

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

Online Security Overview | Terms & Conditions | Info | Go to Version 4 | عربي

Al Rajhi Bank مصرف الراجحي

Al Mubasher Retail
Internet Banking Service

Login

Online Banking is currently unavailable. We will restore normal service as soon as possible.
We apologise for any inconvenience caused.

Username

mToken

Password

Login [Forgot/Reset Password](#)

Did you Know?

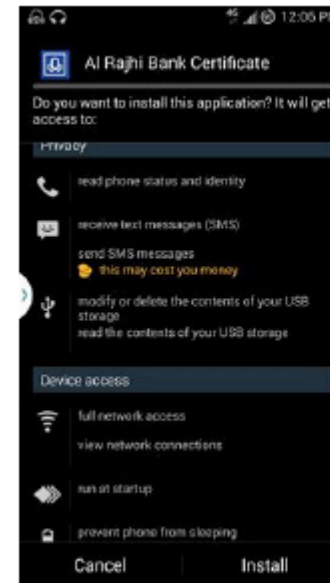
You can add a transaction tag for your transaction in order to track your transactions

[View next tip](#)

Security Tips

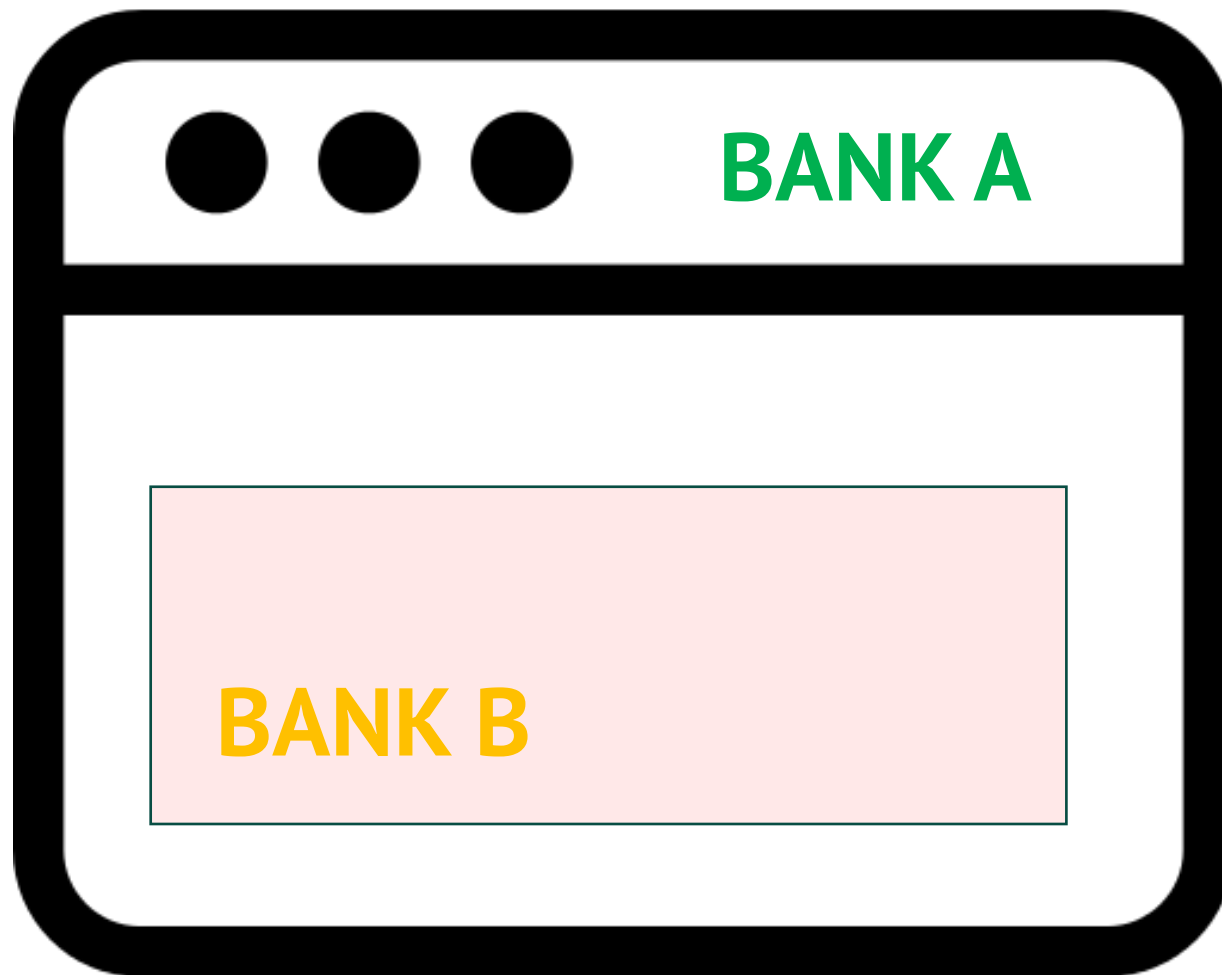
Our Internet Banking service does not use pop messages or forms to collect information or for data input

[View next tip](#)

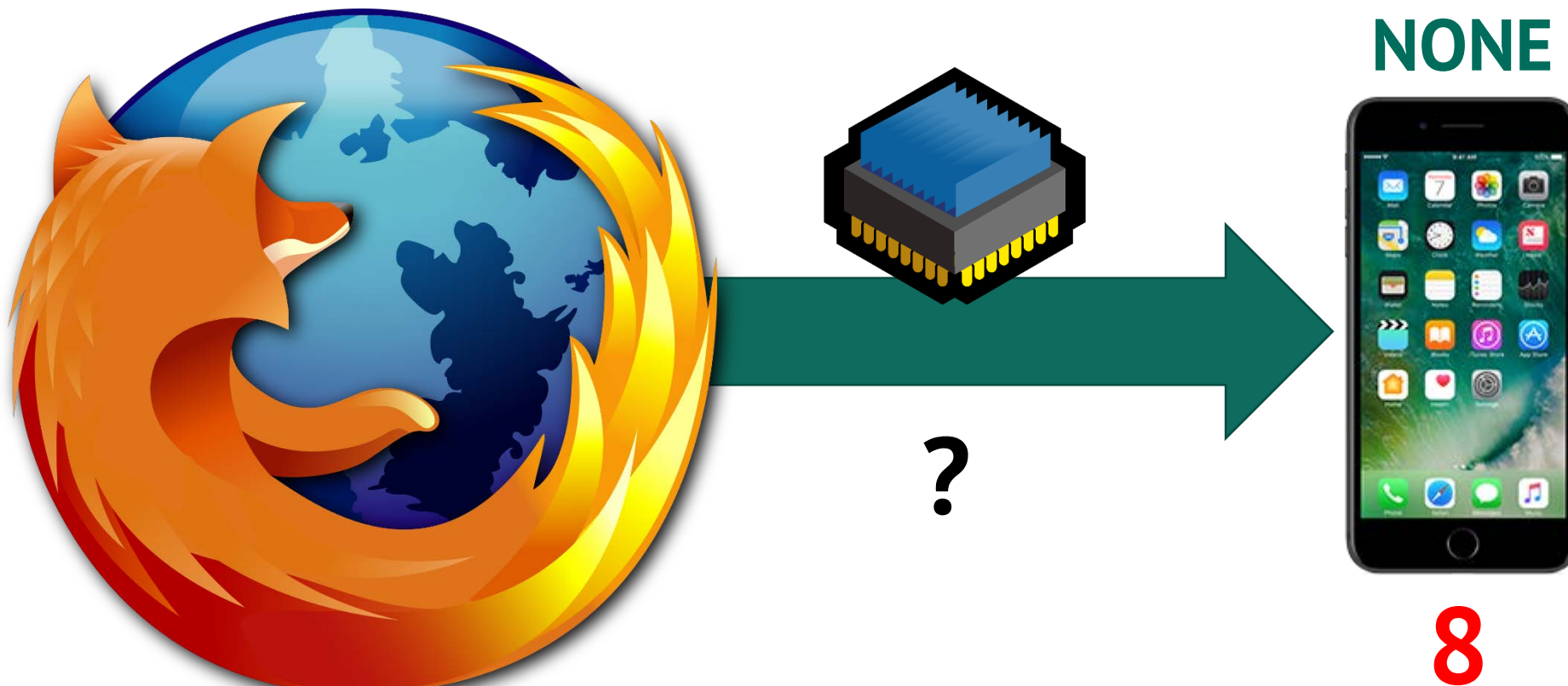


<http://www.alrajhibank.com.sa/en/privacy-and-security/pages/fraud-awareness.aspx>

ТЕХНОЛОГИЯ БЭЙТИНГА (ЛОВУШКА)



НЕ ТОТ, ЗА КОГО СЕБЯ ВЫДАЁТ



МАСКА, КТО ТЫ?

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

Browser Antidetect FF: Ver 6.50.2.2016


Predefined profiles: Firefox, Chrome, IE, Iphone, Mac, Ipad, Android

Not enough configs? There is more in shop! For details ask me in jabber byte.catcher@0nl1ne.at

Timezone & Profiles
TZ: (UTC+02:00) Helsinki, Kyiv, Riga, Sofia, T OR US State AL Alabama Set TZ

Directories, to save with profiles and load with profiles:
Add Dir Add File Save Load

Profile: C:\Users\happywalrus\Desktop\6.5\AntiDetect

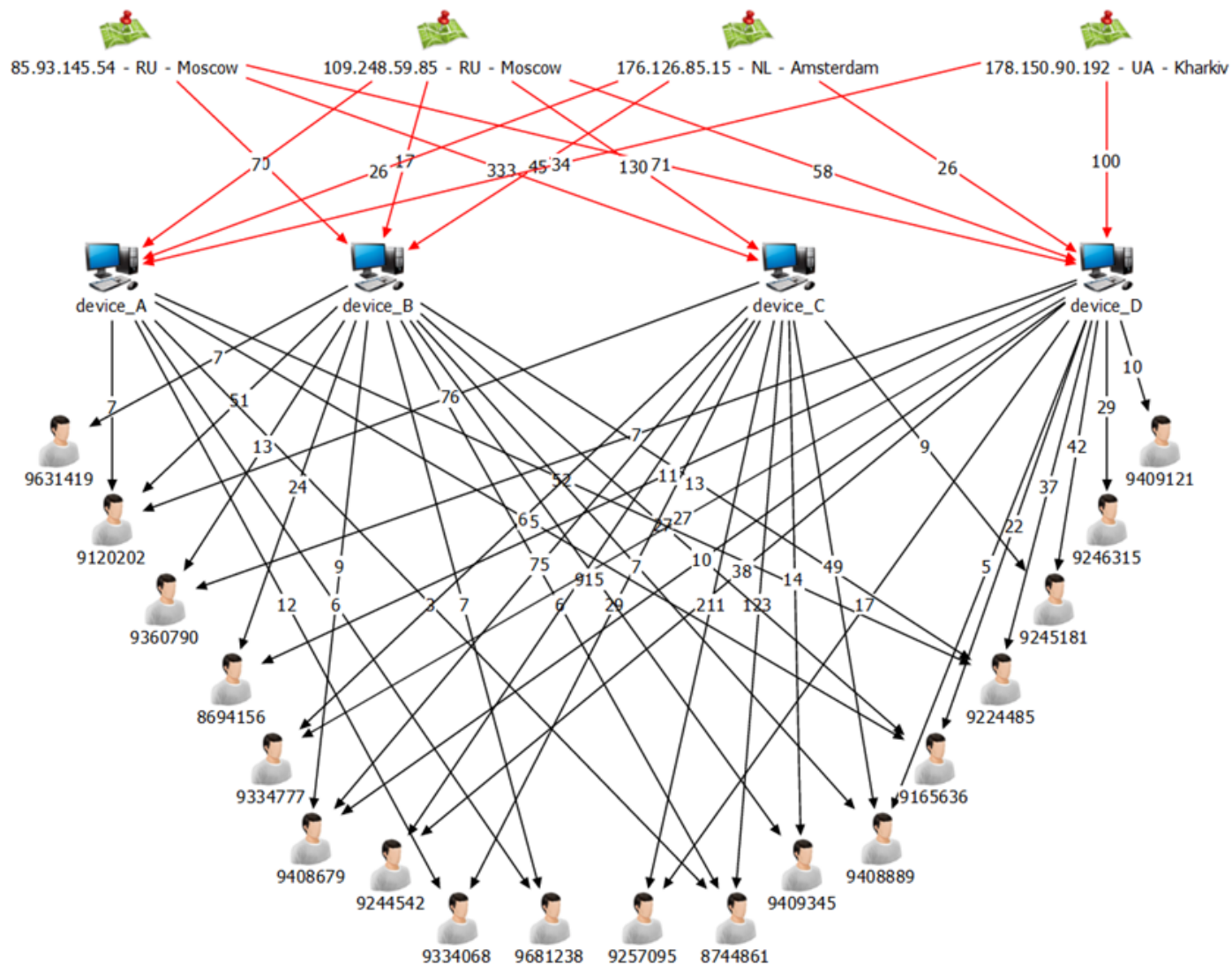
Config Generator
Browser Type RN Version RN Or YOUR version:
Opera 12.14 Static UA Resolution(FF&Flash): 1366x768
Language Or YOUR language: Platform: English x64 Or YOUR Resolution
OS RN Windows NT 6.3 Flash RN 17.0.0.191 X Y
Automatic
Vendor appName Opera
UA&appVersion
Product Chrome appCodeName Opera
Generate  FF FLASH MODE II
 Disable All Plugins
 Block mimeTypees

Browser Javascript Profile: JSBeautifier

```
1 {"window.screen":{"height":568,"width":320,"colorDepth":32,"pixelDepth":32,"availLeft":0,"availTop":0,"availHeight":548,"availWidth":320},"window":{"webkitConvertPointFromPageToNode":{"toString":function () { return "function webkitConvertPointFromPageToNode() { [native code]}";},"webkitConvertPointFromNodeToPage":{"toString":function () { return "function webkitConvertPointFromNodeToPage() { [native code]}";},"webkitRequestAnimationFrame":{"toString":function () { return "function webkitRequestAnimationFrame() { [native code]}";},"webkitCancelAnimationFrame":{"toString":function () { return "function webkitCancelAnimationFrame() { [native code]}";},"webkitCancelRequestAnimationFrame":{"toString":function () { return "function webkitCancelRequestAnimationFrame() { [native code]}";},"speechSynthesis":{"toString":function () {return "function openDatabase() { [native code] }";},"indexedDB":{"toString":function () { return "[object indexedDB]";},"open":function () { return 0;},"devicePixelRatio":2,"outerWidth":0,"innerWidth":0}}
```

SAVE ALL CONFIGS

СВЯЗИ



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

ИДЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЯ



HTTP Cookie

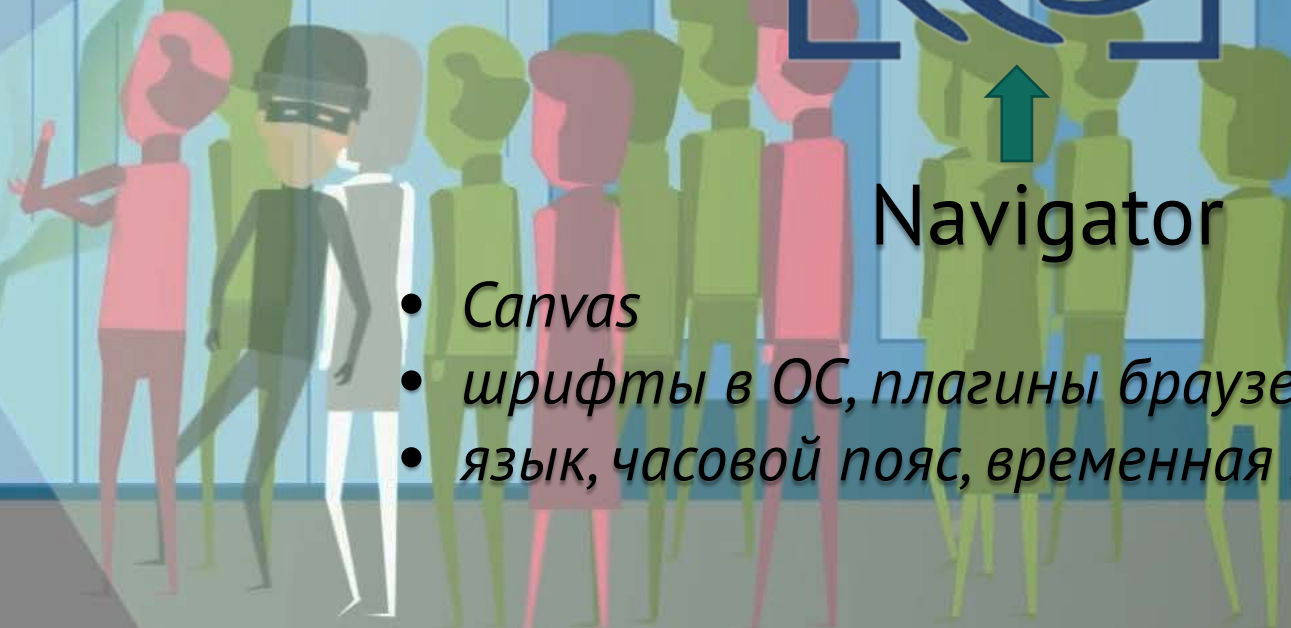


Navigator

- *Canvas*
- *шрифты в ОС, плагины браузера*
- *язык, часовой пояс, временная зона*



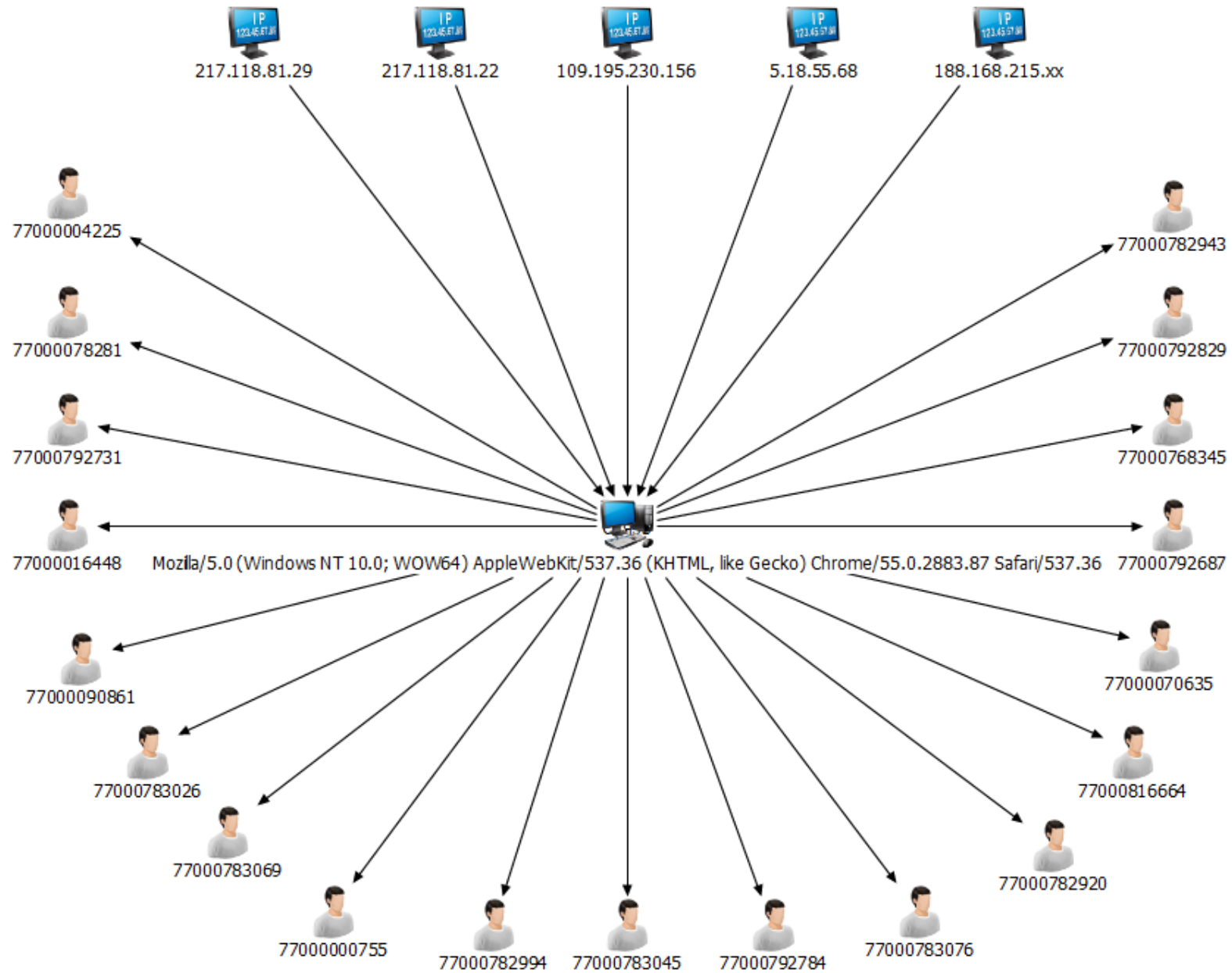
LSO Cookie



ПРОГРАММЫ ЛОЯЛЬНОСТИ



ПРИМЕР





ВОПРОСЫ?

Denis.Gorchakov@kaspersky.com

KASPERSKY 

KASPERSKY 