31/05/2018

БЕЗОПАСНОСТЬ НА УРОВНЕ СЕТИ: WEB-ИЗОЛЯЦИЯ, АНАЛИЗ ПОТОКОВ

Александр Джаганян

Руководитель направления сетевой безопасности ЦИБ компании «Инфосистемы Джет»
as.djaganyan@jet.su / +7 962 953-12-71

БОЛЕЕ 90% КИБЕРАТАК НАЧИНАЮТСЯ С ВЕБ-САЙТОВ И ЭЛЕКТРОННОЙ ПОЧТЫ*

Web

более
1400
новых уязвимостей обнаружено
браузеров и плагинов за 2017 год

78%
web-сайтов
использовались
для доставки вредоносов

E-mail

83%
рост активности
фишинг-URL

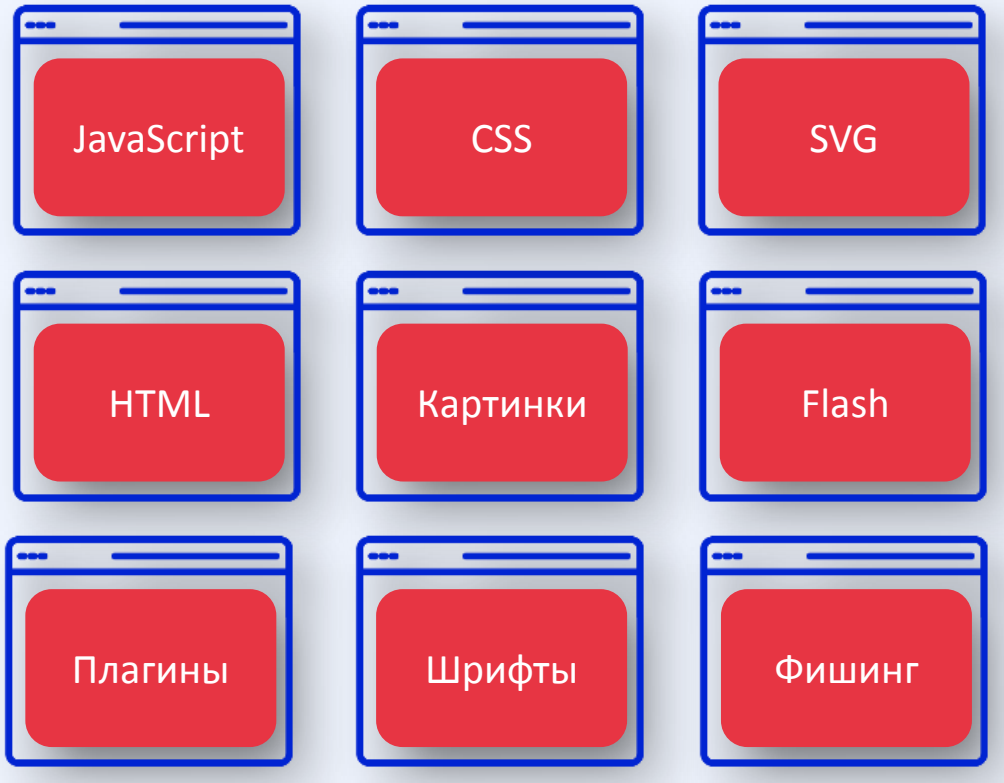
Целенаправленные
фишинг-атаки на предприятия

12%
пользователей
нажимают на неизвестные
ссылки в сообщениях

* По данным Verizon DBIR, Symantec, Gartner, Sophos

БРАУЗЕРЫ – КАК ЦЕЛЬ АТАКИ НА РАБОЧУЮ СТАНЦИЮ

Продвинутое ВПО использует уязвимости браузера, доставляя свой код через веб-страницы

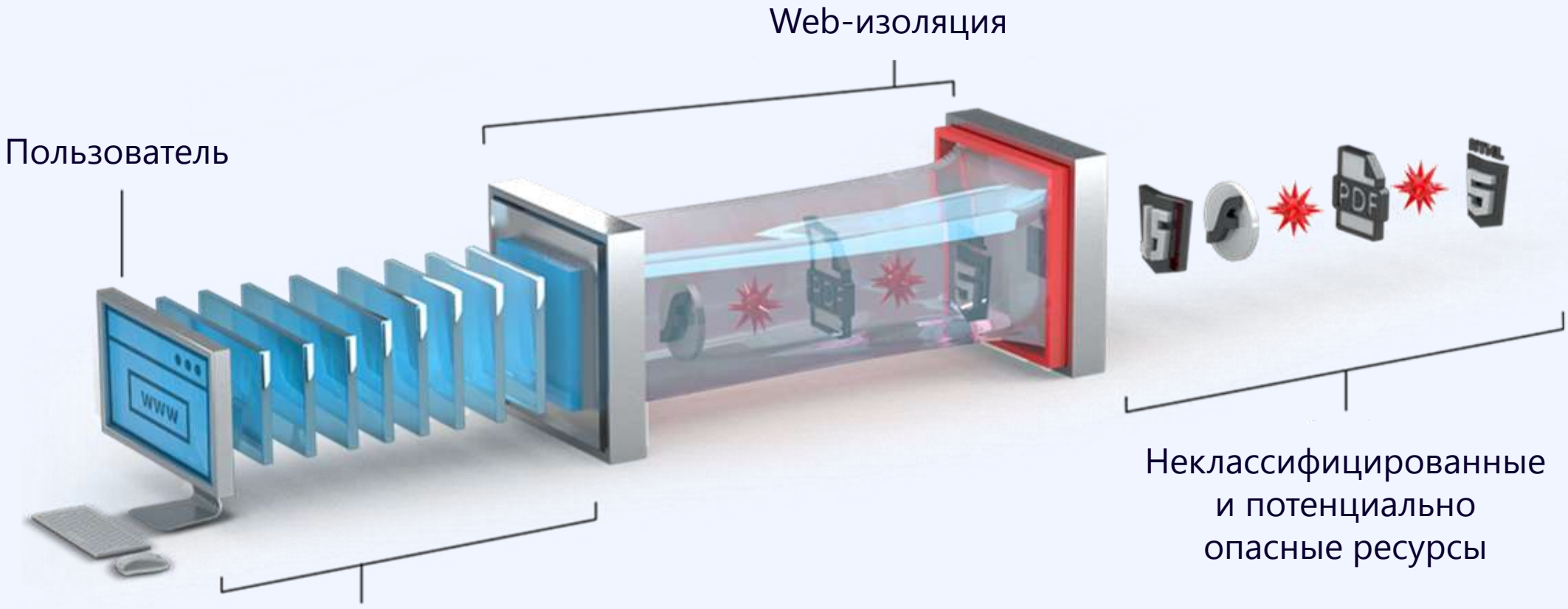


«СЕРАЯ ЗОНА»

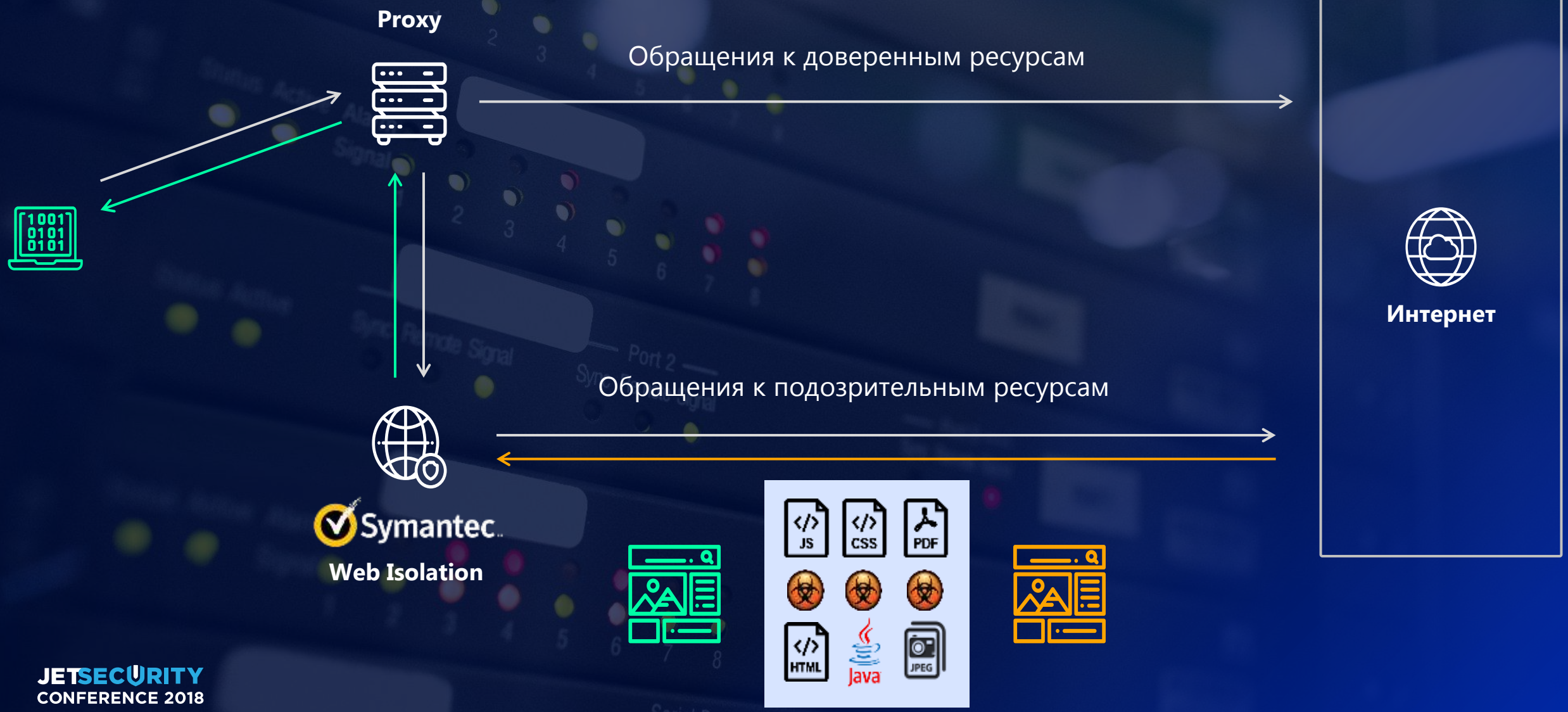
ПРОБЛЕМЫ НЕИЗВЕСТНЫХ WEB-САЙТОВ

- Ежедневное появление миллионов новых доменов и поддоменов
- 71% новых доменов существуют не более 24-х часов
- Многие из них являются легитимными,
  но некоторые являются ресурсами злоумышленников
- Трудно детектировать новые угрозы и полагаться
  на детектирование
- Трудно настроить защиту без чрезмерной блокировки

ЧТО ТАКОЕ WEB ISOLATION?



ИНТЕГРАЦИЯ WEB ISOLATION И PROXYSG / ASG



ОБНАРУЖЕНИЕ АНОМАЛИЙ НА УРОВНЕ СЕТИ

JETSECURITY
CONFERENCE 2018

NETWORK BEHAVIOR ANALYSIS

Сенсор

- Сеть как сенсор безопасности
- Контекстный анализ с историческим аудитом данных NetFlow
- Улучшение планирования, диагностики, оценки соответствия

Видимость

- Наблюдение за распределенной сетью
- Мониторинг сегментации
- Агрегация и анализ телеметрии для установления базового поведенческого уровня в сети

Реакция

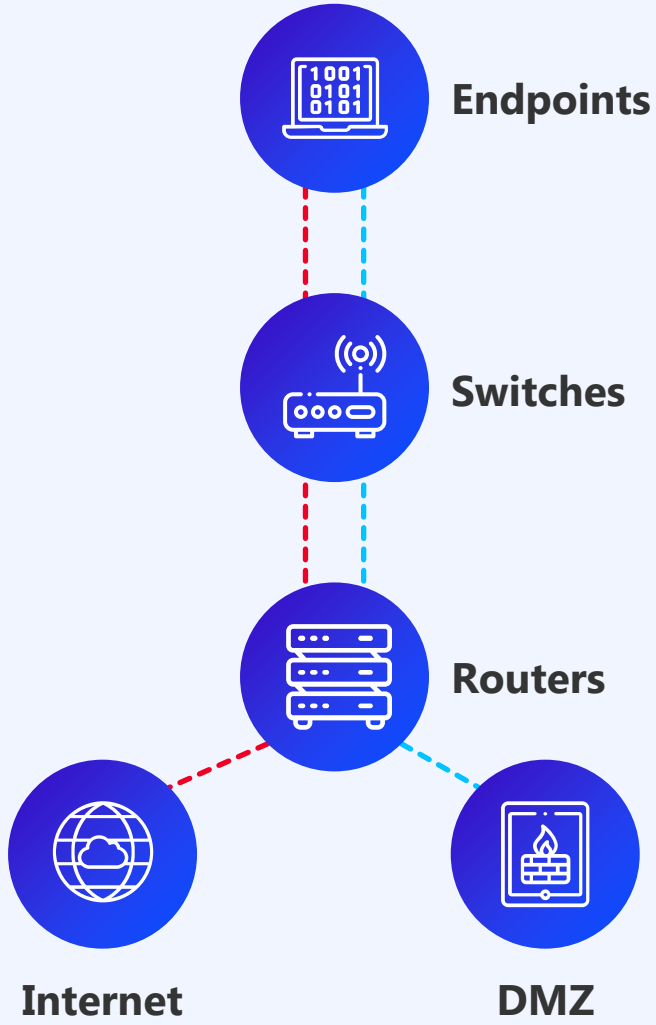
- Обнаружение аномалий, вызванных вредоносными активностями
- Упрощение и ускорение расследований инцидентов
- Интеграция для блокировки вредоносной активности

Flowmon
Driving Network Visibility

CISCO

Flowmon
Driving Network Visibility

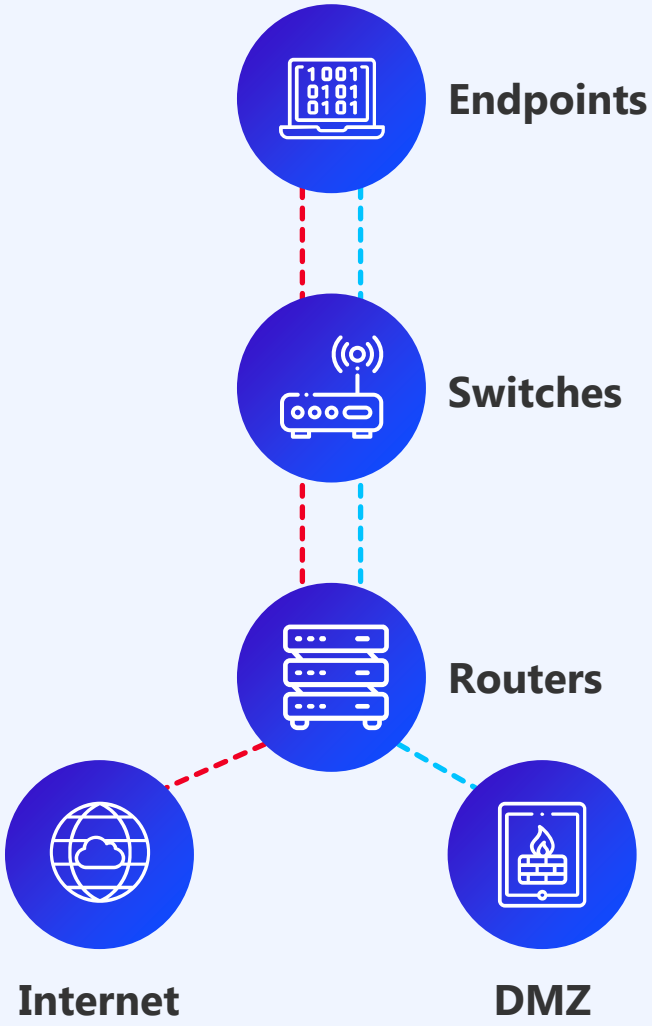
- Обнаруживает и предупреждает о ненормальном сетевом поведении, нехарактерным для этого устройства
- Сообщает об аномальных активностях в сетевом потоке
- Обнаружение вторжений и атак, которые невозможно детектировать стандартными сигнатурными инструментами
- Обнаружение «майнинга» в сети



cisco

Stealthwatch

- Интегрируется с сетью для контроля и блокировки вредоносной активности
- Обогащает контекст за счет интеграции с прокси-сервером и агентов
- Обнаруживает вредоносную активность в зашифрованном трафике



СПАСИБО ЗА ВНИМАНИЕ!

31/05/2018

Александр Джаганян

Руководитель направления сетевой безопасности ЦИБ компании «Инфосистемы Джет»
as.djaganyan@jet.su / +7 962 953-12-71