Выявление атак на пользователей систем ДБО

IX Уральский форум «Информационная безопасность финансовой сферы»

Денис Горчаков,

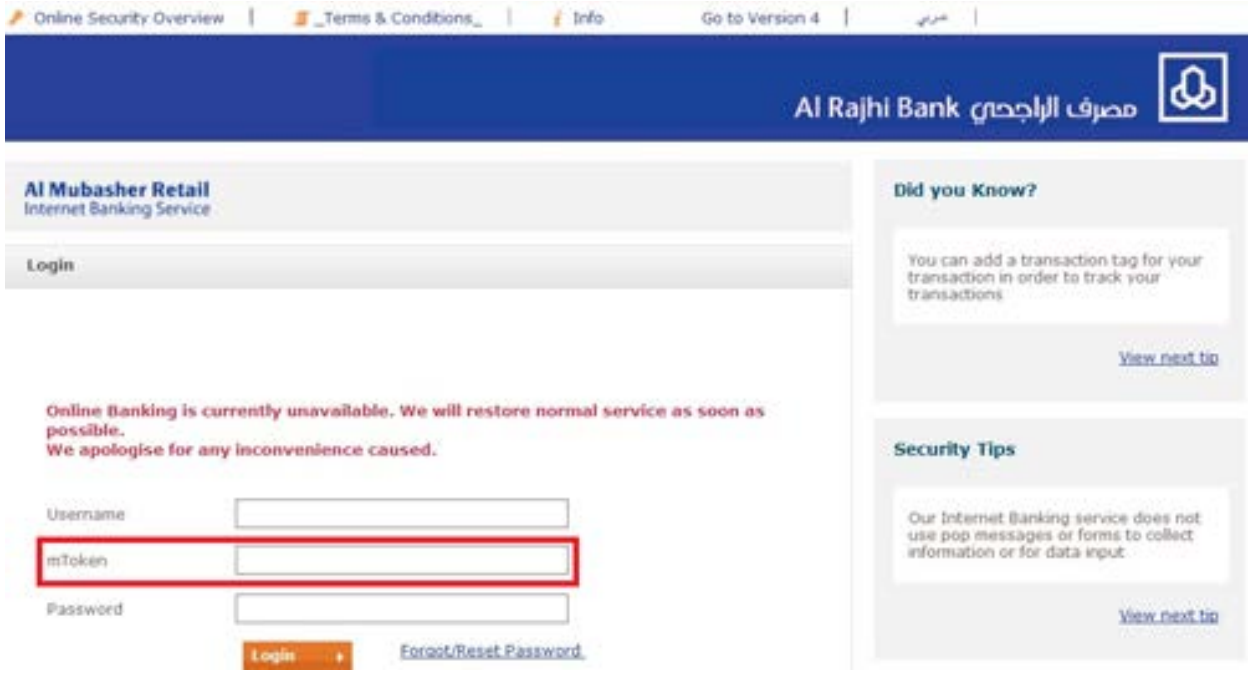
Руководитель группы исследования и анализа мошенничества

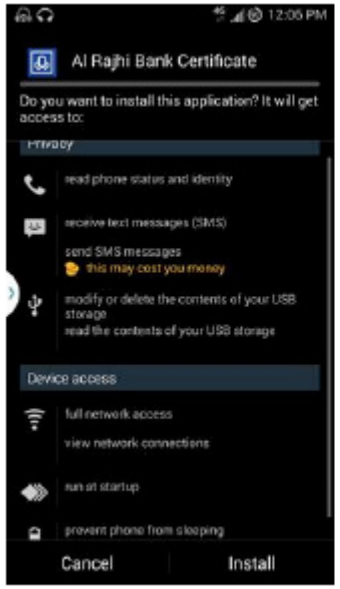
Kaspersky Fraud Prevention

О СЕБЕ

- **Описываем** разработчикам тактики и инструменты мошенников
- **Расследуем** инциденты
- **Исследуем** перспективные угрозы и платёжные технологии

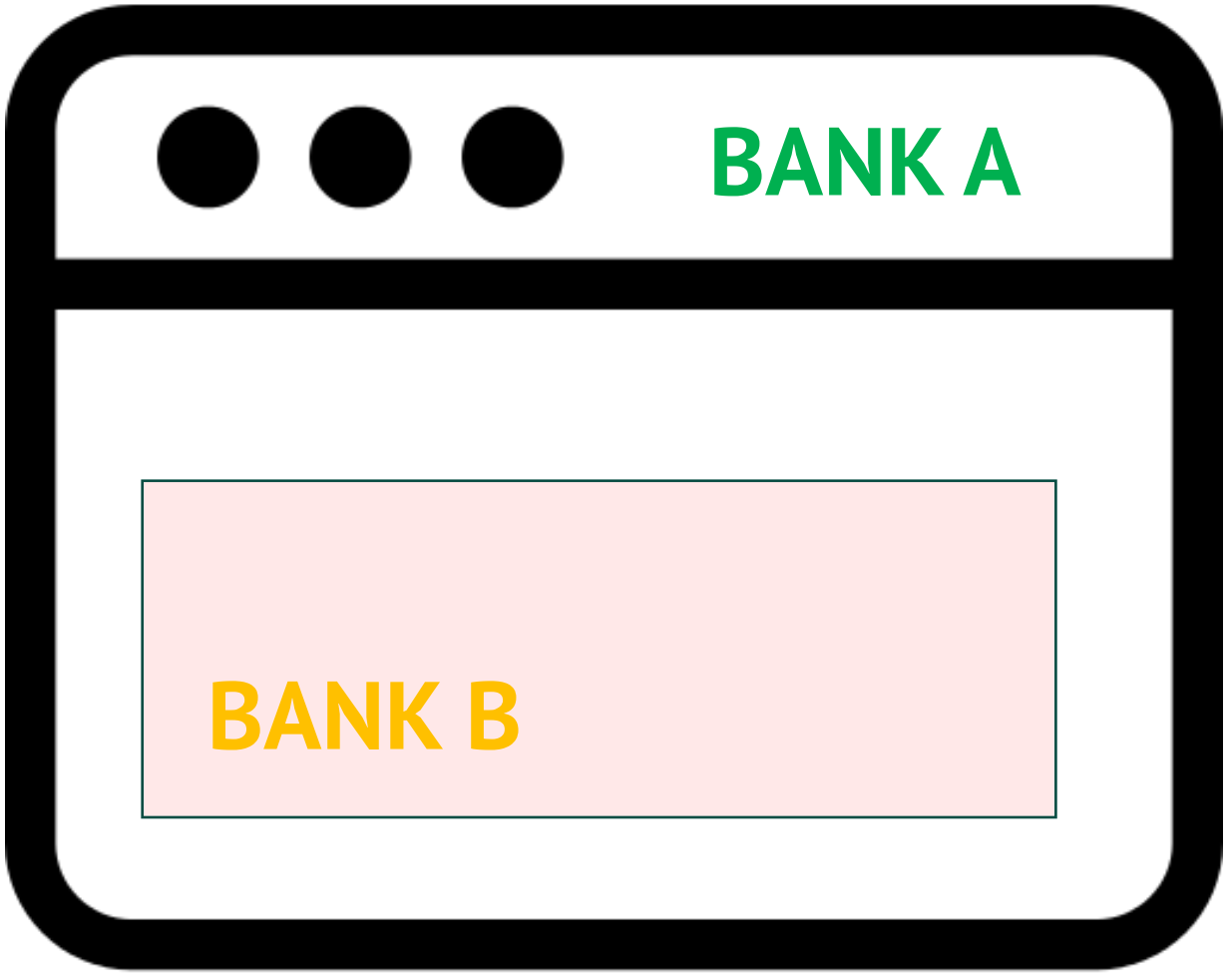
ZEUS, ZITMO … СВЕЖИЙ СЛУЧАЙ С БЛИЖНЕГО ВОСТОКА



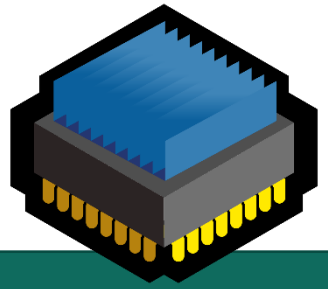


http://www.alrajhibank.com.sa/en/privacy-and-security/pages/fraud-awareness.aspx

ТЕХНОЛОГИЯ БЭЙТИНГА (ЛОВУШКА)



НЕ ТОТ, ЗА КОГО СЕБЯ ВЫДАЁТ



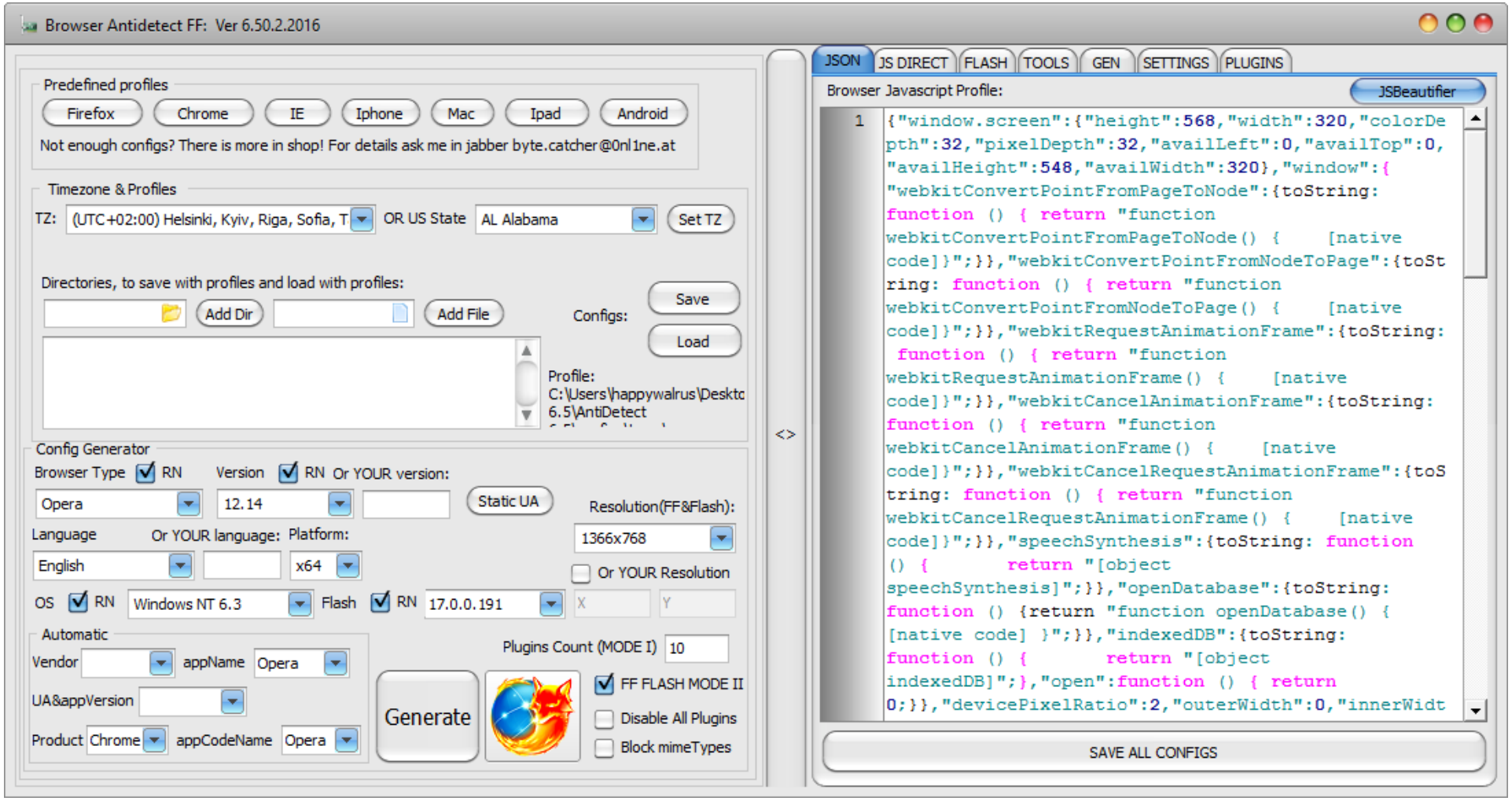
?

NONE

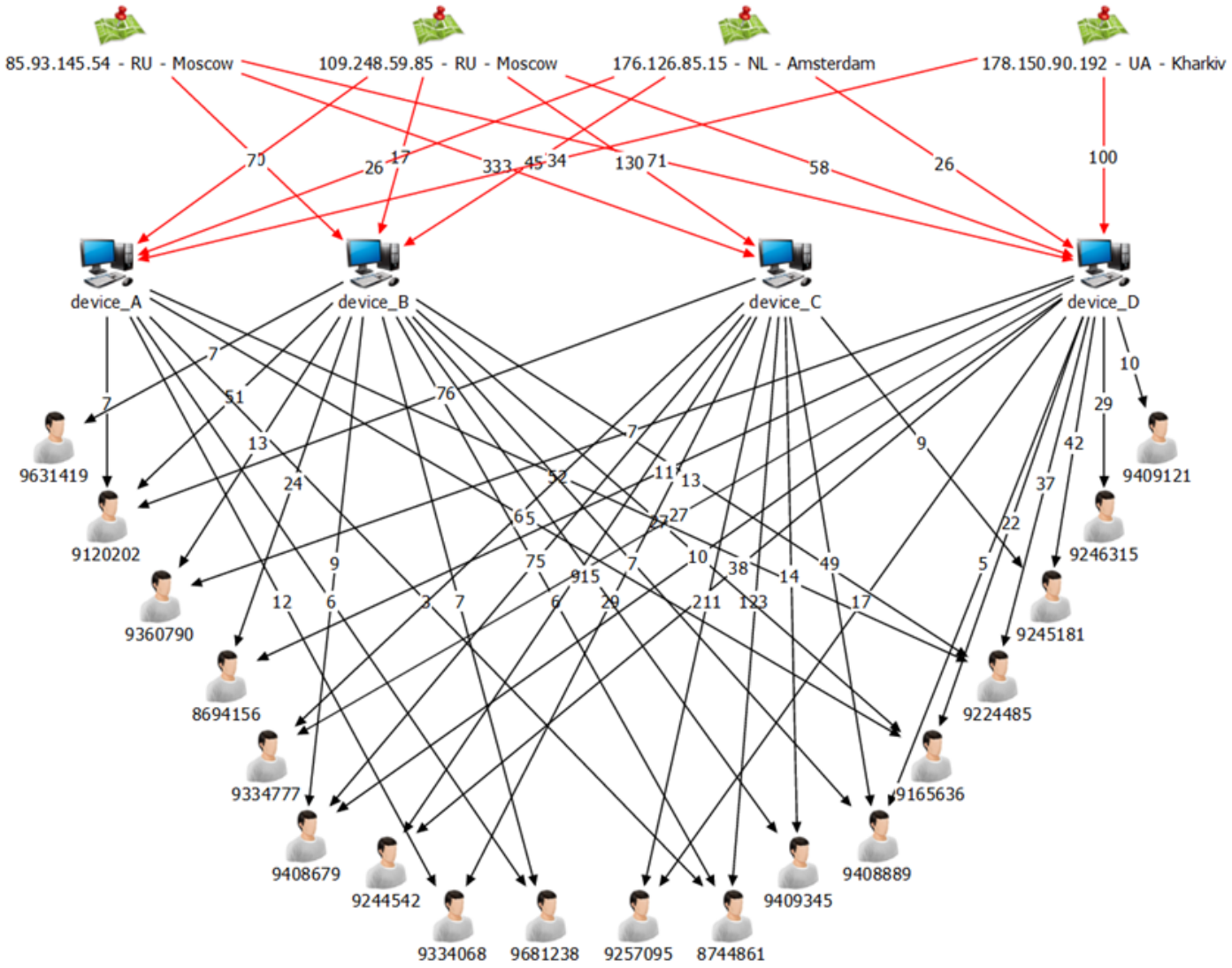
8

МАСКА, КТО ТЫ?

- BROWSER
- canvas
- configs
- New
- prx
- REGISTER
- .DS_Store
- antidetect6.5
- conf.bin
- config
- dirs_to_save
- notes
- result.json
- skinconfig
- timezone

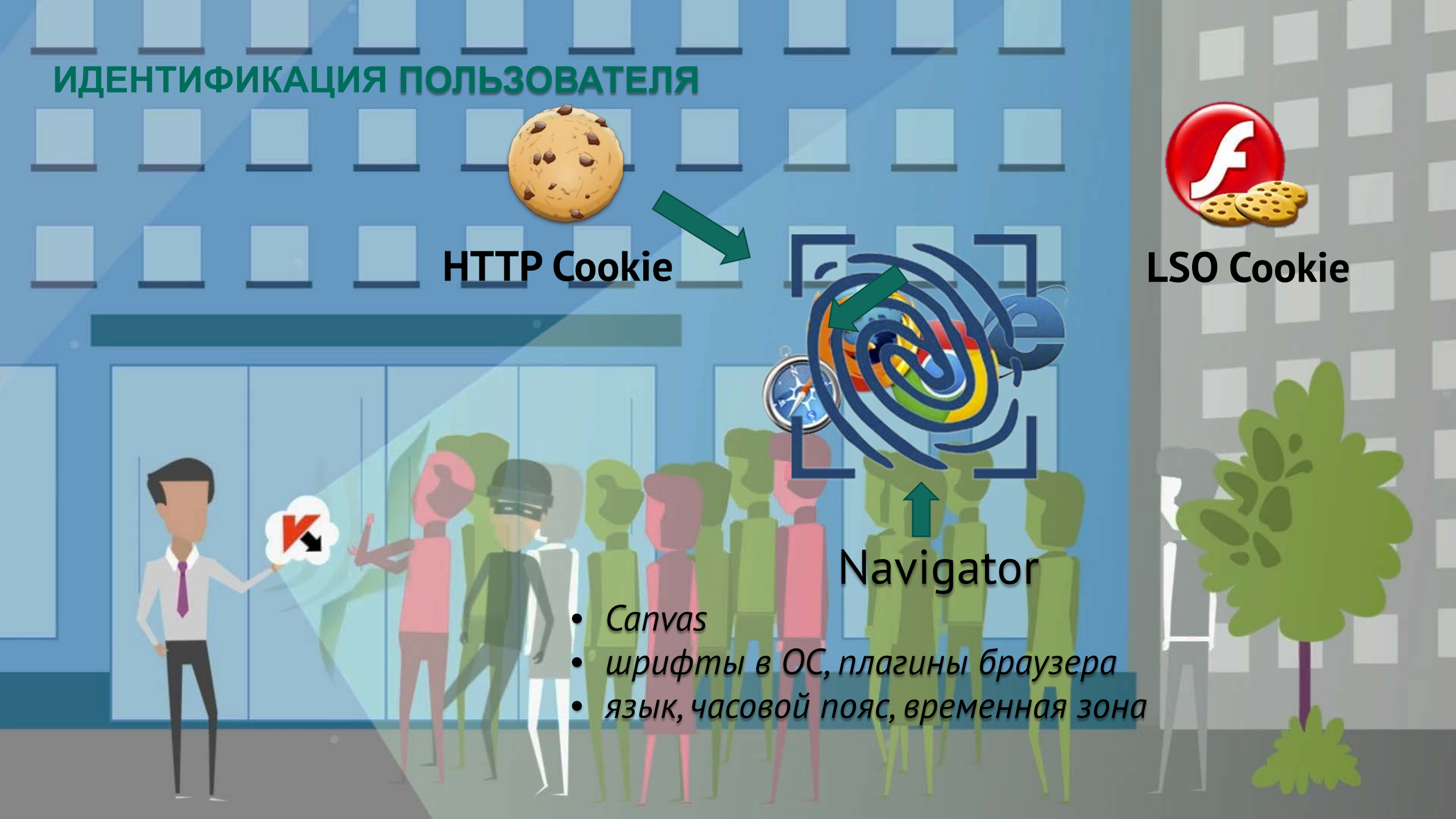


СВЯЗИ



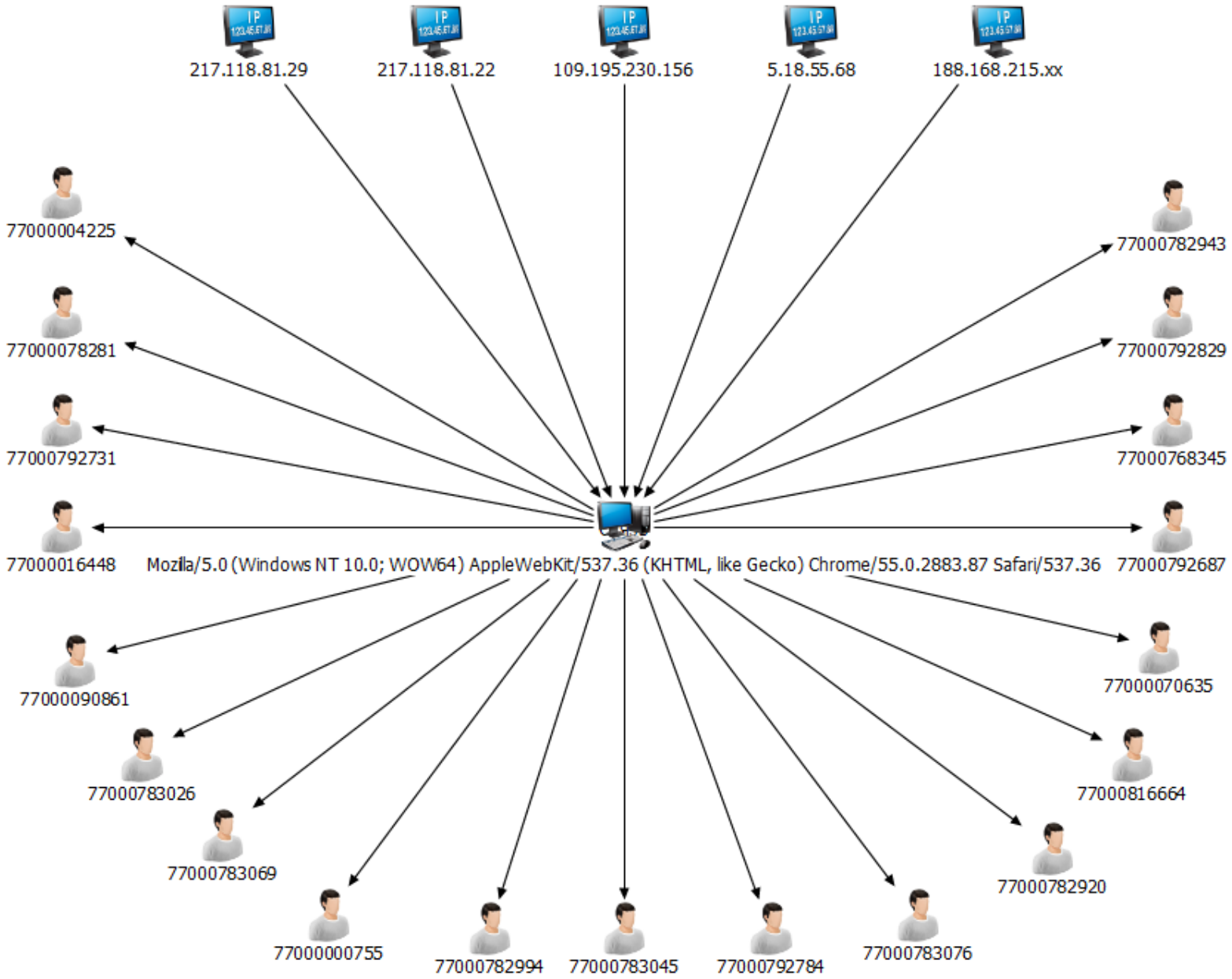
$$T_A = \frac{T_B}{\sqrt{1 - \frac{v^2}{c^2}}}$$

ИДЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЯ



ПРОГРАММЫ ЛОЯЛЬНОСТИ

ПРИМЕР


217.118.81.29
217.118.81.22
109.195.230.156
5.18.55.68
188.168.215.xx
77000004225
77000078281
77000792731
77000016448
77000782943
77000792829
77000768345
77000792687
Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2883.87 Safari/537.36
77000090861
77000783026
77000783069
77000000755
77000782994
77000783045
77000792784
77000783076
77000070635
77000816664
77000782920

ВОПРОСЫ?

Denis.Gorchakov@kaspersky.com

KASPERSKY lab

KASPERSKY lab