JET SECURITY CONFERENCE

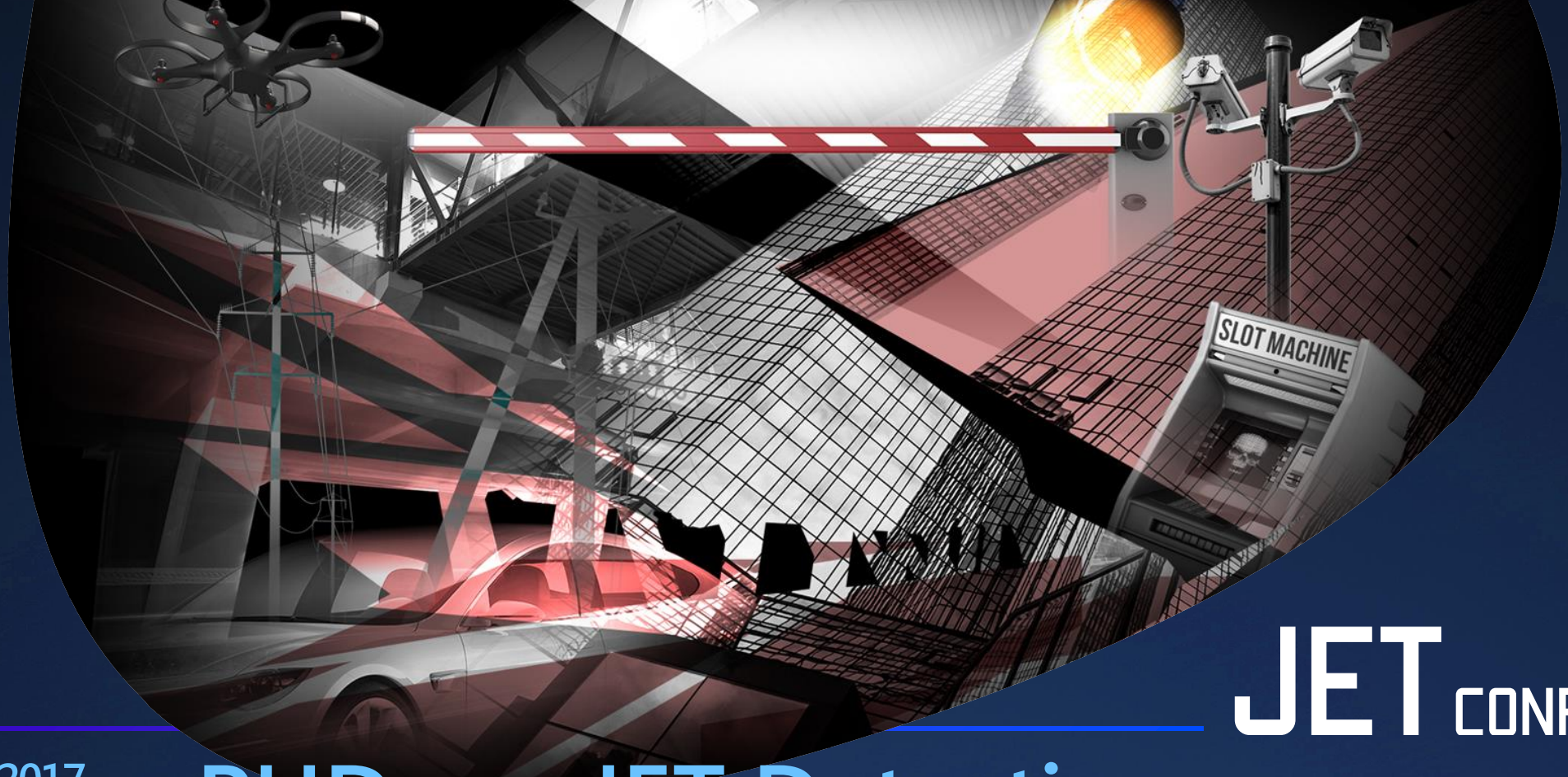
VIII ежегодная конференция
Центра информационной безопасности

1-2 июня 2017 года

WWW.JET.SU

Radisson BLU

Check Point SOFTWARE TECHNOLOGIES LTD
Premier Business Partner IBM
Hewlett Packard Enterprise
f5
IMPERVA
SKYBOX SECURITY
INFOWATCH МЫ РАБОТАЕМ, ЧТОБЫ ЗАЩИЩАТЬ
TREND MICRO
paloalto NETWORKS
FireEye
KASPERSKY PLATINUM PARTNER
POSITIVE TECHNOLOGIES
tufin
FORTINET
SOLAR SECURITY software&services
CYBERARK
TRAPX SECURITY
ONE IDENTITY
RAPID7
iDeals VIRTUAL DATA ROOM



JET CONFERENCE

01/06/2017

PHDays: JET Detective на защите платежной инфраструктуры города

JET

CONFERENCE

Цели и задачи

- Решение сложных задач в сжатые сроки
- Тестирование схемы эксплуатации связок разных линий поддержки
- Проверка идей на потенциальное развитие

JET

CONFERENCE

Общая схема

JET

CONFERENCE

Платежная инфраструктуры

500 счетов

10 счетов

JET

CONFERENCE

Банк и его механизмы

- C2C - PanEntryMode
- E-Banking – login\pass + OTP
- Операции по картам в казино и обратно
- Операции в операторе связи

JET

CONFERENCE

Стратегия защиты

- Собственный скрипт сбора информации о устройствах
- Honeypot для доступа в ДБО и страницу C2C

- Контроль компрометации счетов
- Контроль всей денежной массы

JET

CONFERENCE

Найденные уязвимости

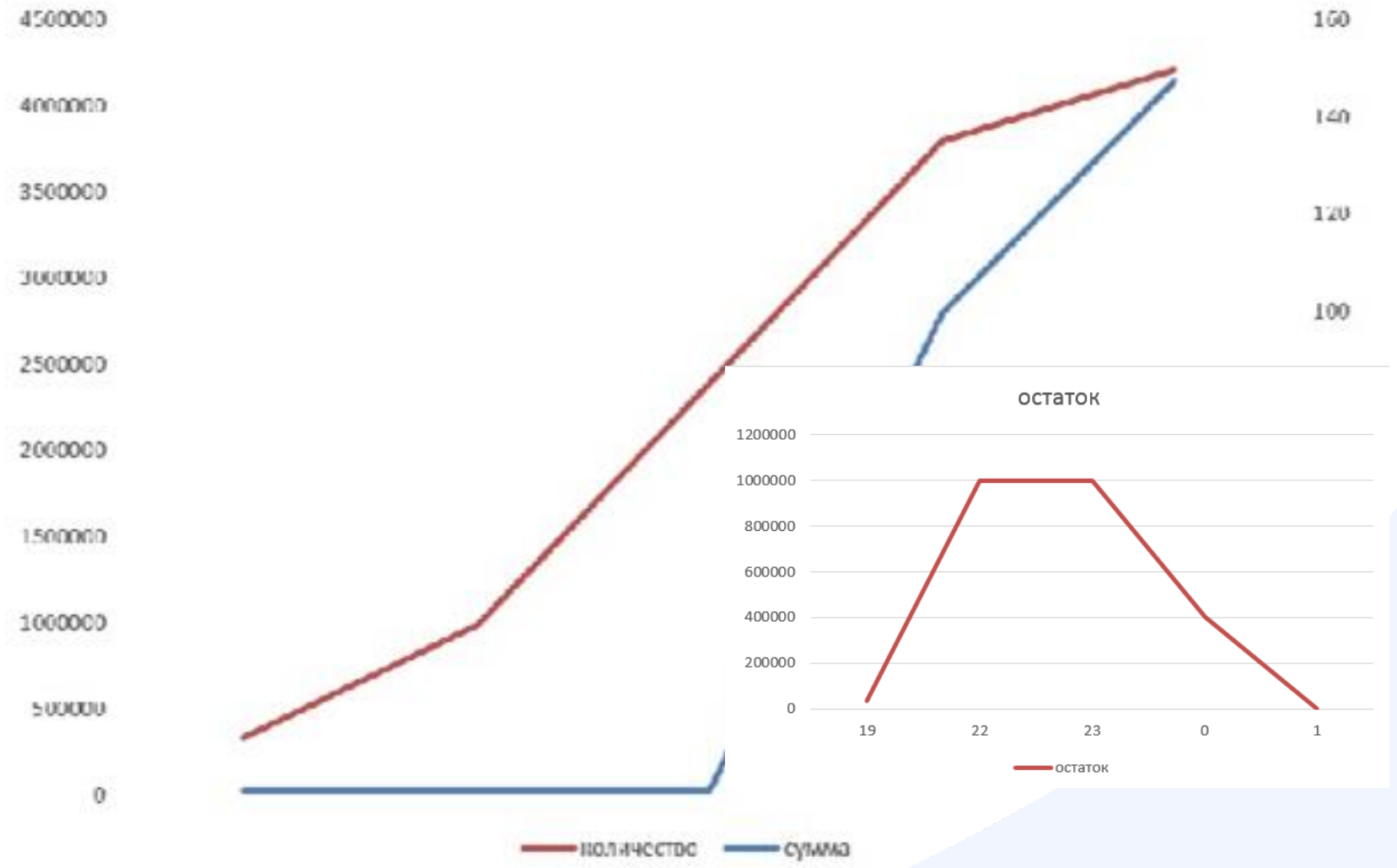
Почти все реквизиты C2C были разбросаны по городу

WEB поддавался sql инъекциям

Login+pass были слабыми + имели алгоритмы генерации серий

JET

CONFERENCE



JET

CONFERENCE

Использованные модели

- Черные списки по устройствам и счетам
- Контроль новых операций по счетам
- Выявление новых fingerprint
- Профили операций
- Частота операций

JET

CONFERENCE

Итог и не найденные уязвимости

В активном режиме атакующие смогли провести 2 операции на 1 рублю, при совокупных попытках более чем в 2000 операций на сумму более 500К.

Остались не использованы сервисы казино и пополнение счета телеком оператора.

JET

CONFERENCE

JET CONFERENCE

00/00/2017

ИНФОСИСТЕМЫ ДЖЕТ

Спасибо за внимание!