Positive Technologies

Application Security

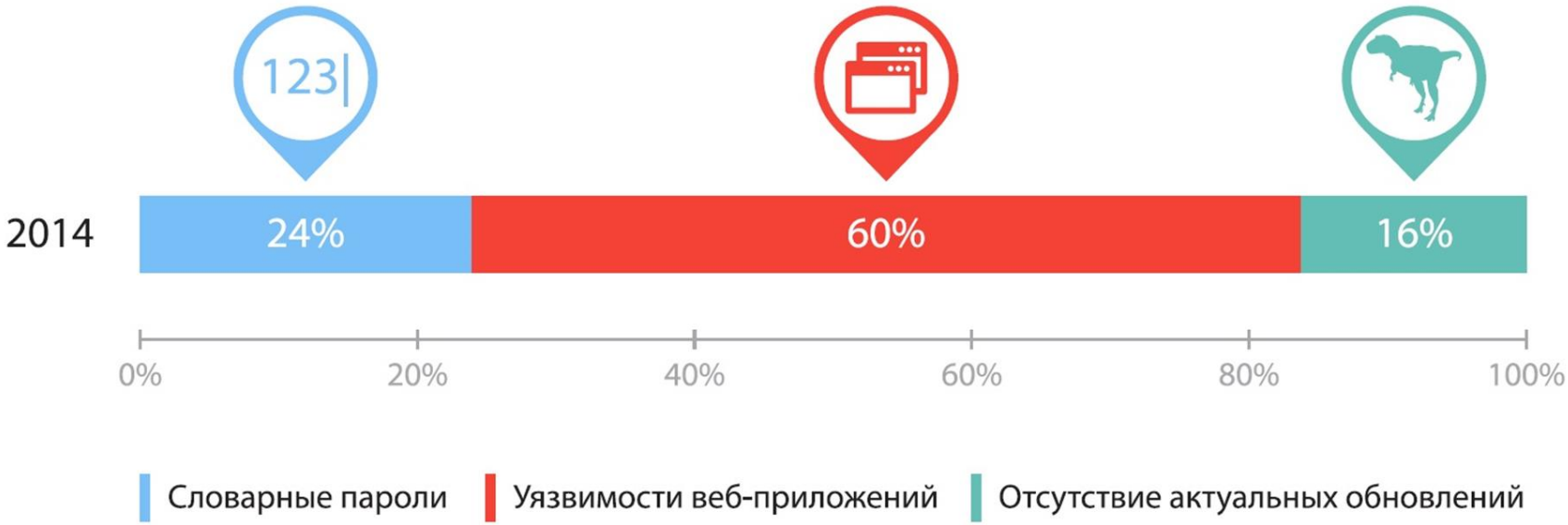
Интеллектуальная защита веб-приложений

Алексей Голдбергс

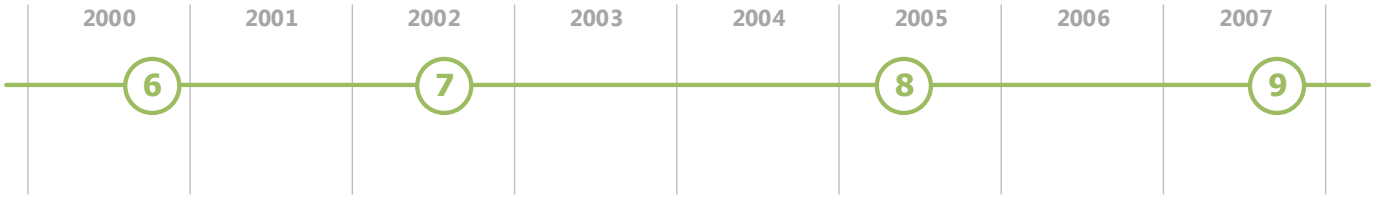
POSITIVE TECHNOLOGIES

SecurITy conference

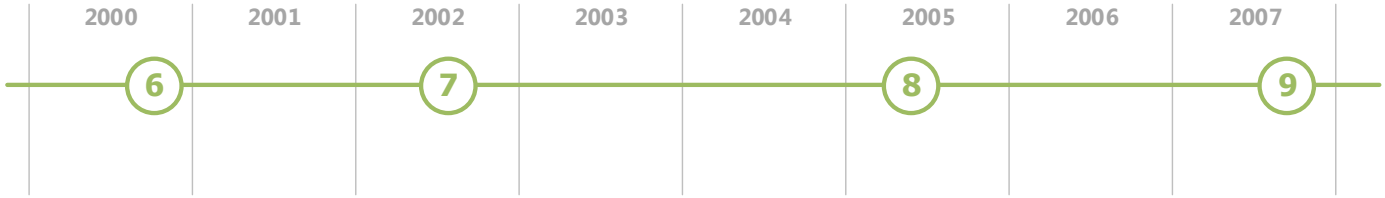
Векторы атак

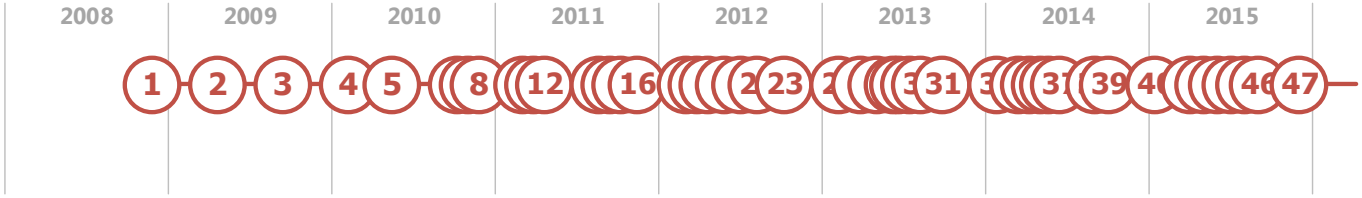


Проблема #1: динамика изменений



Проблема #1: динамика изменений





Проблема #1: это не предел

Amazon May'11 Deployment Stats

(production hosts & environment only)

11.6 seconds

Mean time between deployment

1,079

Max # of deployment in a single hour

10,000

Mean # of hosts simultaneously receiving a deployment

30,000

Max # of hosts simultaneously receiving a deployment

Проблема #2: рост сложности атак

Обычная атака,
2000-ый год:

```
admin’ or 1=1 --
```

Проблема #2: рост сложности атак

Обычная атака,
2000-ый год:

```
admin' or 1=1 --
```

Обычная атака,
2016-ый год:

```
<?xml version='1.0' encoding='UTF-8'?>
<SOAP-ENV:Envelope xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<SOAP-ENV:Header xmlns:ns0="admin" ns0:WASRemoteRuntimeVersion="8.5.5.1"
ns0:JMXMessageVersion="1.2.0" ns0:SecurityEnabled="true"
ns0:JMXVersion="1.2.0">
<LoginMethod>BasicAuth</LoginMethod>
</SOAP-ENV:Header>
<SOAP-ENV:Body>
<ns1:getAttribute xmlns:ns1="urn:AdminService" SOAP-
ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
<objectname
xsi:type="ns1:javax.management.ObjectName">rO0ABXNyADJzdW4ucmVmbGVjdC5hb
m5vdGF0aW9uLkFubm90YXRpb25JbnZvY2F0aW9uSGFuZGxlclXK9Q8Vy36lAgACTAAMbWVtY
mVyVmFsdWVzdAAPTGphdmEvdXRpbC9NYXA7TAAEdHlwZXQAEUxqYXZhL2xhbmcvQ2xhc3M7e
HBzfQAAAAEADWphdmEudXRpbC5NYXB4cgAXamF.....uKgpPeBhzgCAAFJAAV2YWx1ZXhyABB
qYXZhLmxhbmcuTnVtYmVyhqyVHQuU4IsCAAB4cAAAAAFzcgARamF2YS51dGlsLkhhc2hNYXA
FB9rBwxZg0QMAAkYACmxvYWRGYWN0b3JJAAl0aHJlc2hvbGR4cD9AAAAAAAAAdwgAAAAQAAA
AAHh4dnIAEmphdmEubGFuZy5PdmVycmlkZQAAAAAAAAAAAAAAAeHBxAH4AOg==</objectnam
e>
<attribute xsi:type="xsd:string">ringBufferSize</attribute>
</ns1:getAttribute>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Что не так?

Для защиты Web-приложений придумали Web Application Firewall (WAF)

- WAF фильтрует запросы к приложению по заданному набору шаблонов (негативная модель, «черный список»)

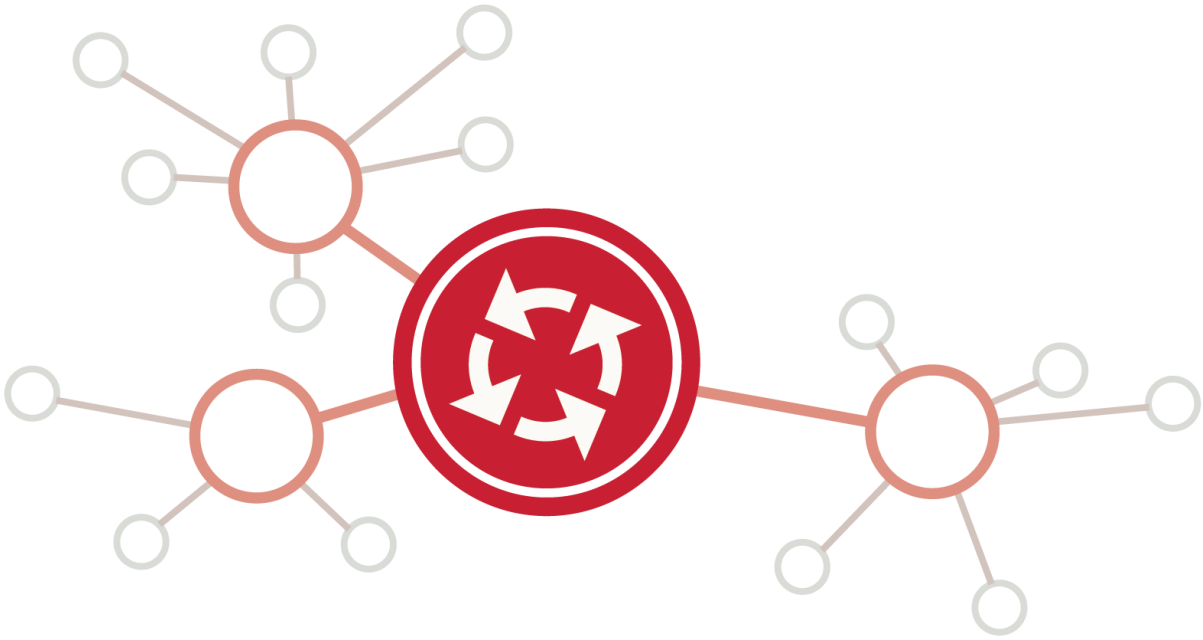
Недостатки подхода:

- Уязвимость к 0-day атакам
  - WAF не может заблокировать атаку, если у него нет ее шаблона
- Занимает много времени
  - Правила должны быть написаны (или настроены) администратором вручную
- Подвержен ошибкам
  - Требует от администратора WAF глубоких знаний об внутреннем устройстве приложения

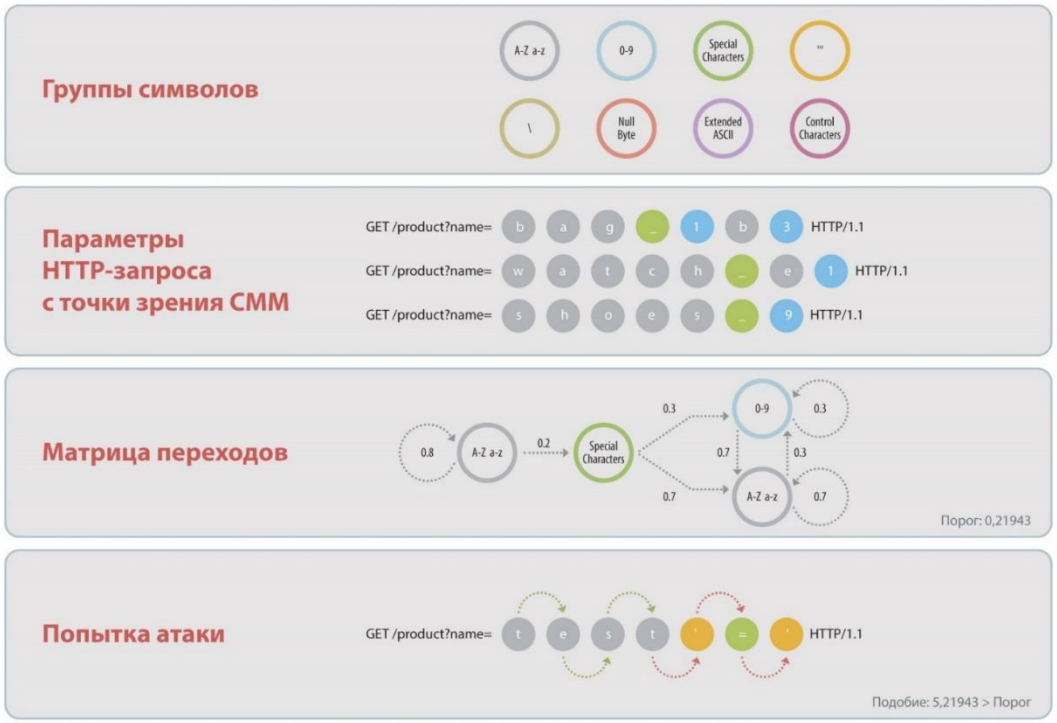
Как жить дальше?

- Позитивная модель безопасности приложения («белый список») как основной метод защиты

- Автоматическое формирование и корректировка модели методами машинного обучения



Скрытые Марковские Модели (CMM)

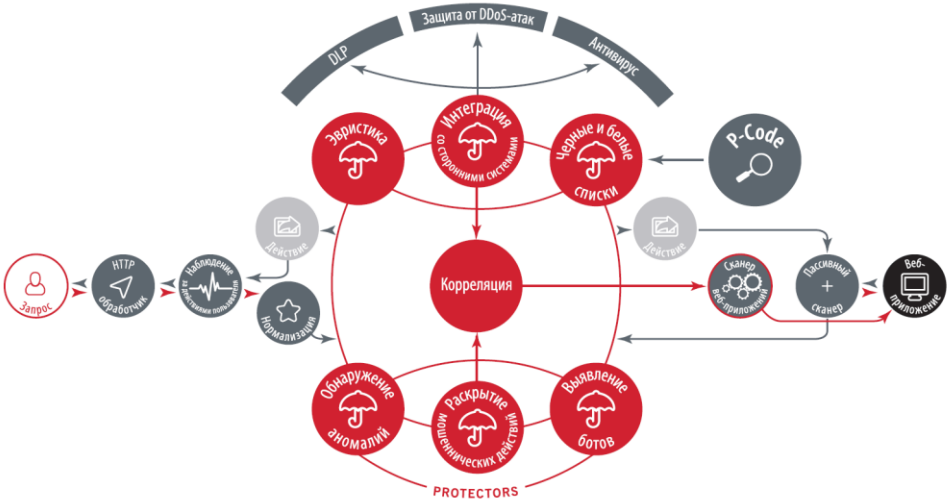


- Группы символов, а не отдельные знаки
- Отдельная модель для каждого атрибута запроса (параметр, заголовок, cookie)
- Итеративное обучение
- Обнаружение и фильтрация выбросов
- Отслеживание ошибок и автоматическое переобучение
- Возможность ручного предварительного обучения

- До 75% 0-day атак

Другие 25%

- Корреляция и приоритизация событий, акцент на основных угрозах
- Самообучаемая модель поведения пользователя для защиты от веб-фрода
- Виртуальные патчи (вместе с PT Application Inspector)
- Анализ содержимого и пассивный сканер безопасности
- Встроенный модуль динамического тестирования безопасности приложений



Спасибо!

POSITIVE TECHNOLOGIES

ptsecurity.com