e-Crime Intelligence in Financial Sector

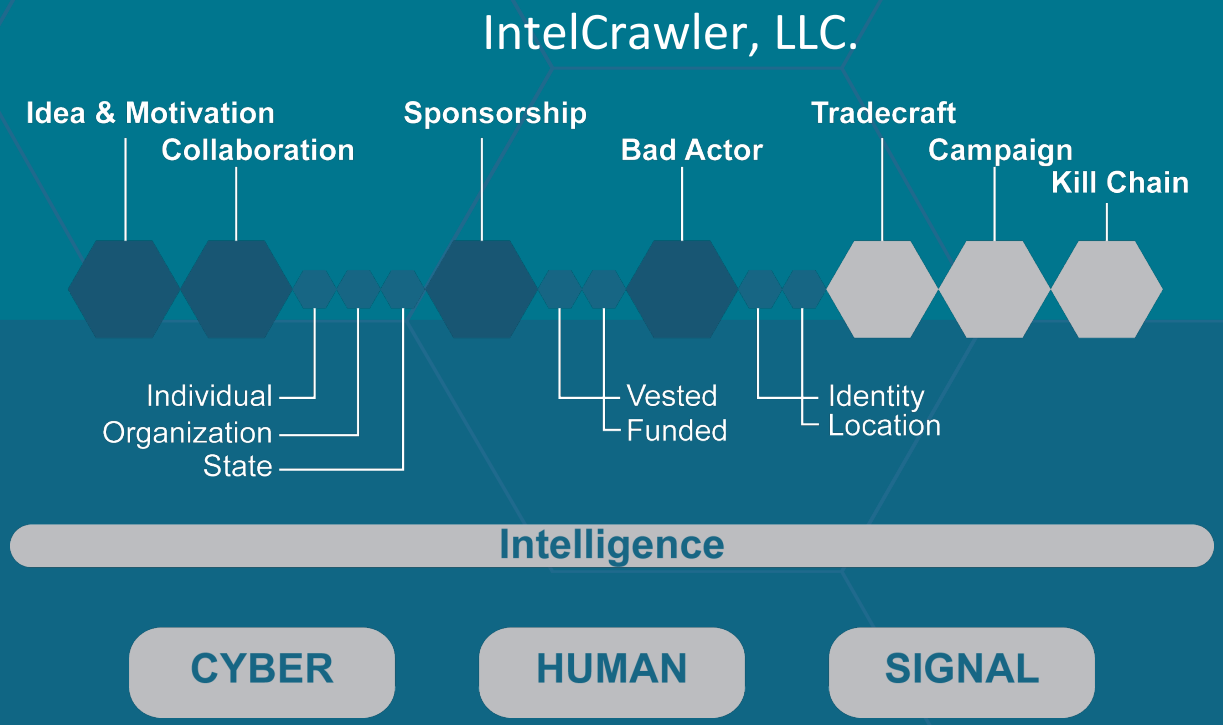
Andrew Komarov
President & Chief Intelligence Officer

Agenda

1. Malware Intelligence
2. O-Day Marketplaces
3. Anti-Fraud Bypass Trends
4. POS e-Crimes
5. Money Laundering Intelligence
6. Questions

Executive Summary

- Cyber Intelligence
- Context-aware Cyber Intelligence Platform (SIGINT)
- Operative Human Intelligence (HUMINT)



Capability & Capacity

15 years HUMINT experience

20 years SIGINT experience

1,520,000 bad actors monitored

752,000 attacks identified

5 TB per day of aggregated data

Rapid intelligence response

Communications and Technologies

Energy and Natural Resources

Financial Services

Healthcare

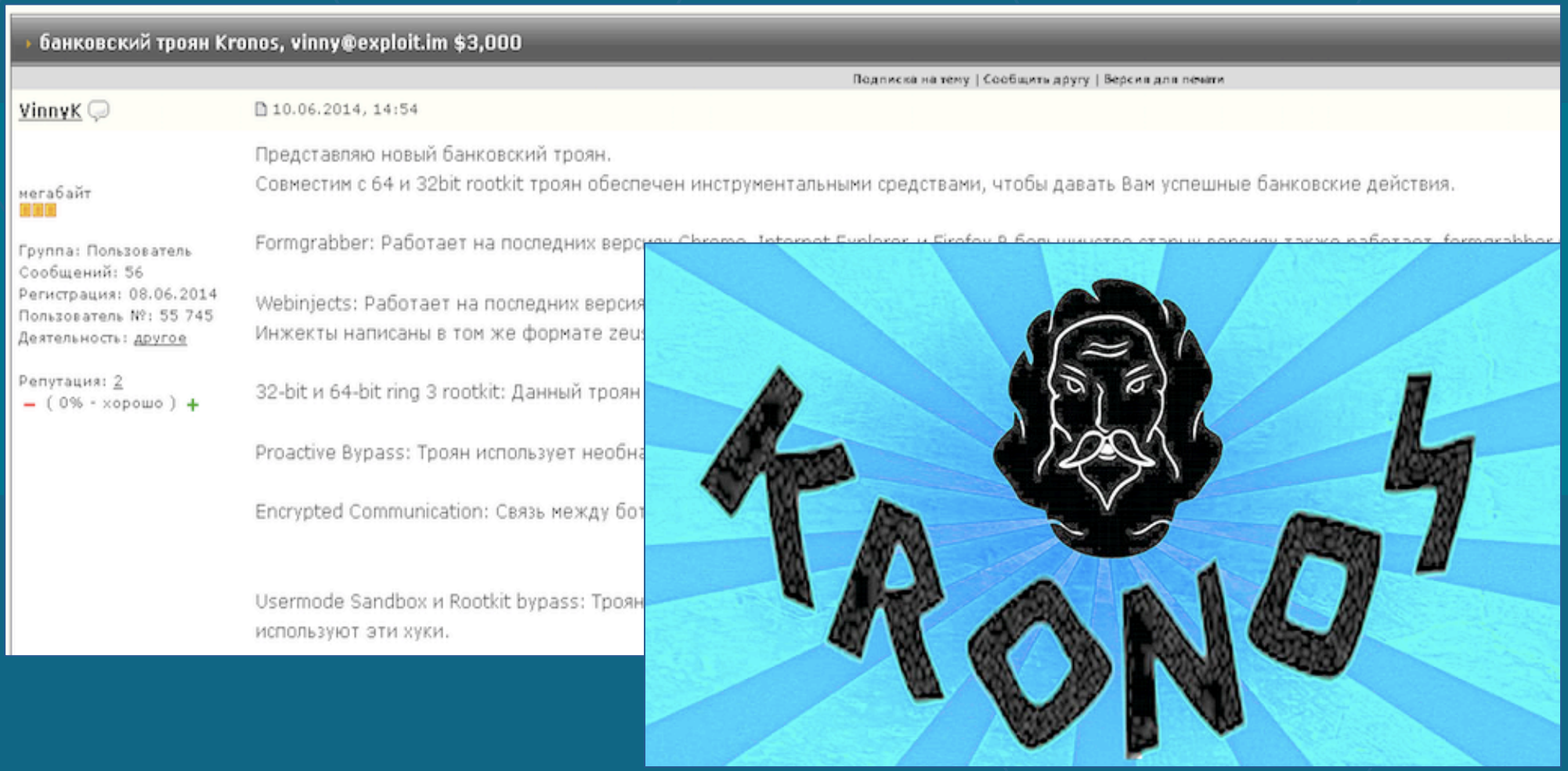
Manufacturing

Public Sector

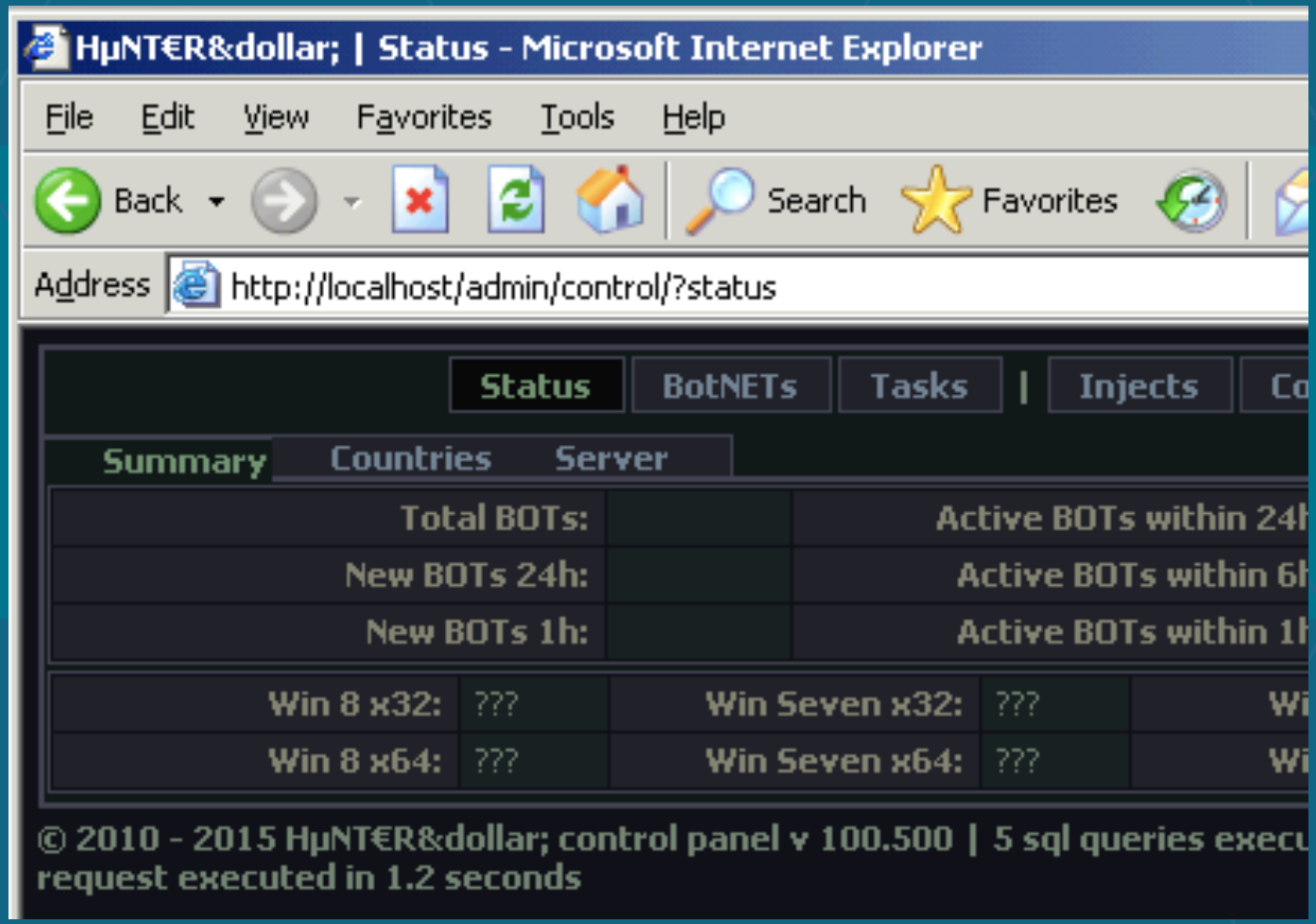
Consumer and Retail

Travel and Transportation

New Players in Online-Banking Theft

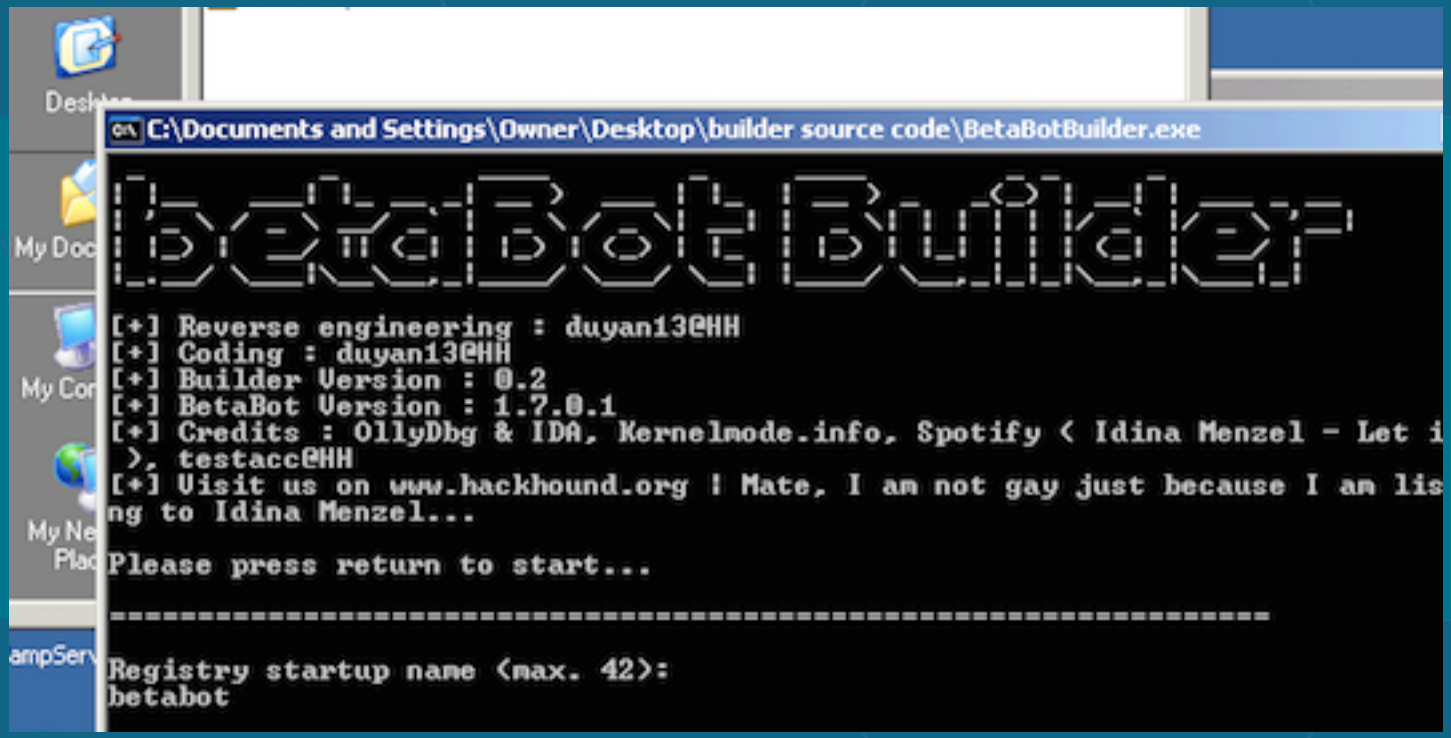


Online-Banking Theft Malware Trends



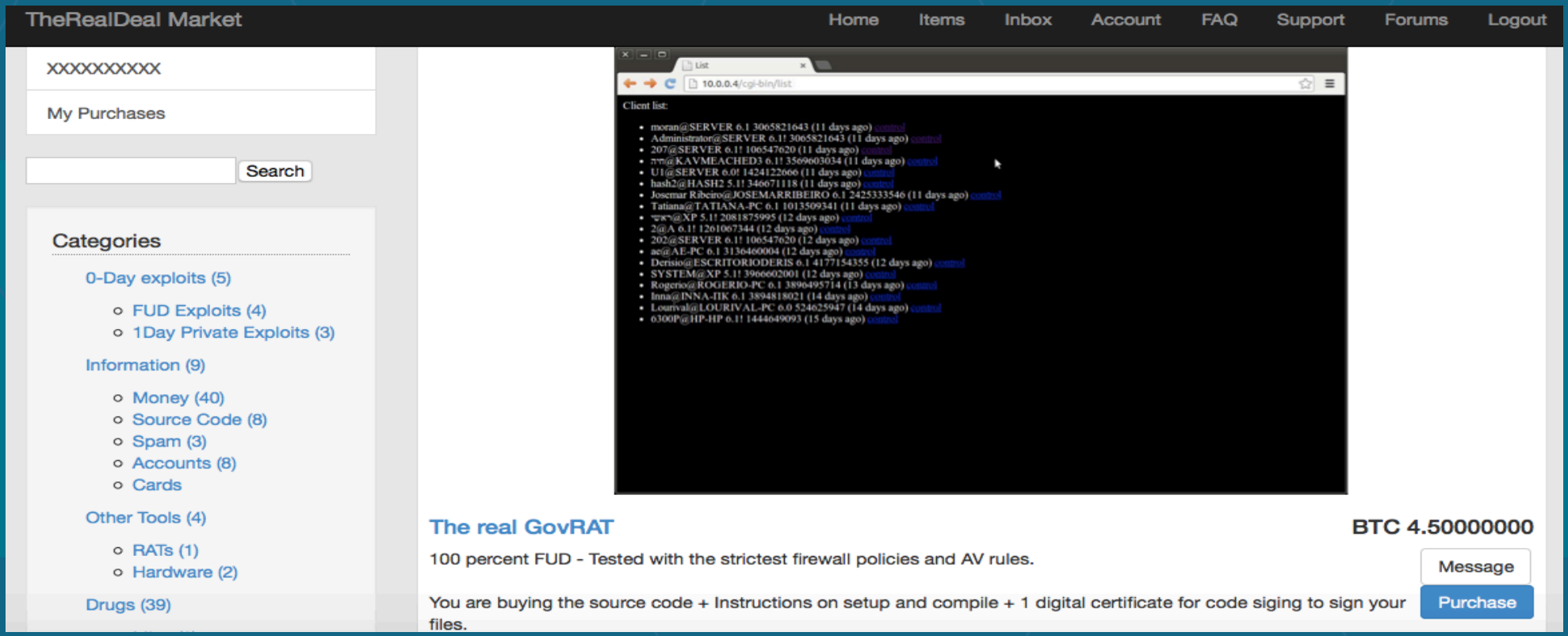
#1 - HunterDollar

Online-Banking Theft Malware Trends



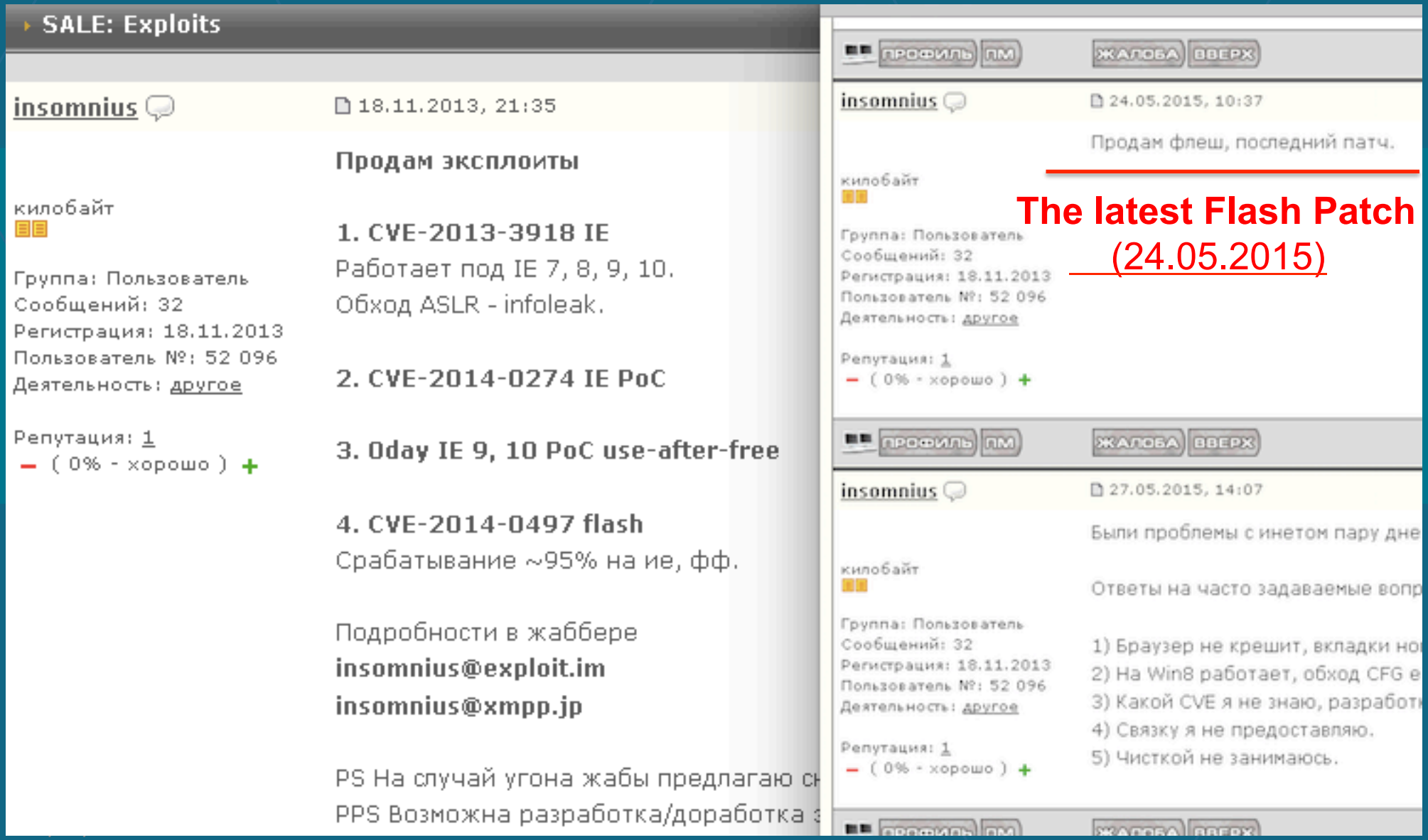
#2 - BetaBot

APTs become easier – Sign Your Malware!



+1 Digital Certificate for Code Signing (BTC 4.50)

0-Day Exploits Trading - Huge Market



SALE: Exploits

insomnius — 18.11.2013, 21:35

Продам эксплоиты

1. CVE-2013-3918 IE
Работает под IE 7, 8, 9, 10.
Обход ASLR - infoleak.

2. CVE-2014-0274 IE PoC

3. Oday IE 9, 10 PoC use-after-free

4. CVE-2014-0497 flash
Срабатывание ~95% на ие, фф.

Подробности в жаббере
insomnius@exploit.im
insomnius@xmpp.jp

PS На случай угона жабы предлагаю сн
PPS Возможна разработка/доработка э

килобайт
Группа: Пользователь
Сообщений: 32
Регистрация: 18.11.2013
Пользователь №: 52 096
Деятельность: другое
Репутация: 1
– (0% - хорошо) +

ПРОФИЛЬ ПМ ЖАЛОБА ВВЕРХ

insomnius — 24.05.2015, 10:37

Продам флеш, последний патч.

The latest Flash Patch (24.05.2015)

килобайт
Группа: Пользователь
Сообщений: 32
Регистрация: 18.11.2013
Пользователь №: 52 096
Деятельность: другое
Репутация: 1
– (0% - хорошо) +

ПРОФИЛЬ ПМ ЖАЛОБА ВВЕРХ

insomnius — 27.05.2015, 14:07

Были проблемы с инетом пару дне

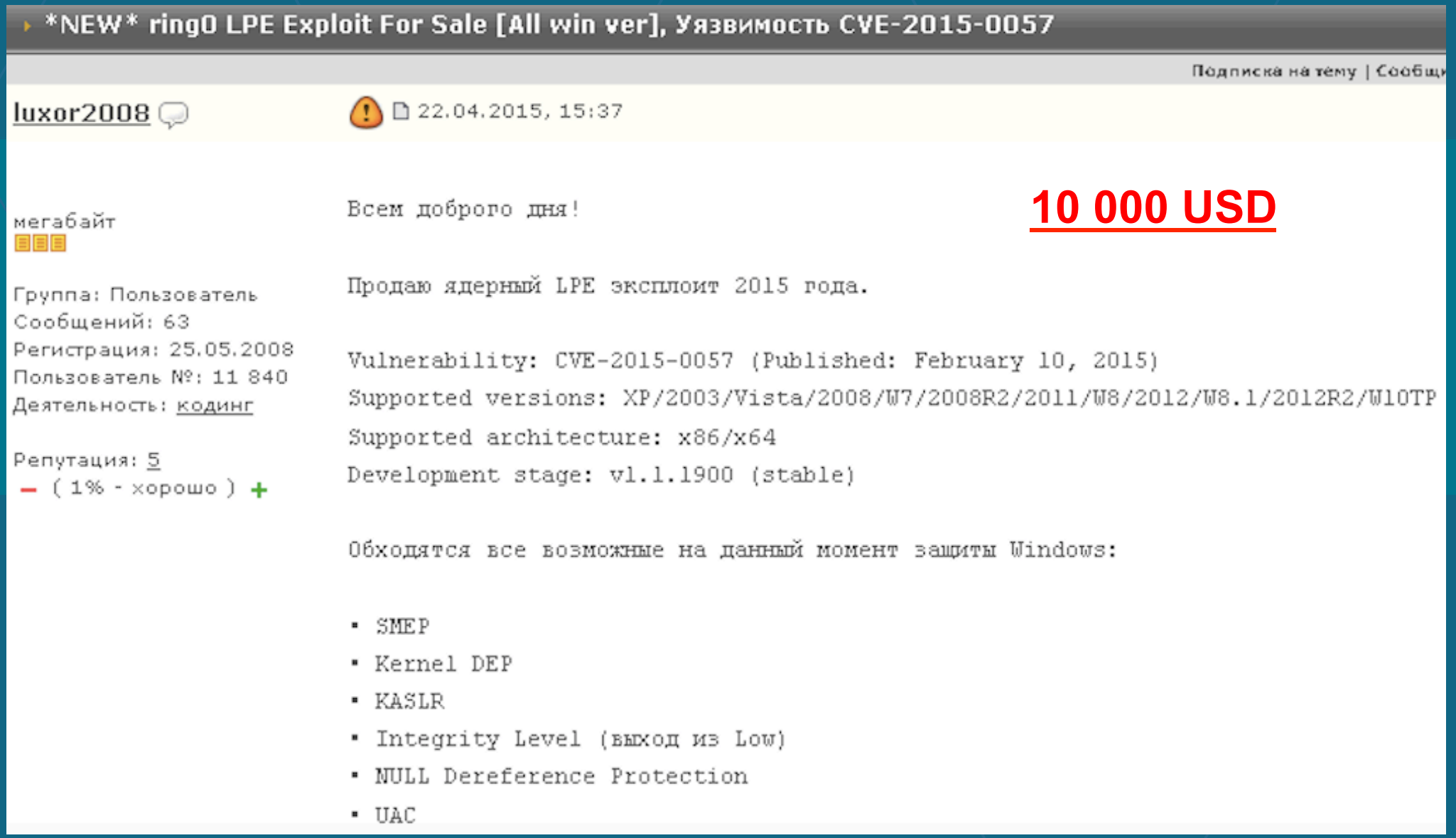
Ответы на часто задаваемые вопр

1) Браузер не крешит, вкладки но
2) На Win8 работает, обход CFG е
3) Какой CVE я не знаю, разработ
4) Связку я не предоставляю.
5) Чисткой не занимаюсь.

килобайт
Группа: Пользователь
Сообщений: 32
Регистрация: 18.11.2013
Пользователь №: 52 096
Деятельность: другое
Репутация: 1
– (0% - хорошо) +

ПРОФИЛЬ ПМ ЖАЛОБА ВВЕРХ

0-Day Exploits Trading - Huge Market



NEW ringO LPE Exploit For Sale [All win ver], Уязвимость CVE-2015-0057

Подписка на тему | Сообщ

luxor2008

22.04.2015, 15:37

мегабайт

Группа: Пользователь
Сообщений: 63
Регистрация: 25.05.2008
Пользователь №: 11 840
Деятельность: кодинг

Репутация: 5
– (1% - хорошо) +

Всем доброго дня!

10 000 USD

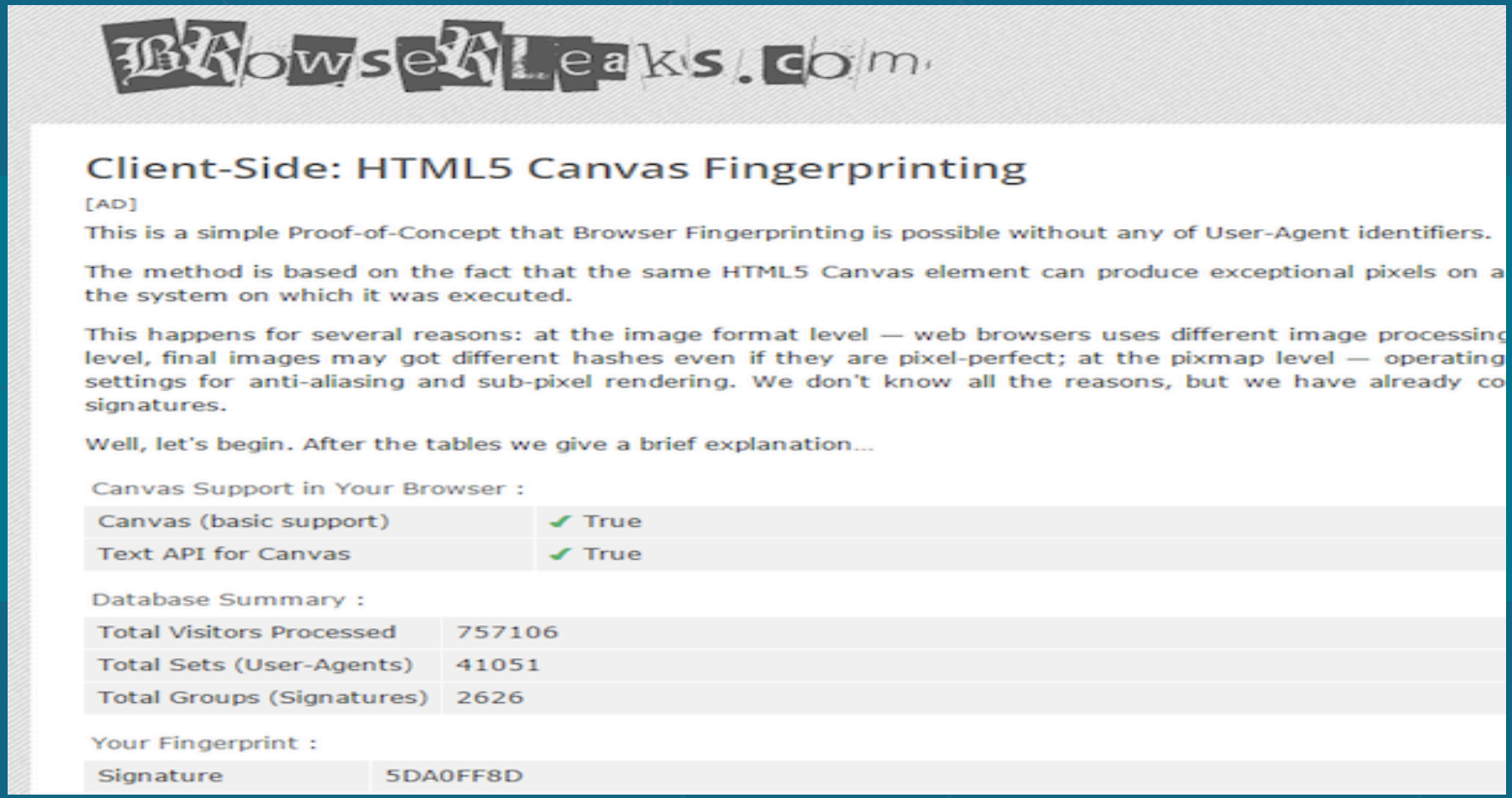
Продаю ядерный LPE эксплоит 2015 года.

Vulnerability: CVE-2015-0057 (Published: February 10, 2015)
Supported versions: XP/2003/Vista/2008/W7/2008R2/2011/W8/2012/W8.1/2012R2/W10TP
Supported architecture: x86/x64
Development stage: v1.1.1900 (stable)

Обходятся все возможные на данный момент защиты Windows:

- SMEP
- Kernel DEP
- KASLR
- Integrity Level (выход из Low)
- NULL Dereference Protection
- UAC

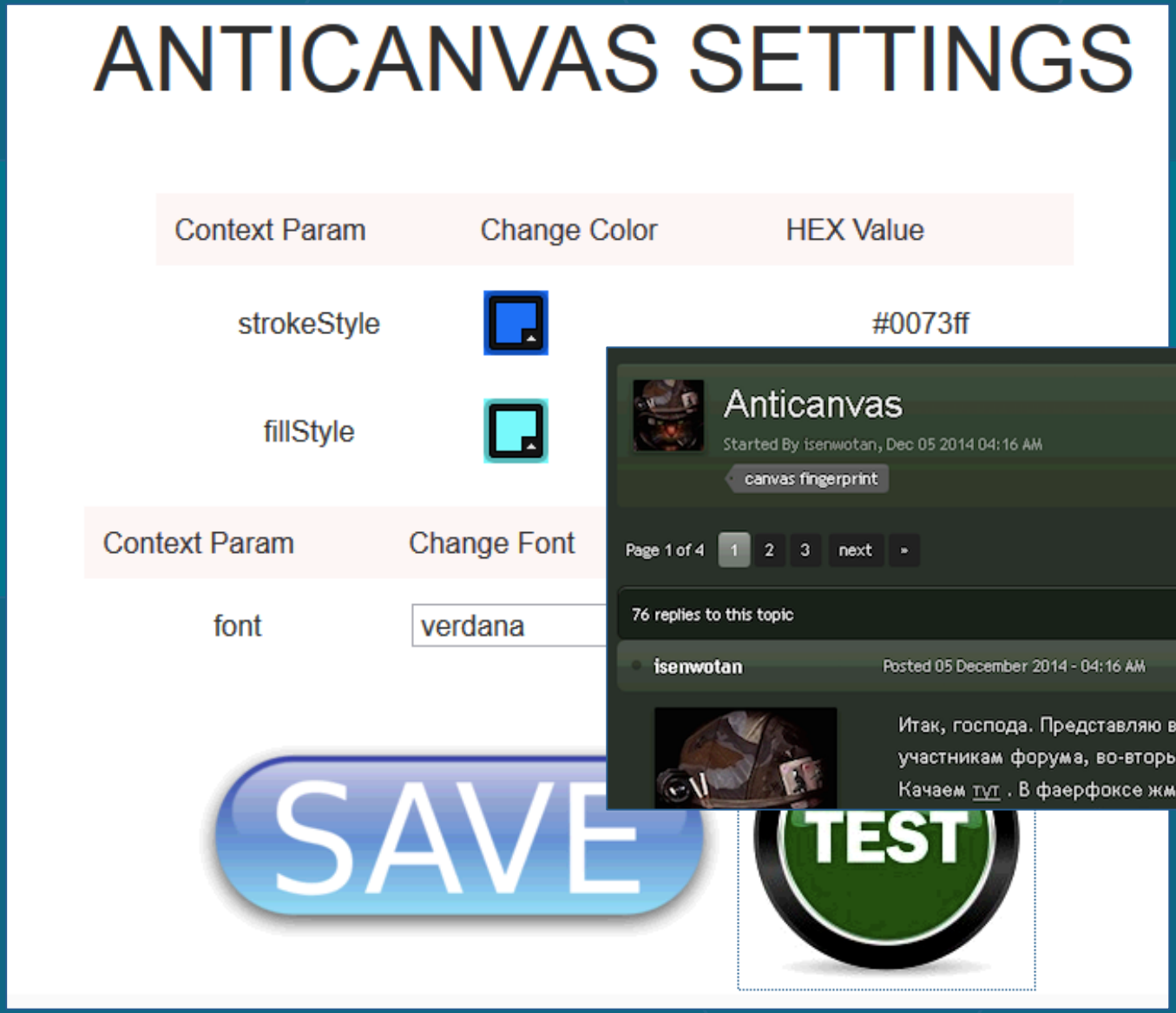
Browser Anti-Detect Mechanisms



Used In 99% Anti-Fraud Products (Online-Banking)

Browser Anti-Detect Mechanisms

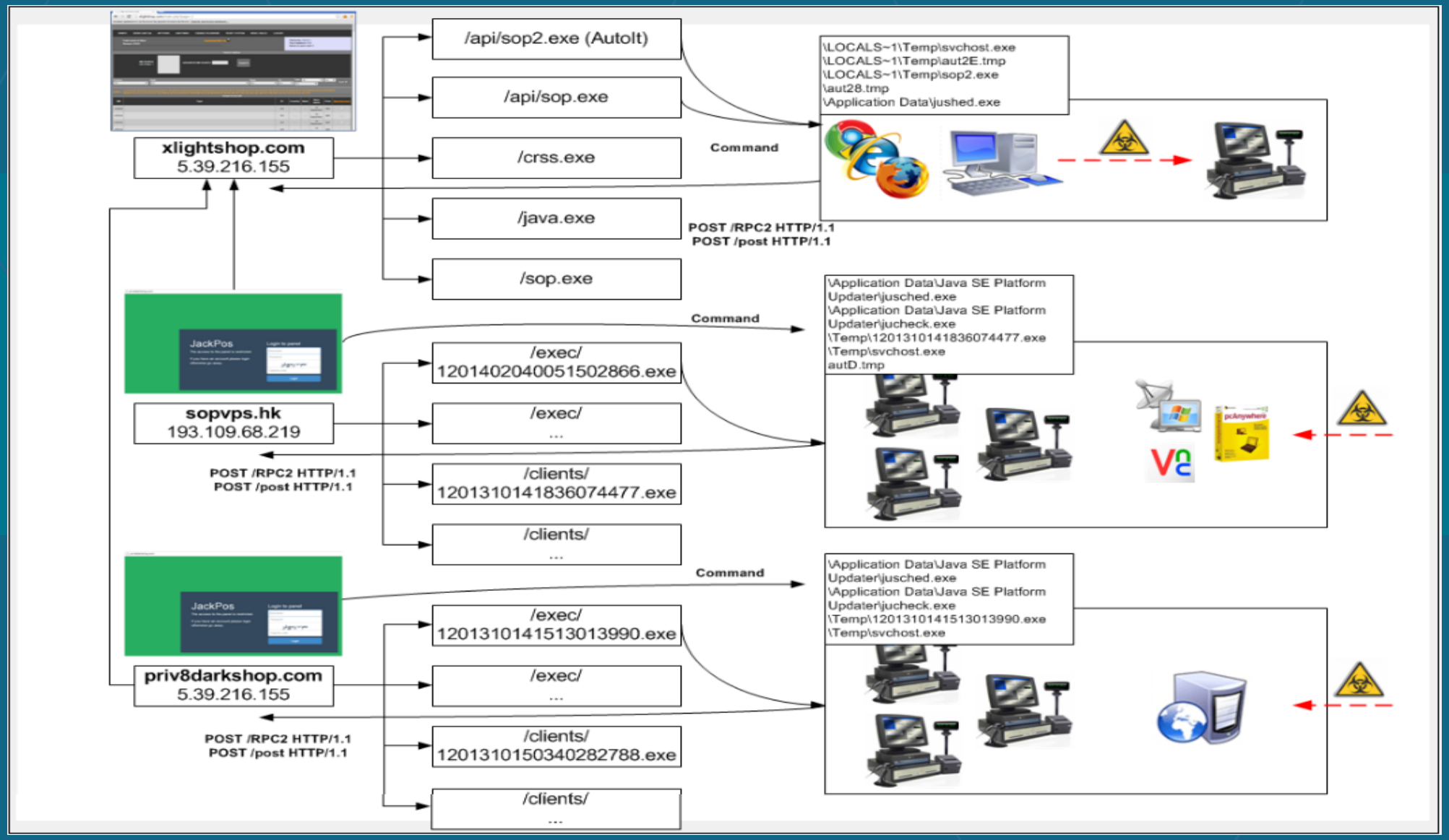
- WebCRT
- Canvas

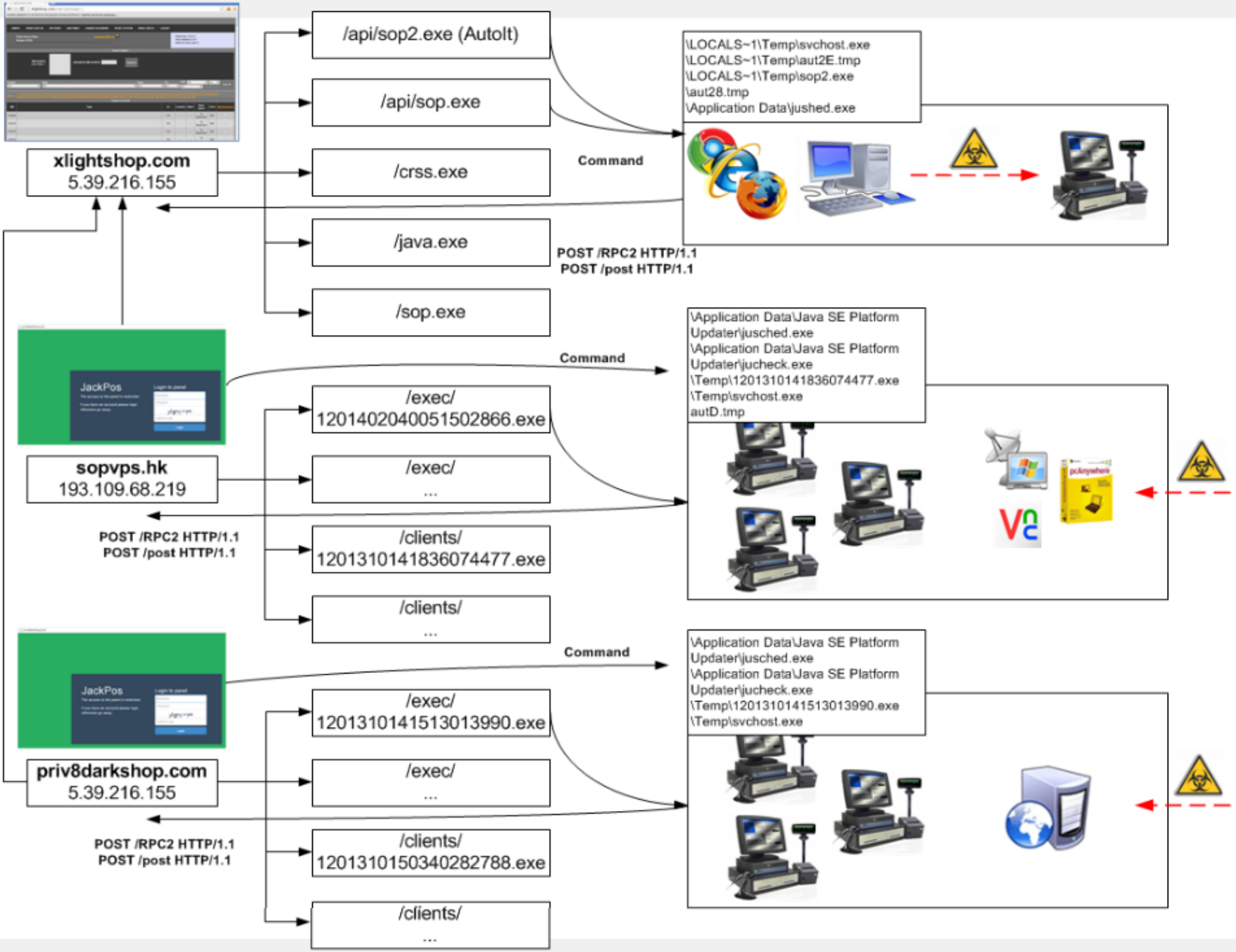


Point-of-Sales Infections

vs

Cyber Attack Lifecycle (POS)




/api/sop2.exe (AutoIt)
/api/sop.exe
/crss.exe
/java.exe
/sop.exe
xlightshop.com
5.39.216.155
Command
\LOCALS~1\Temp\svchost.exe
\LOCALS~1\Temp\aut2E.tmp
\LOCALS~1\Temp\sop2.exe
\aut28.tmp
\Application Data\jushed.exe
POST /RPC2 HTTP/1.1
POST /post HTTP/1.1
JackPos
sopvps.hk
193.109.68.219
Command
/exec/
120140204005150286 6.exe
/exec/
...
/clients/
120131014183607447 7.exe
/clients/
...
POST /RPC2 HTTP/1.1
POST /post HTTP/1.1
\Application Data\Java SE Platform Updater\jusched.exe
\Application Data\Java SE Platform Updater\jucheck.exe
\Temp\120131014183607447 7.exe
\Temp\svchost.exe
autD.tmp
pcAnywhere
JackPos
priv8darkshop.com
5.39.216.155
Command
/exec/
120131014151301399 0.exe
/exec/
...
/clients/
120131015034028278 8.exe
/clients/
...
POST /RPC2 HTTP/1.1
POST /post HTTP/1.1
\Application Data\Java SE Platform Updater\jusched.exe
\Application Data\Java SE Platform Updater\jucheck.exe
\Temp\120131014151301399 0.exe
\Temp\svchost.exe

Money Laundering Intelligence

Reasons for Suspicion

Fraud

Money Laundering

Corruption

Sanctions

Drug / Weapon / Human Trafficking

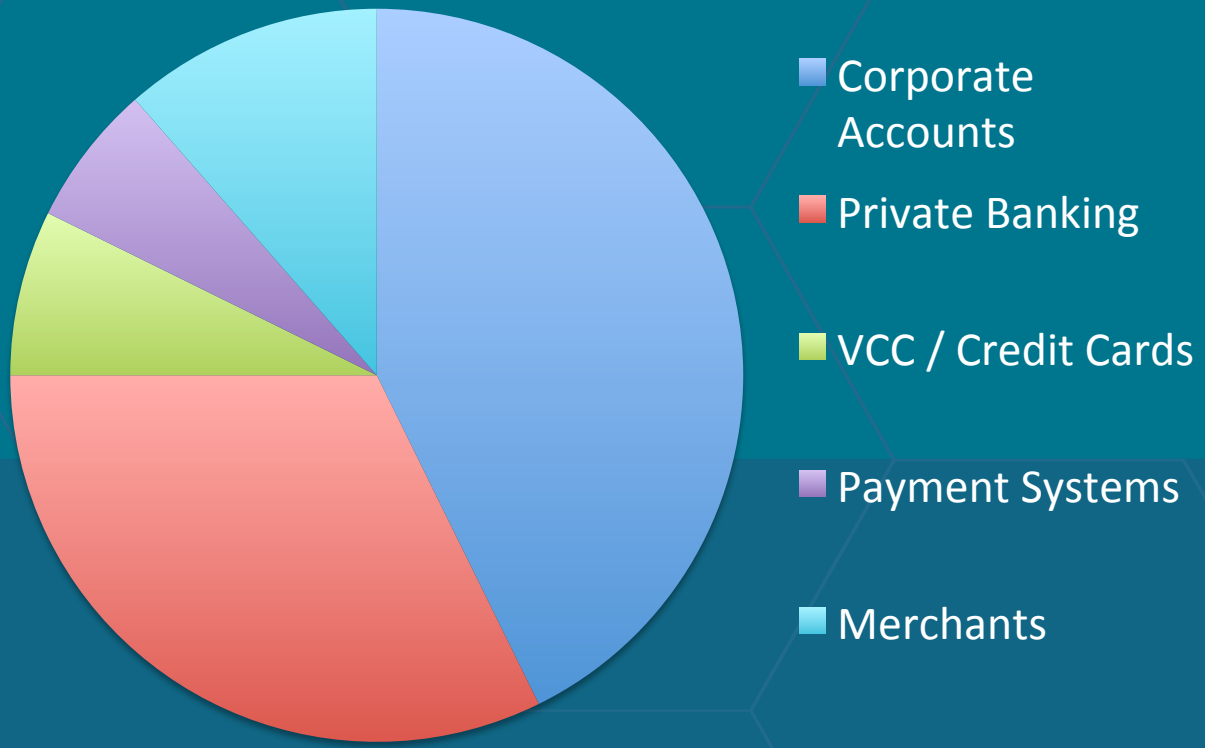
Tax Evasion

Declined Business

Organized Crime

Money Laundering Intelligence

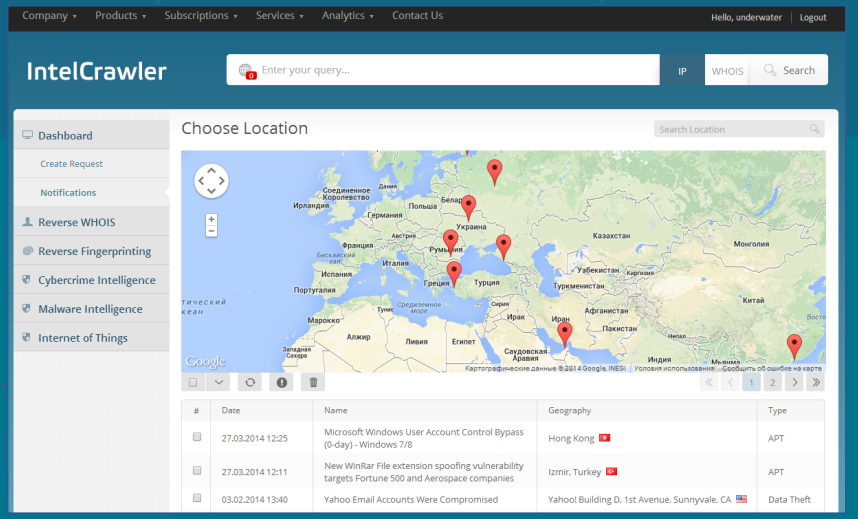
Statistics



Money Laundering Intelligence Database

Types Of Intelligence

- Money Mules
- Suspicious Organizations
- Government / Sanctioned Lists
- E-Crime / Organized Crime



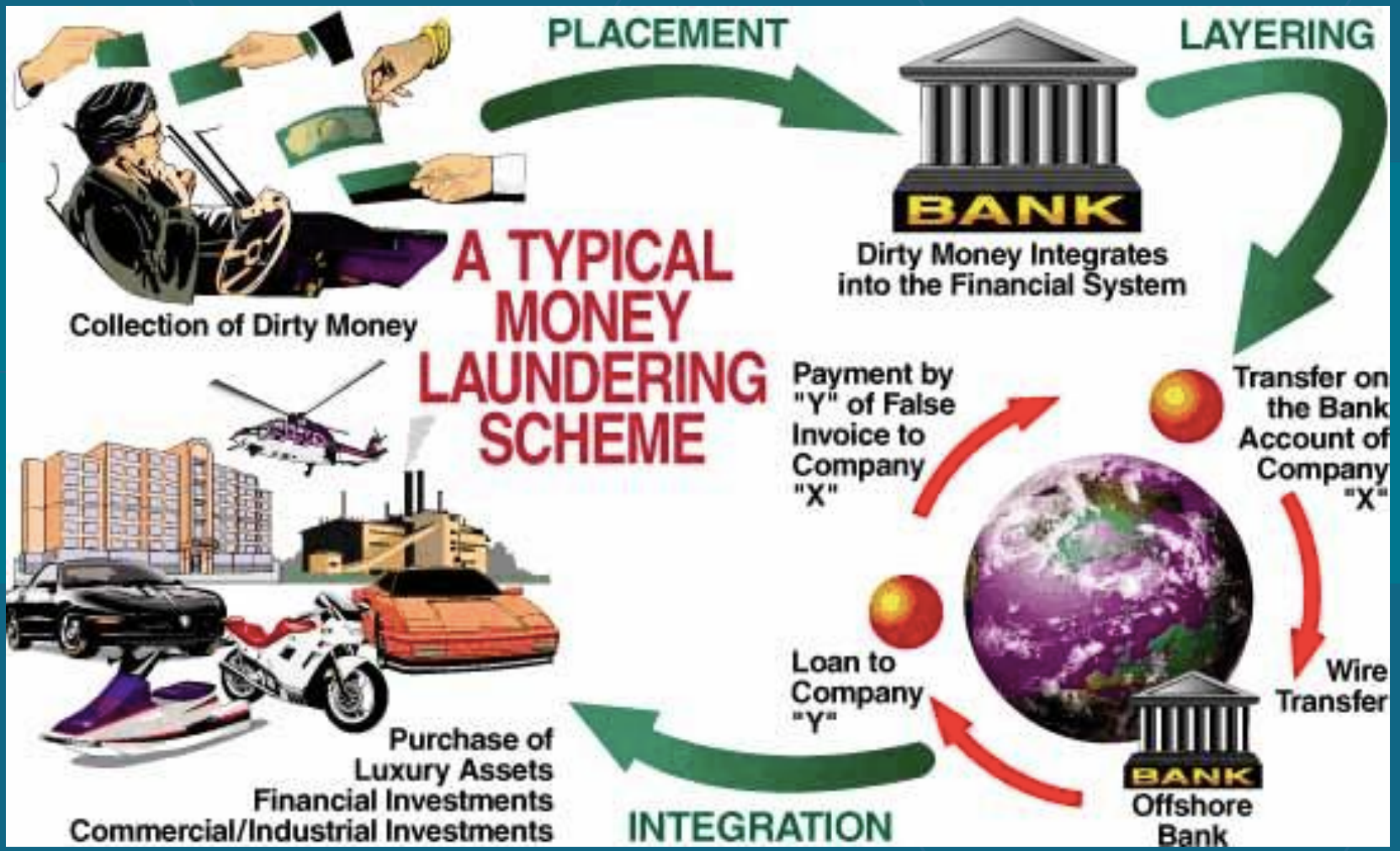
Alternatives

- Thompson Reuters Risk Intelligence
- Lexis Nexis

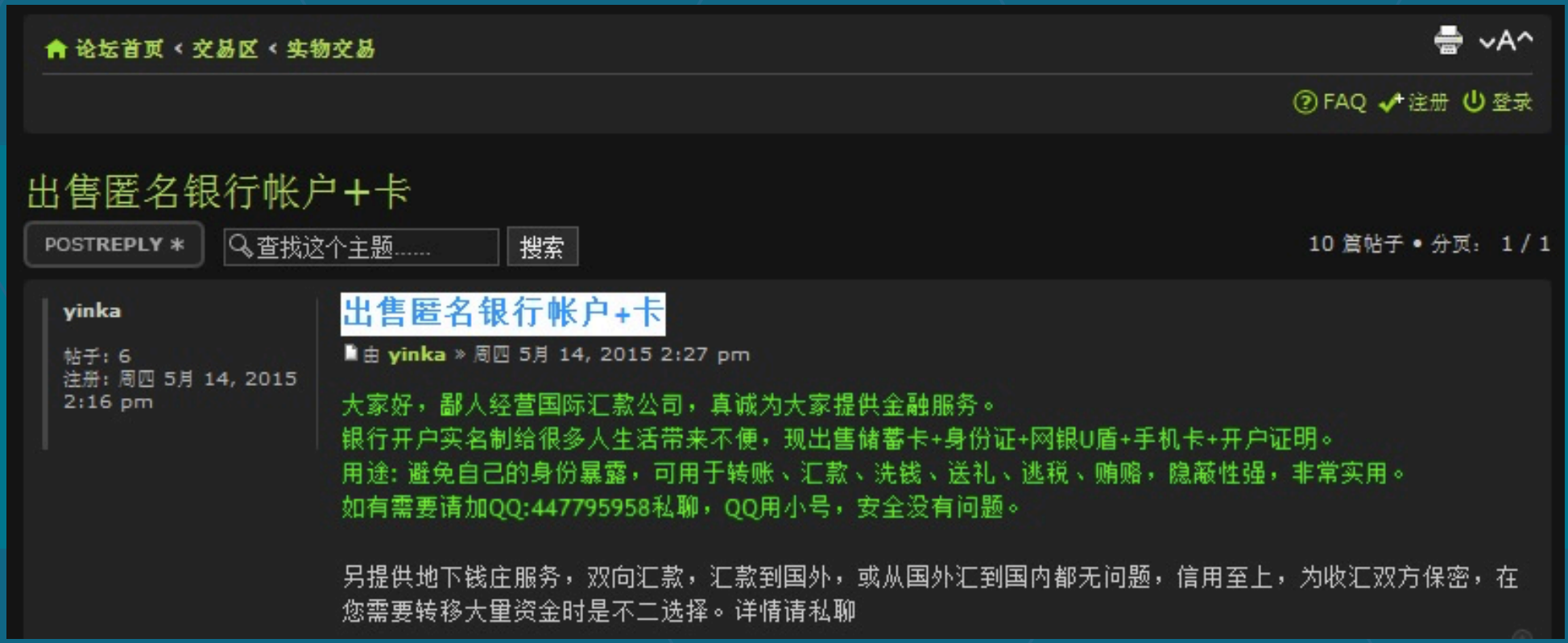
STYX
XML
JSON

SUBSCRIBE (Only For Banks & LEA)

Money Laundering – Typical Scheme



Money Laundering – Non-Typical Scheme



“Providing Anonymous Banking Accounts” (EU/USA/UK) (14.05.2015, 2:27 PM)

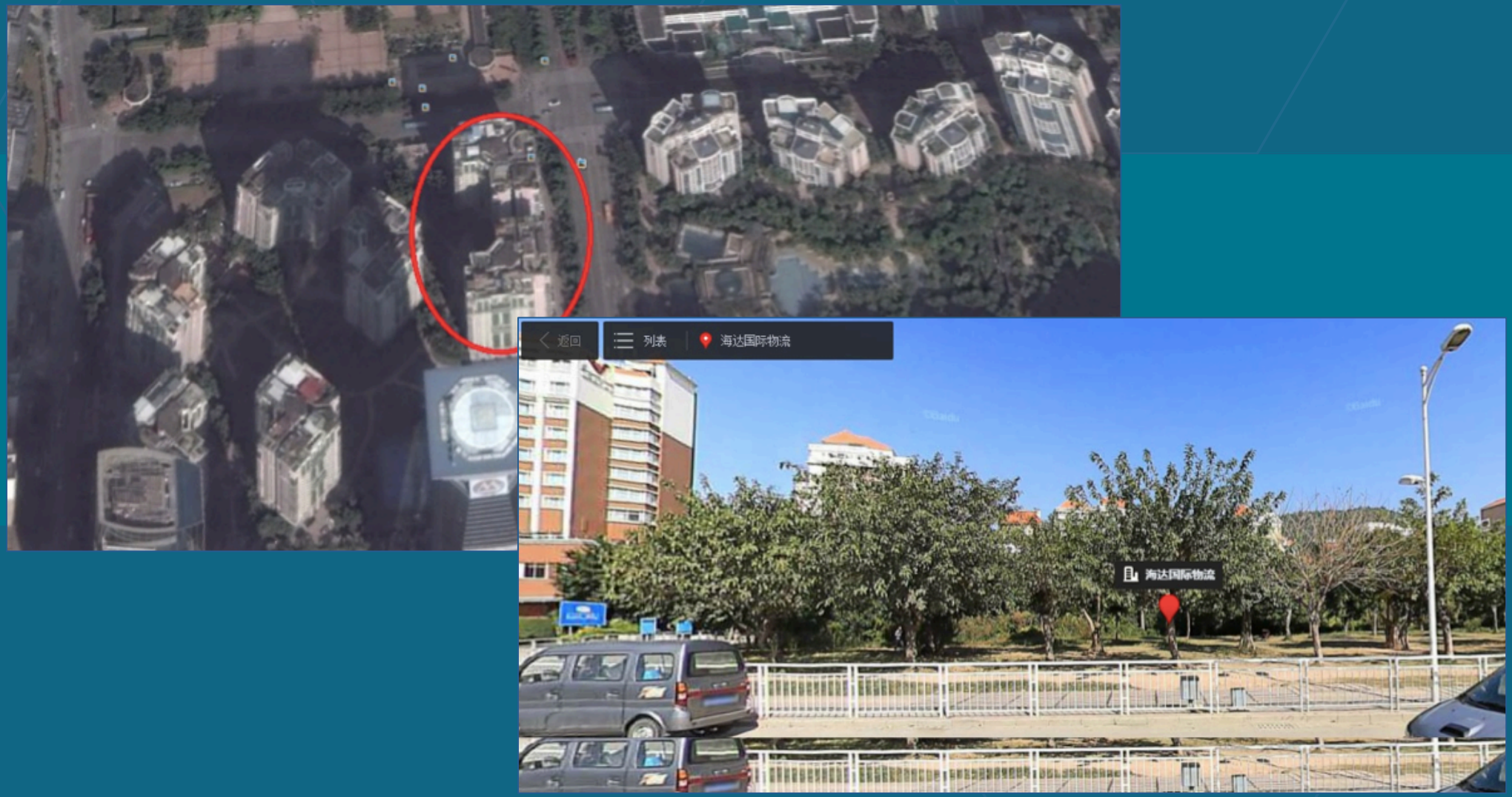
Money Laundering – Non-Typical Scheme

Оплаченная реклама

VISA	**Обнал-сервис от Mavr009** Налим юр. лица (комиссия от 30%) и физ. лица (комиссия от 25%). АКЦИЯ: налим QIWI за 15%. Крупная приемка в КИТАЕ. ДЕПОЗИТ 22 000 USD. 	**Примем заливы на Китай.** от Mavr009
VISA	**Интернет-магазин дебетовых карт - debet.cc** On-line сервис по продаже дебетовых карт - 24/7. QIWI/Яндекс кошельки. Оперативная доставка.	**Дебетовые карты** от LaCoka
VISA	**[РФ] Обнал-сервис QIWI, WebMoney, Yandex от QvP.** (просматривают: 1) Налим QIWI, WM, ЯД, Принимаю заливы на МТС,Билайн, Мегафон. Всегда в наличие QIWI карты. ДЕПОЗИТ 5000 $	**Обнал-сервис QIWI, WM, ЯД** от QvP

15/25% - big corporate accounts
Also Individuals. Will help you to transfer or hide your money

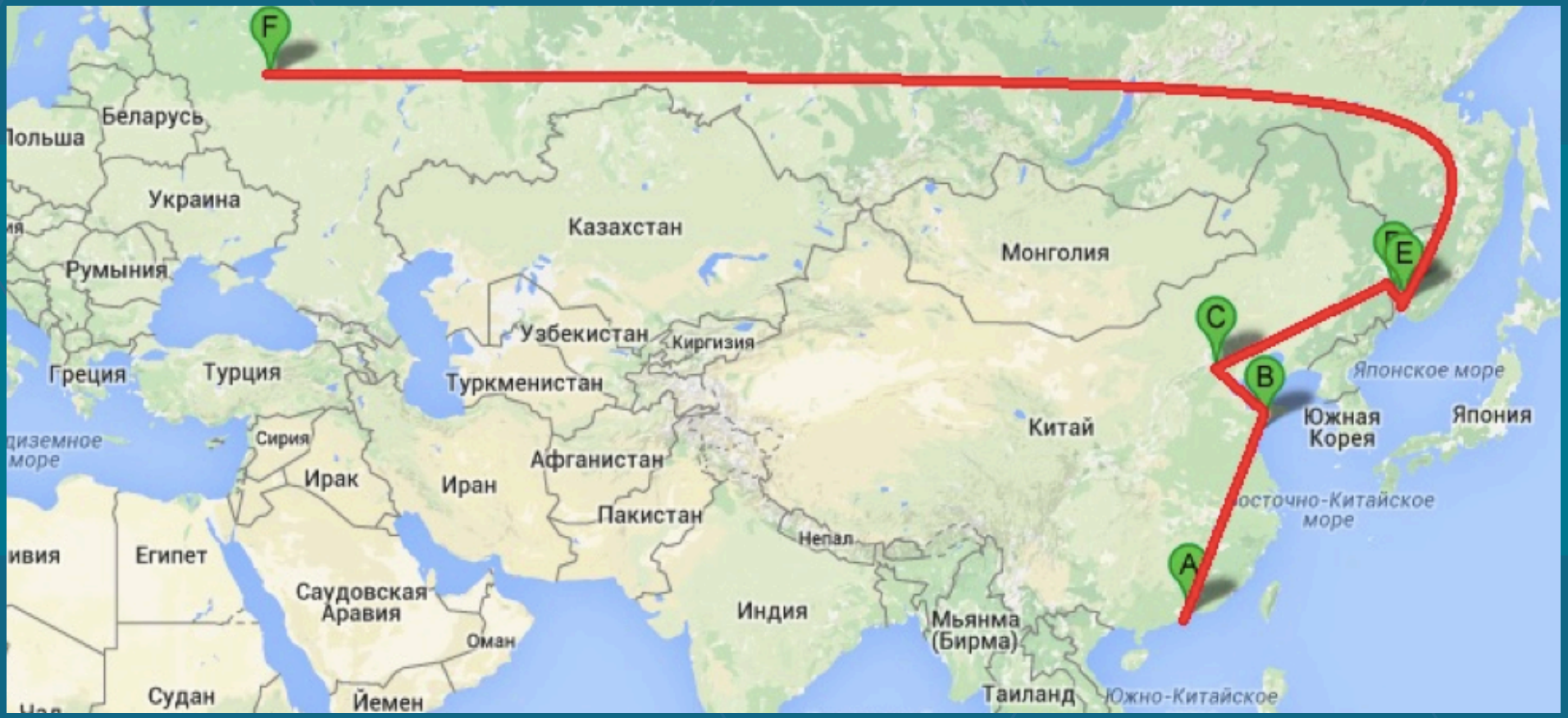
Money Laundering – Non-Typical Scheme



Money Laundering – Non-Typical Scheme

Sea-Based Logistics, Warehouse

Money Laundering – Non-Typical Scheme



"Asian" Path

QUESTIONS

ak@intelcrawler.com
www.intelcrawler.com