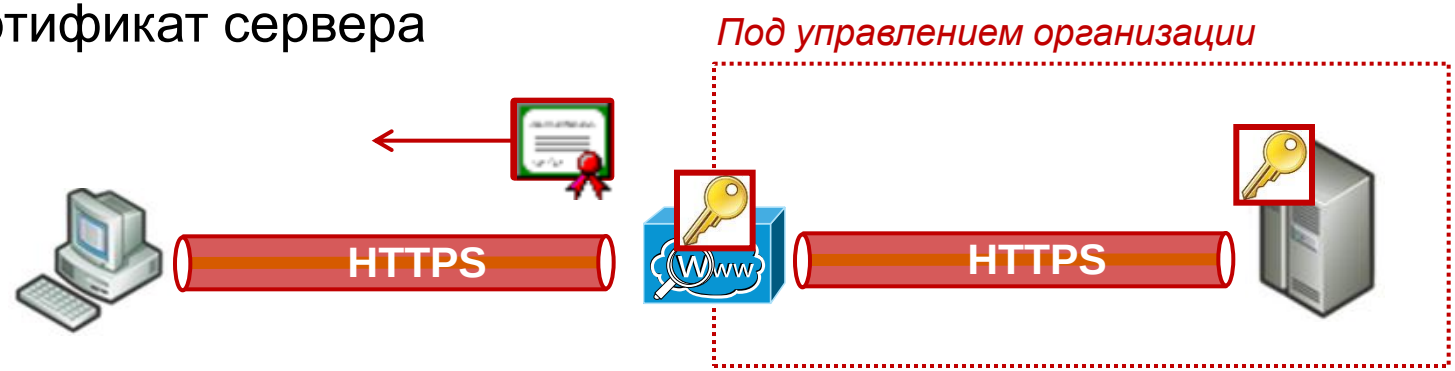
- HTTPS = HTTP внутри SSL/TLS-туннеля
- Перлюстрировать HTTPS недостаточно (хотя именно это некоторые российские продукты DLP и делают)– необходимо проверять содержимое SSL/TLS-туннелей

Сценарии применения SSL/TLS-инспекции

- Защита пользователя. Закрытый ключ сервера не известен. SSL/TLS-инспектор подменяет сертификат сервера

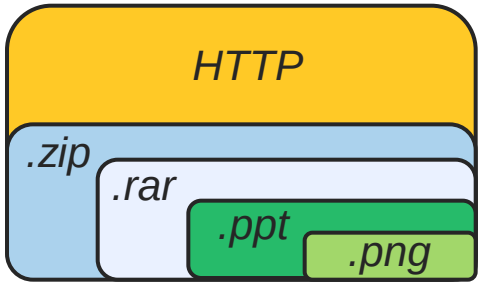


- Защита сервера. Сертификат и закрытый ключ сервера известны. SSL/TLS-инспектор устанавливает туннель, используя сертификат сервера



DLP. Важные аспекты

- Содержимое (контент):
  - Контроль неструктурированных данных: декодирование коммуникационных протоколов и приложений (например, JABBER, веб-чат)
  - Контроль структурированных данных: необходимо распознавать различные структуры и форматы данных (например, DOCX, PPTX, RTF)



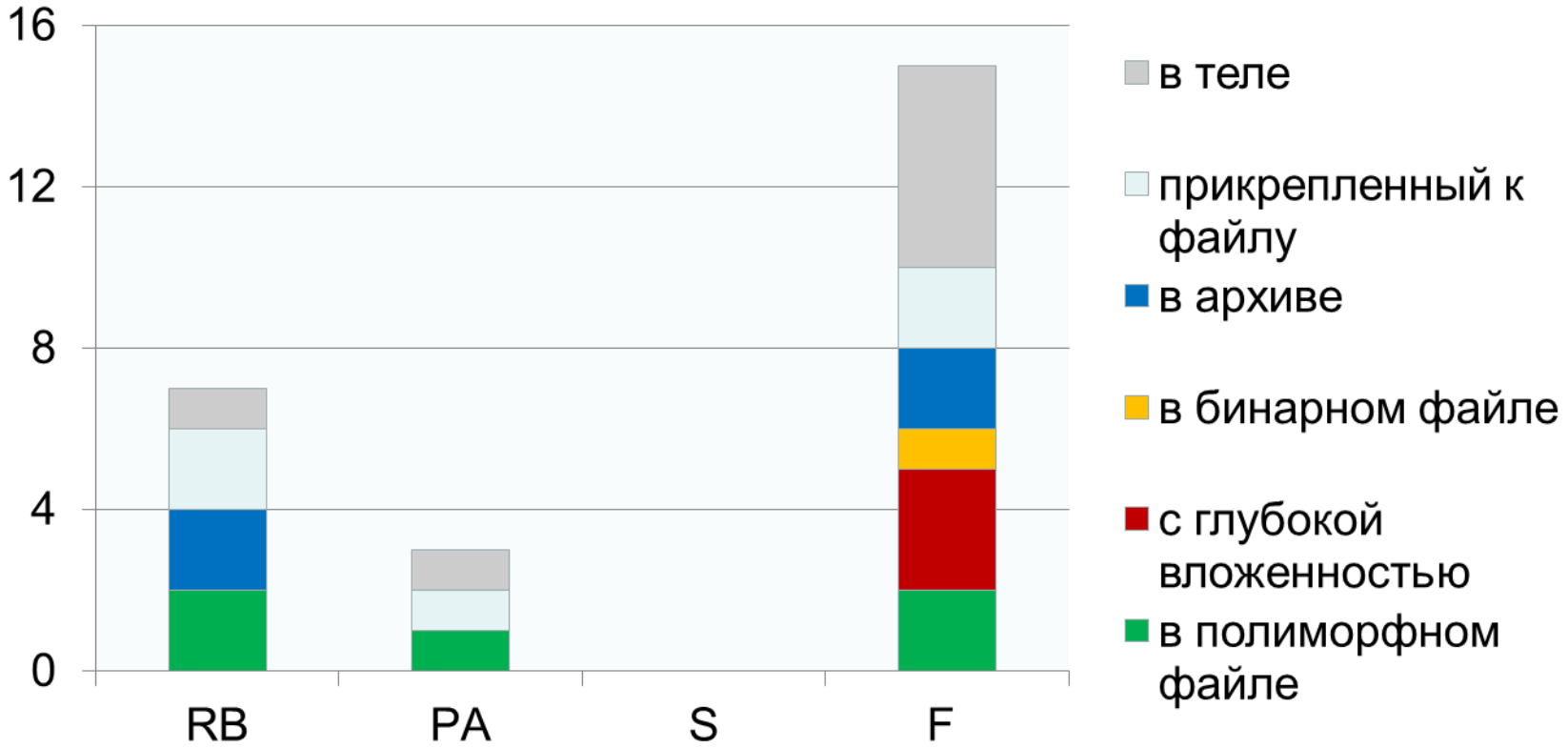
HTTP(upload2.jsp)
multipart[1]
mime(Wireless_LAN_Solution_-_Customer_091103_v_o.zip)
zip(Wireless_LAN_Solution_-_Customer_091103_v_o.rar)
rar(Wireless_LAN_Solution_-_Customer_091103_v_o.pptx)
ms-powerpoint
embedded-image(image26.png)

- Контекст
- Местоположение

Распознавание структурированных данных на практике

Solidex

Анонимные результаты испытаний 4-х СЗИ, от которых требовалось найти заданный текст в файле (всего 15 тестов)



DLP. Важные аспекты (2)

- Содержимое
- Каналы:
  - Контроль передаваемых данных в рамках приложений и протоколов по всем портам и независимо от номера порта
  - Контроль данных, передаваемых в различных сессиях приложения (например, передача файла, инициируемая в рамках сессии обмена короткими сообщениями)
- Местоположение

DLP. Важные аспекты (3)

- Содержимое
- Каналы
- Местоположение:
  - IP-адреса
  - Идентификаторы пользователей
  - Рейтинги узлов Интернет (идентификация drop-серверов)

Содержание

Solidex

- Data Loss Prevention (DLP)
- Advanced Persistent Threat (APT)
- Vulnerability Management (VM)
- Бонус

APT, или современная угроза

Solidex

- **Advanced** Threat: для вторжения могут быть выбраны любые атаки и инструменты, включая специально разработанные, ранее нигде не встречавшиеся
- **Persistent** Threat: целенаправленная, длительная

«А Вы слышали про APT?»

Solidex

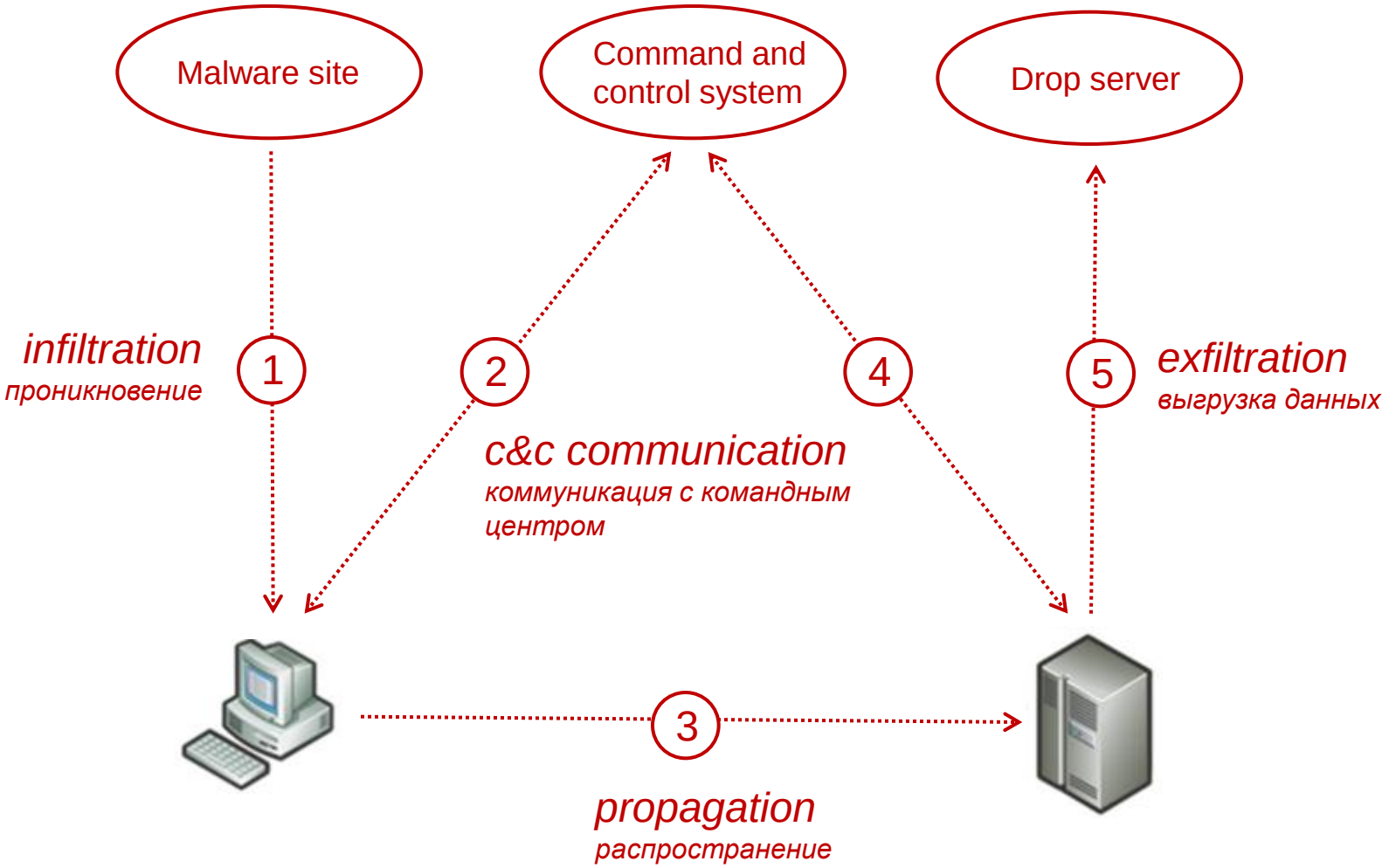
У наших клиентов есть убеждение, что «джентельменский набор» средств защиты информации (Firewall, IPS, AV) является защитой от всех возможных угроз

APT против «джентельменского набора»

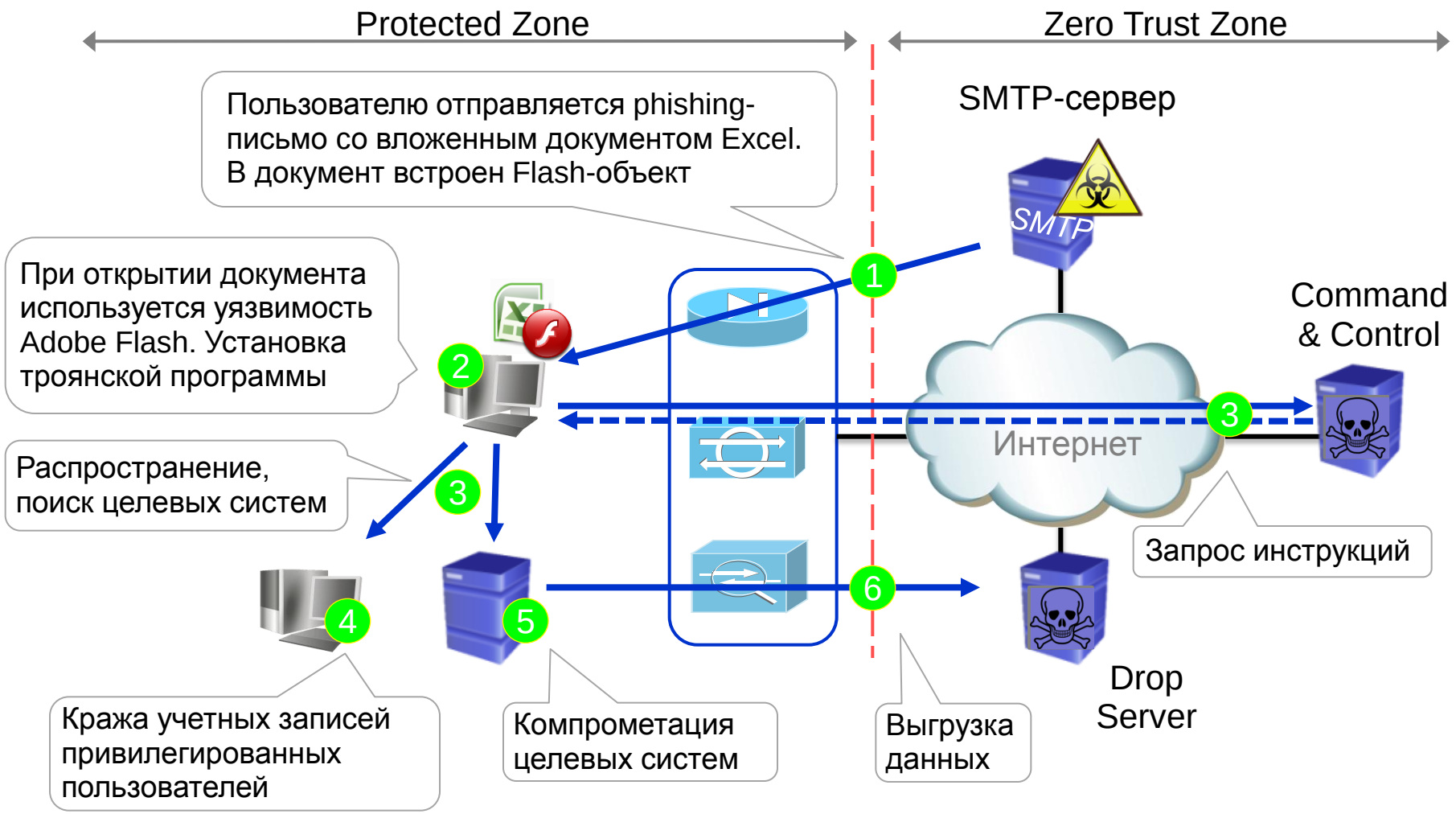
Firewall, IPS, Antivirus оказываются «слепы» в силу используемых против них техник уклонения

СЗИ	**Техника уклонения**
FW	маскировка в разрешенных каналах
IPS	уязвимости «Zero day»
AV	полиморфизм embedded malware вирусы «Zero day»

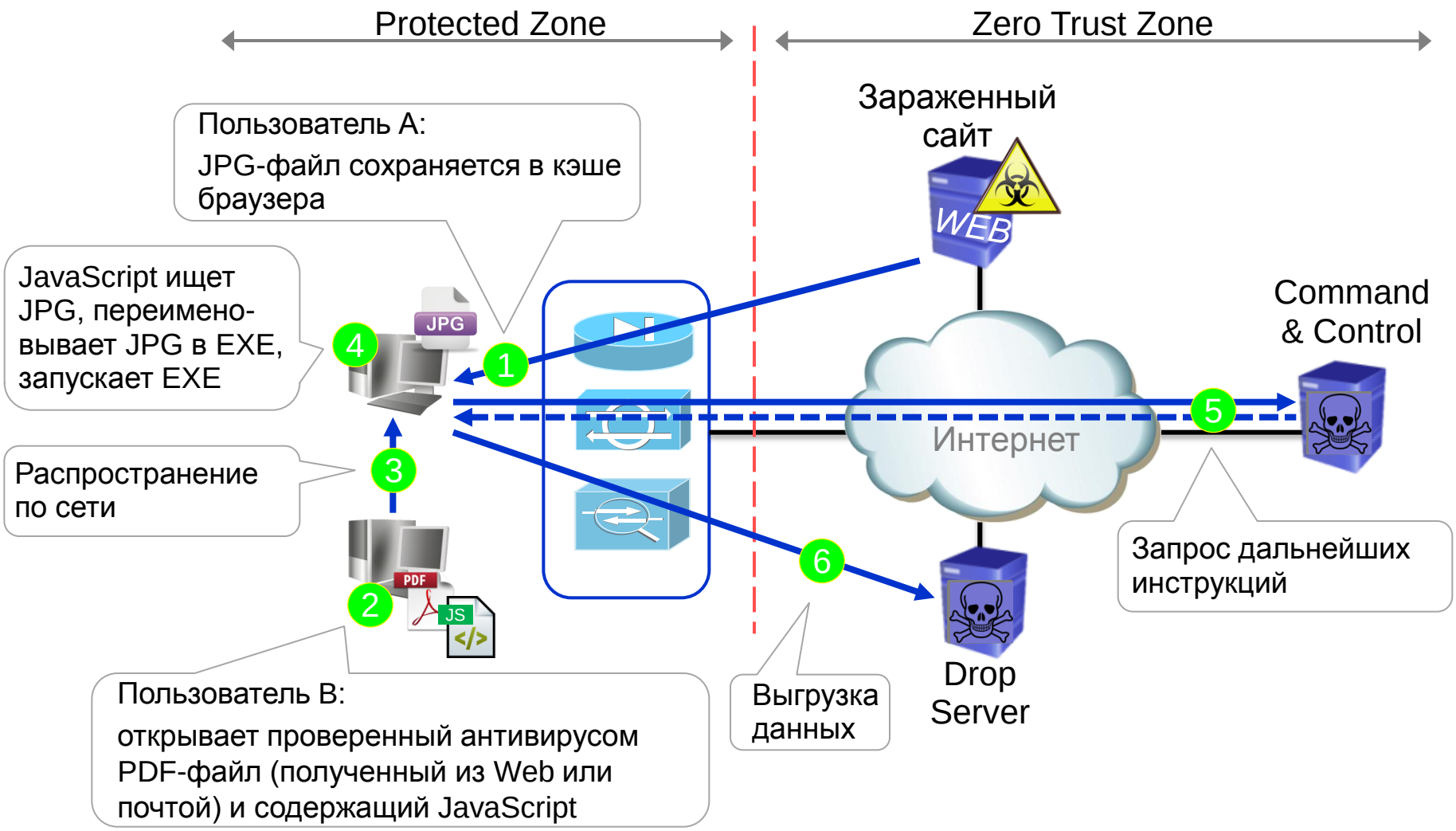
Стадии APT


Malware site
Command and control system
Drop server
infiltration
проникновение
1
2
4
5
exfiltration
выгрузка данных
c&c communication
коммуникация с командным центром
3
propagation
распространение

Пример атаки 1 (атака RSA)



Пример атаки 2



Содержание

- Data Loss Prevention (DLP)
- Advanced Persistent Threat (APT)
- Vulnerability Management (VM)
- Бонус

Задачи VM

- Проактивный метод защиты от угроз
- Сужение поверхности атак
- Направления применения:
  - Сканирование извне (например, публичных веб-ресурсов)
  - Сканирование внутри (например, сетевых устройств, ОС, приложений и сервисов)

Бонус: Penetration Test

- Проверка от лица злоумышленника
- Разведка «вглубь», выявление advanced-уязвимостей
- Хотя модуль «Pentest» может содержаться в и сканере уязвимостей, он реализует простейшие автоматизированные элементы атаки (к примеру, перебор пароля, fuzzing)