



**IntelCrawler™**  
cyber threat intelligence

## **e-Crime Intelligence in Financial Sector**

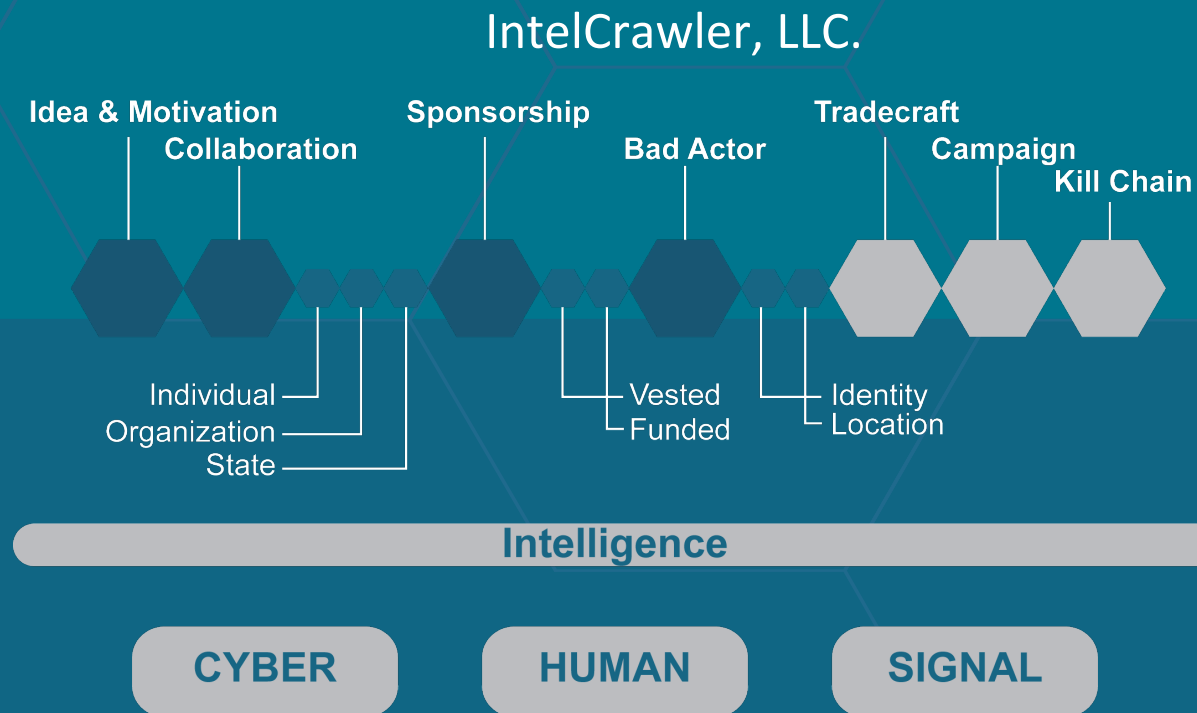
**Andrew Komarov**  
**President & Chief Intelligence Officer**

# 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

Банковский троян Kronos, vinny@exploit.im \$3,000

Подписка на тему | Сообщить другу | Версия для печати

**VinnyK** 10.06.2014, 14:54

Представляю новый банковский троян.  
Совместим с 64 и 32bit rootkit троян обеспечен инструментальными средствами, чтобы давать Вам успешные банковские действия.

мегабайт

Группа: Пользователь  
Сообщений: 56  
Регистрация: 08.06.2014  
Пользователь №: 55 745  
Деятельность: [другое](#)

Репутация: 2  
- ( 0% - хорошо ) +

Formgrabber: Работает на последних версиях Chrome, Internet Explorer и Firefox. В браузере сразу запускается formgrabber.


Webinjects: Работает на последних версиях браузеров. Инжекты написаны в том же формате zeus.

32-bit и 64-bit ring 3 rootkit: Данный троян использует эти хуки.

Proactive Bypass: Троян использует необна.

Encrypted Communication: Связь между ботом и сервером зашифрована.

Usermode Sandbox и Rootkit bypass: Троян использует эти хуки.



# Online-Banking Theft Malware Trends

## #1 - HunterDollar

Address <http://localhost/admin/control/?status>

**Status** BotNETs Tasks Injects Co

Summary		Countries	Server	
Total BOTs:			Active BOTs within 24h	
New BOTs 24h:			Active BOTs within 6h	
New BOTs 1h:			Active BOTs within 1h	
Win 8 x32:	???	Win Seven x32:	???	Wi
Win 8 x64:	???	Win Seven x64:	???	Wi

© 2010 - 2015 HunterDollar; control panel v 100.500 | 5 sql queries executed request executed in 1.2 seconds

# Online-Banking Theft Malware Trends

## #2 - BetaBot

```
C:\Documents and Settings\Owner\Desktop\builder source code\BetaBotBuilder.exe

betaBot Builder

[+] Reverse engineering : duyan13@HH
[+] Coding : duyan13@HH
[+] Builder Version : 0.2
[+] BetaBot Version : 1.7.0.1
[+] Credits : OllyDbg & IDA, Kernelmode.info, Spotify < Idina Menzel - Let it be, testacc@HH
[+] Visit us on www.hackhound.org | Mate, I am not gay just because I am listening to Idina Menzel...

Please press return to start...

-----

Registry startup name <max. 42>:
betabot
```

# APTs become easier – Sign Your Malware!

TheRealDeal Market

Home Items Inbox Account FAQ Support Forums Logout

XXXXXXXXXX

My Purchases

Search

Categories

- 0-Day exploits (5)
  - FUD Exploits (4)
  - 1Day Private Exploits (3)
- Information (9)
  - Money (40)
  - Source Code (8)
  - Spam (3)
  - Accounts (8)
  - Cards
- Other Tools (4)
  - RATs (1)
  - Hardware (2)
- Drugs (39)

**The real GovRAT** BTC 4.50000000

100 percent FUD - Tested with the strictest firewall policies and AV rules.

You are buying the source code + Instructions on setup and compile + 1 digital certificate for code signing to sign your files.

Message Purchase

```
Client list:
• moran@SERVER 6.1 3065821643 (11 days ago) control
• Administrator@SERVER 6.1 3065821643 (11 days ago) control
• 207@SERVER 6.1 106547620 (11 days ago) control
• KAVMEACHED3 6.1 3569603034 (11 days ago) control
• U1@SERVER 6.0 1424122666 (11 days ago) control
• hash2@HASH2 5.1 346671118 (11 days ago) control
• Josemar Ribeiro@JOSEMAR RIBEIRO 6.1 2425333546 (11 days ago) control
• Tatiana@TATIANA-PC 6.1 1013569341 (11 days ago) control
• XP 5.1 2081875995 (12 days ago) control
• 2@a 6.1 1261067344 (12 days ago) control
• 202@SERVER 6.1 106547620 (12 days ago) control
• ac@AE-PC 6.1 3136460004 (12 days ago) control
• Derisio@ESCRITORIODERIS 6.1 4177154355 (12 days ago) control
• SYSTEM@XP 5.1 3966602001 (12 days ago) control
• Rogério@ROGERIO-PC 6.1 3896495714 (13 days ago) control
• Inna@INNA-ITK 6.1 3894818021 (14 days ago) control
• Lourival@LOURIVAL-PC 6.0 524625947 (14 days ago) control
• 0300P@HP-HP 6.1 1444049093 (15 days ago) control
```

+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**

килобайт

Группа: Пользователь  
Сообщений: 32  
Регистрация: 18.11.2013  
Пользователь №: 52 096  
Деятельность: другое

Репутация: 1  
- ( 0% - хорошо ) +

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 с  
PPS Возможна разработка/доработка з

**insomnius** 24.05.2015, 10:37

**Продам флеш, последний патч.**

килобайт

Группа: Пользователь  
Сообщений: 32  
Регистрация: 18.11.2013  
Пользователь №: 52 096  
Деятельность: другое

Репутация: 1  
- ( 0% - хорошо ) +

**The latest Flash Patch  
(24.05.2015)**

**insomnius** 27.05.2015, 14:07

Были проблемы с инетом пару дне

килобайт

Группа: Пользователь  
Сообщений: 32  
Регистрация: 18.11.2013  
Пользователь №: 52 096  
Деятельность: другое

Репутация: 1  
- ( 0% - хорошо ) +


Ответы на часто задаваемые вопро


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

# 0-Day Exploits Trading - Huge Market

► \*NEW\* ring0 LPE Exploit For Sale [All win ver], Уязвимость CVE-2015-0057

Подписка на тему | Сообщить

[luxor2008](#) 

 22.04.2015, 15:37

мегабайт



Всем доброго дня!

**10 000 USD**

Группа: Пользователь

Сообщений: 63

Регистрация: 25.05.2008

Пользователь №: 11 840

Деятельность: [кодинг](#)

Репутация: 5

- ( 1% - хорошо ) +

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

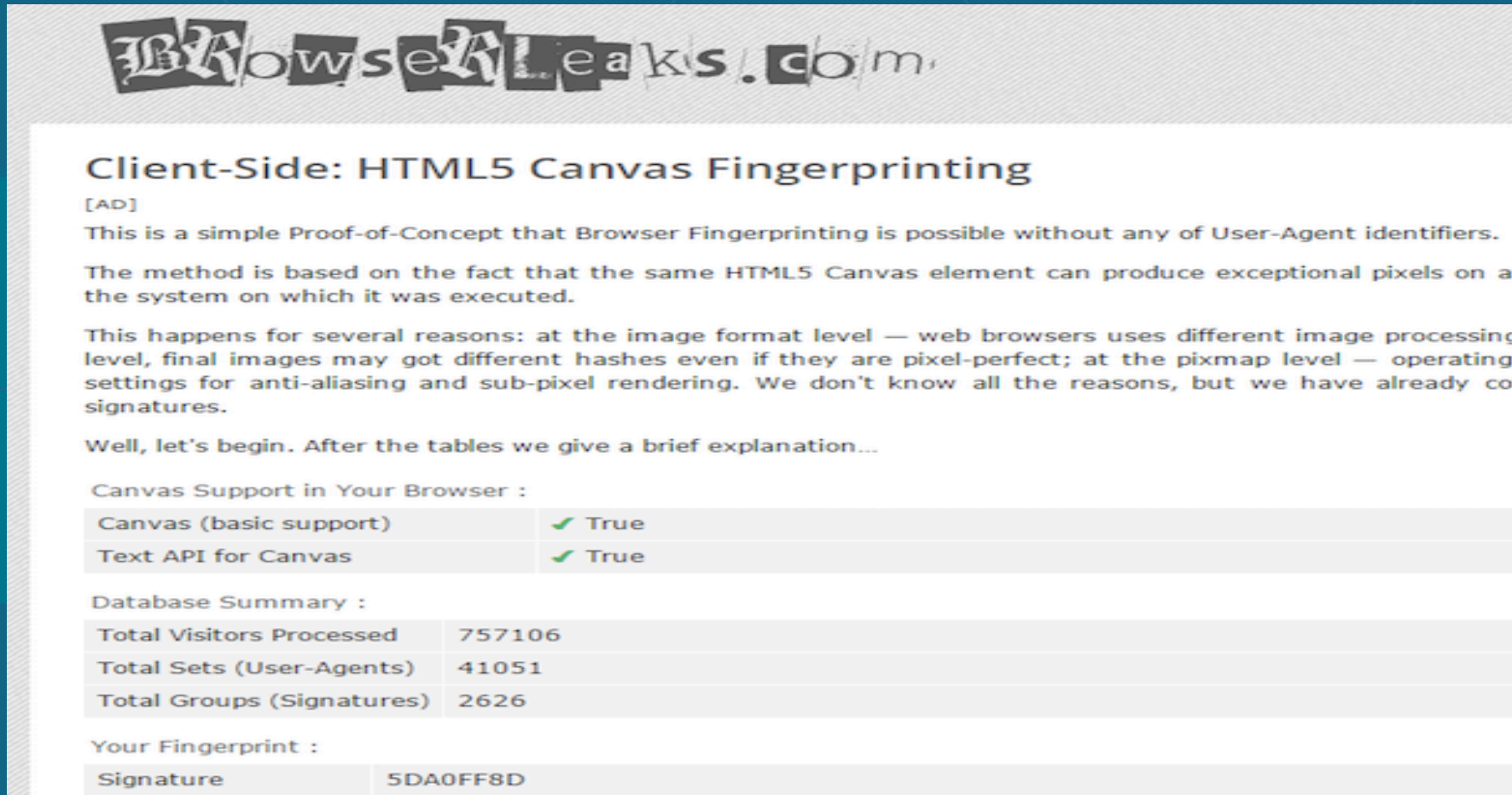
Supported architecture: x86/x64

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



**BrowserLeaks.com**

## Client-Side: HTML5 Canvas Fingerprinting

[AD]

This is a simple Proof-of-Concept that Browser Fingerprinting is possible without any of User-Agent identifiers.

The method is based on the fact that the same HTML5 Canvas element can produce exceptional pixels on a the system on which it was executed.

This happens for several reasons: at the image format level — web browsers uses different image processing level, final images may got different hashes even if they are pixel-perfect; at the pixmap level — operating settings for anti-aliasing and sub-pixel rendering. We don't know all the reasons, but we have already co signatures.

Well, let's begin. After the tables we give a brief explanation...

Canvas Support in Your Browser :

Canvas (basic support)	✓ True
Text API for Canvas	✓ True

Database Summary :

Total Visitors Processed	757106
Total Sets (User-Agents)	41051
Total Groups (Signatures)	2626

Your Fingerprint :

Signature	5DA0FF8D
-----------	----------

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

# Browser Anti-Detect Mechanisms

## ANTICANVAS SETTINGS

Context Param	Change Color	HEX Value
---------------	--------------	-----------

strokeStyle		#0073ff
-------------	---	---------

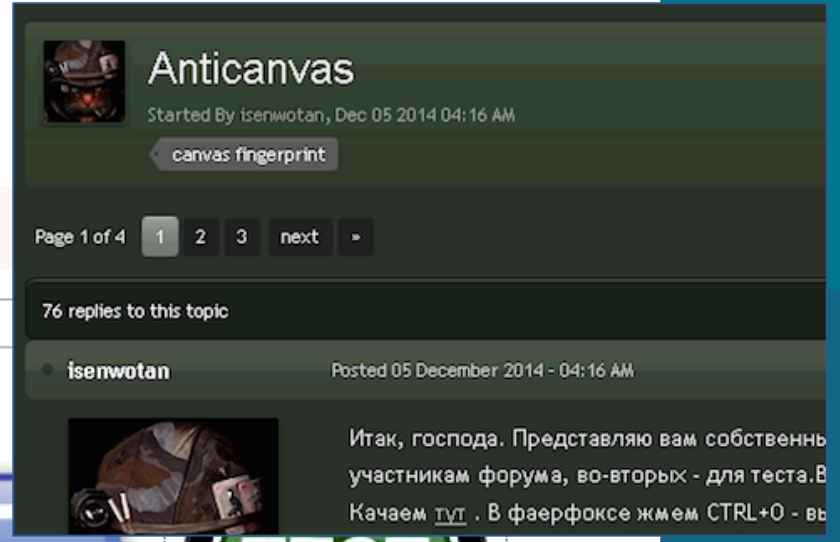
fillStyle	
-----------	---

Context Param	Change Font
---------------	-------------

font	verdana
------	---------

SAVE

TEST



Anticanvas  
Started By isenwotan, Dec 05 2014 04:16 AM  
canvas fingerprint

Page 1 of 4 1 2 3 next >

76 replies to this topic

isenwotan Posted 05 December 2014 - 04:16 AM

Итак, господа. Представляю вам собственнь участникам форума, во-вторых - для теста.В Качаем [TVT](#) . В фаерфоксе жжем CTRL+O - вы

- WebCRT
- Canvas

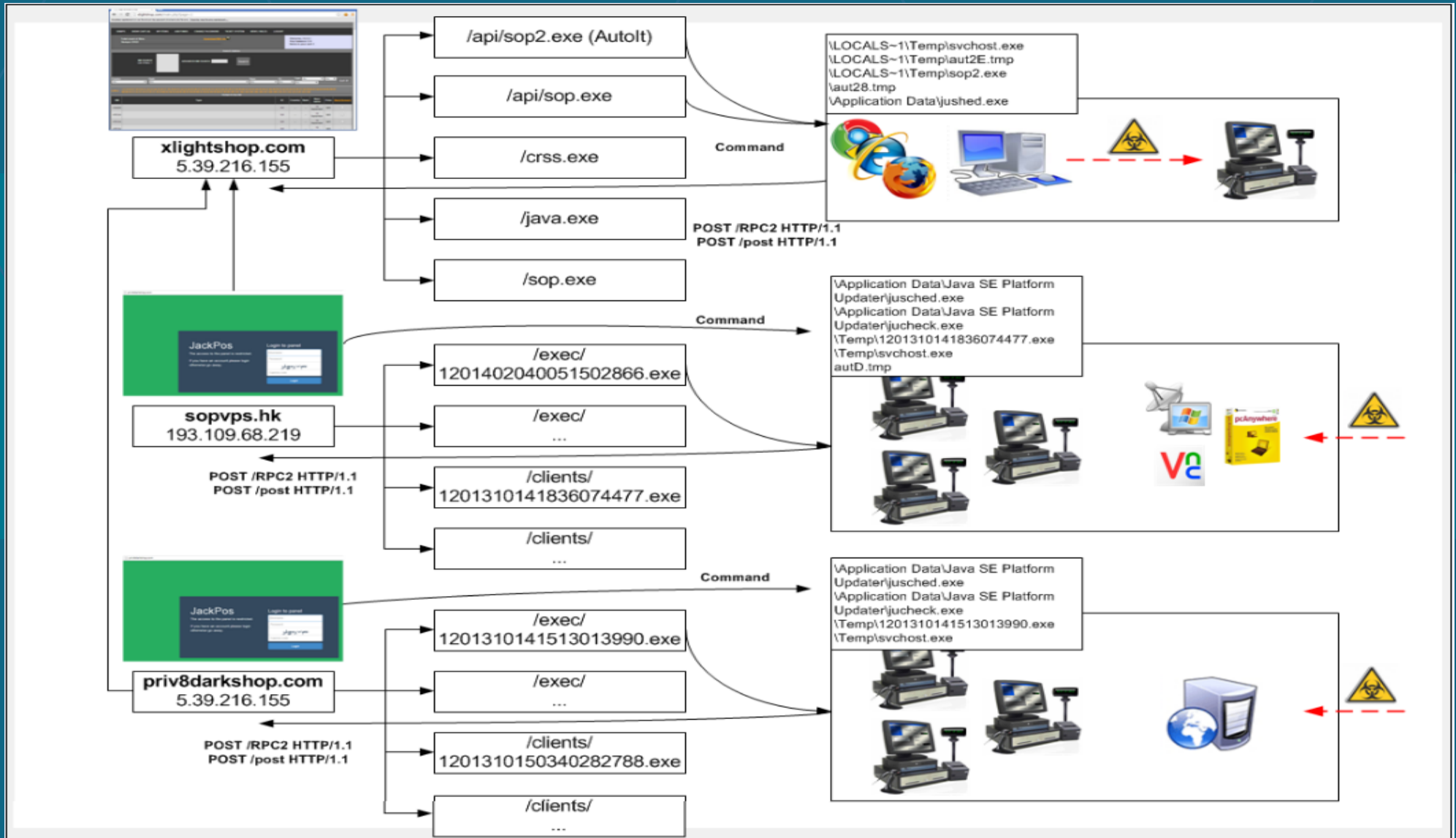
# Point-of-Sales Infections



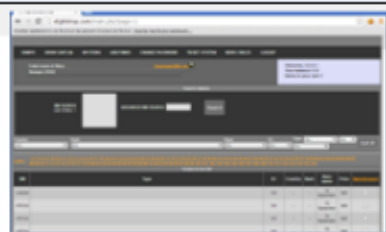
VS



# Cyber Attack Lifecycle (POS)







**xlightshop.com**  
5.39.216.155

- /api/sop2.exe (Autolt)
- /api/sop.exe
- /crss.exe
- /java.exe
- /sop.exe

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



**sopvps.hk**  
193.109.68.219

- /exec/1201402040051502866.exe
- /exec/...
- /clients/1201310141836074477.exe
- /clients/...

Command

Application Data\\Java SE Platform Updater\\jushed.exe  
 Application Data\\Java SE Platform Updater\\jucheck.exe  
 \\Temp\\1201310141836074477.exe  
 \\Temp\\svchost.exe  
 autD.tmp



POST /RPC2 HTTP/1.1  
POST /post HTTP/1.1



**priv8darkshop.com**  
5.39.216.155

- /exec/1201310141513013990.exe
- /exec/...
- /clients/1201310150340282788.exe
- /clients/...

Command

Application Data\\Java SE Platform Updater\\jushed.exe  
 Application Data\\Java SE Platform Updater\\jucheck.exe  
 \\Temp\\1201310141513013990.exe  
 \\Temp\\svchost.exe



POST /RPC2 HTTP/1.1  
POST /post HTTP/1.1

# Money Laundering Intelligence

## Reasons for Suspicion

Fraud

Money Laundering

Corruption

Sanctions

Drug / Weapon / Human Trafficking

Tax Evasion

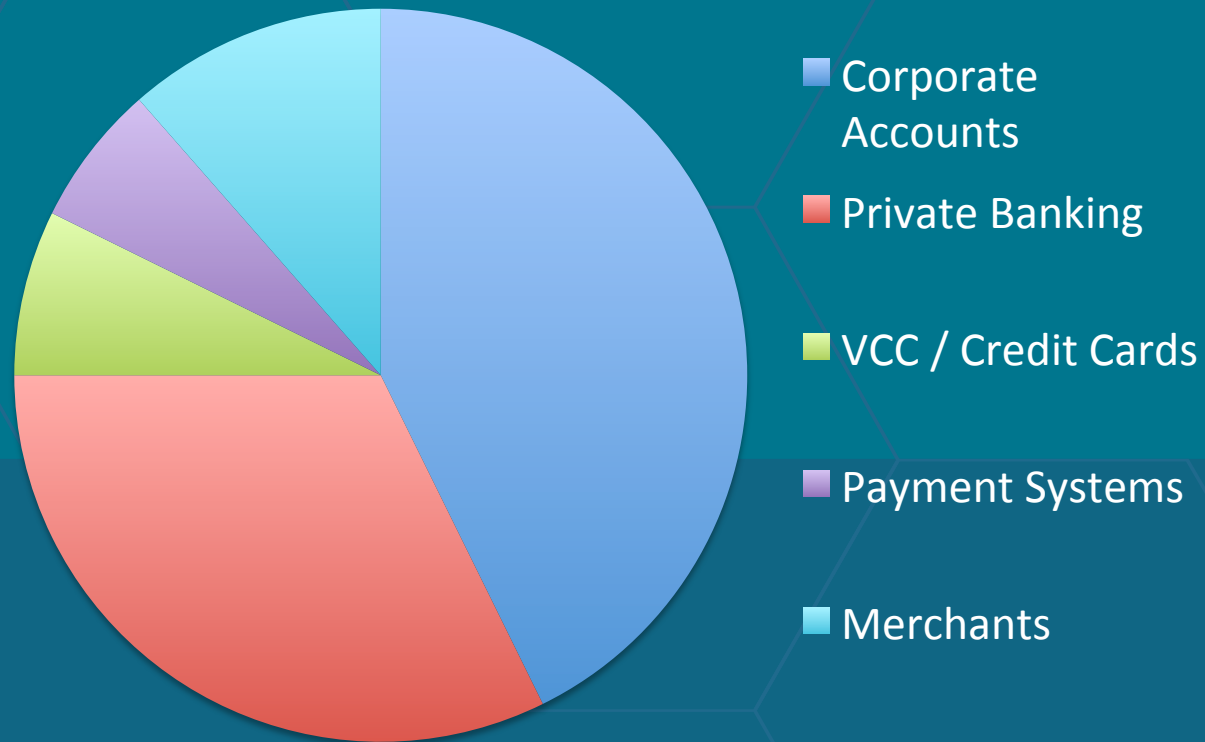
Declined Business

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

SUBSCRIBE (Only For Banks & LEA)

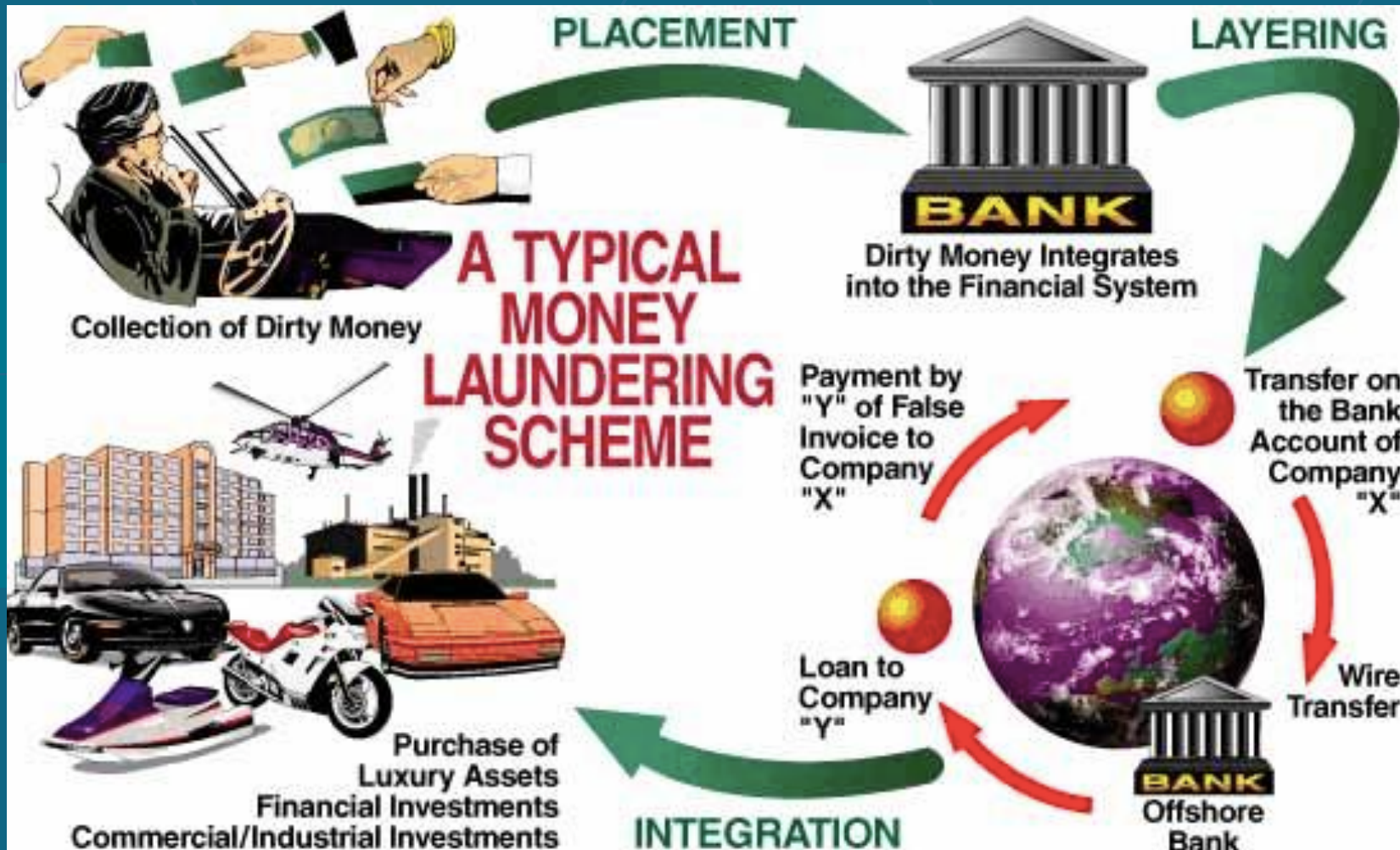
The screenshot shows the IntelCrawler web interface. At the top, there is a navigation menu with links for Company, Products, Subscriptions, Services, Analytics, and Contact Us. Below the navigation is a search bar with the text "Enter your query..." and a "WHOIS" button. The main content area is titled "Choose Location" and features a map of Europe with several red location pins. Below the map is a table with the following data:

#	Date	Name	Geography	Type
1	27.03.2014 12:25	Microsoft Windows User Account Control Bypass (0-day) - Windows 7/8	Hong Kong 🇸🇬	APT
2	27.03.2014 12:11	New WinRAR File extension spoofing vulnerability targets Fortune 500 and Aerospace companies	Izmir, Turkey 🇹🇷	APT
3	03.02.2014 13:40	Yahoo Email Accounts Were Compromised	Yahoo! Building D, 1st Avenue, Sunnyvale, CA 🇺🇸	Data Theft



STYX  
XML  
JSON

# Money Laundering – Typical Scheme



# Money Laundering – Non-Typical Scheme

论坛首页 < 交易区 < 实物交易

FAQ 注册 登录

## 出售匿名银行帐户+卡

POSTREPLY \* 查找这个主题..... 搜索 10 篇帖子 • 分页: 1 / 1

**yinka**  
帖子: 6  
注册: 周四 5月 14, 2015 2:16 pm

### 出售匿名银行帐户+卡








由 **yinka** » 周四 5月 14, 2015 2:27 pm

大家好，鄙人经营国际汇款公司，真诚为大家提供金融服务。  
银行开户实名制给很多人生活带来不便，现出售储蓄卡+身份证+网银U盾+手机卡+开户证明。  
用途: 避免自己的身份暴露，可用于转账、汇款、洗钱、送礼、逃税、贿赂，隐蔽性强，非常实用。  
如有需要请加QQ:447795958私聊，QQ用小号，安全没有问题。

另提供地下钱庄服务，双向汇款，汇款到国外，或从国外汇到国内都无问题，信用至上，为收汇双方保密，在您需要转移大量资金时是不二选择。详情请私聊

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

# Money Laundering – Non-Typical Scheme

Оплаченная реклама		
	<p><b>Обнал-сервис от Mavr009</b> 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.</p>  	 <b>Примем заливов на Китай,</b> от <a href="#">Mavr009</a>
	<p><b>Интернет-магазин дебетовых карт - debet.cc</b> On-line сервис по продаже дебетовых карт - 24/7. QIWI/Яндекс кошельки. Оперативная доставка.</p>	 <b>Дебетовые карты</b> от <a href="#">LaCoka</a>
	<p><b>[РФ] Обнал-сервис QIWI, WebMoney, Yandex от QvP,</b> (просматривают: 1) Налим QIWI, WM, ЯД, Принимаю заливов на МТС,Билайн, Мегафон. Всегда в наличие QIWI карты. ДЕПОЗИТ 5000 \$</p>	 <b>Обнал-сервис QIWI, WM, ЯД</b> от <a href="#">QvP</a>

*15/25% - big corporate accounts*

*Also Individuals. Will help you to transfer or hide your money*



# Money Laundering – Non-Typical Scheme



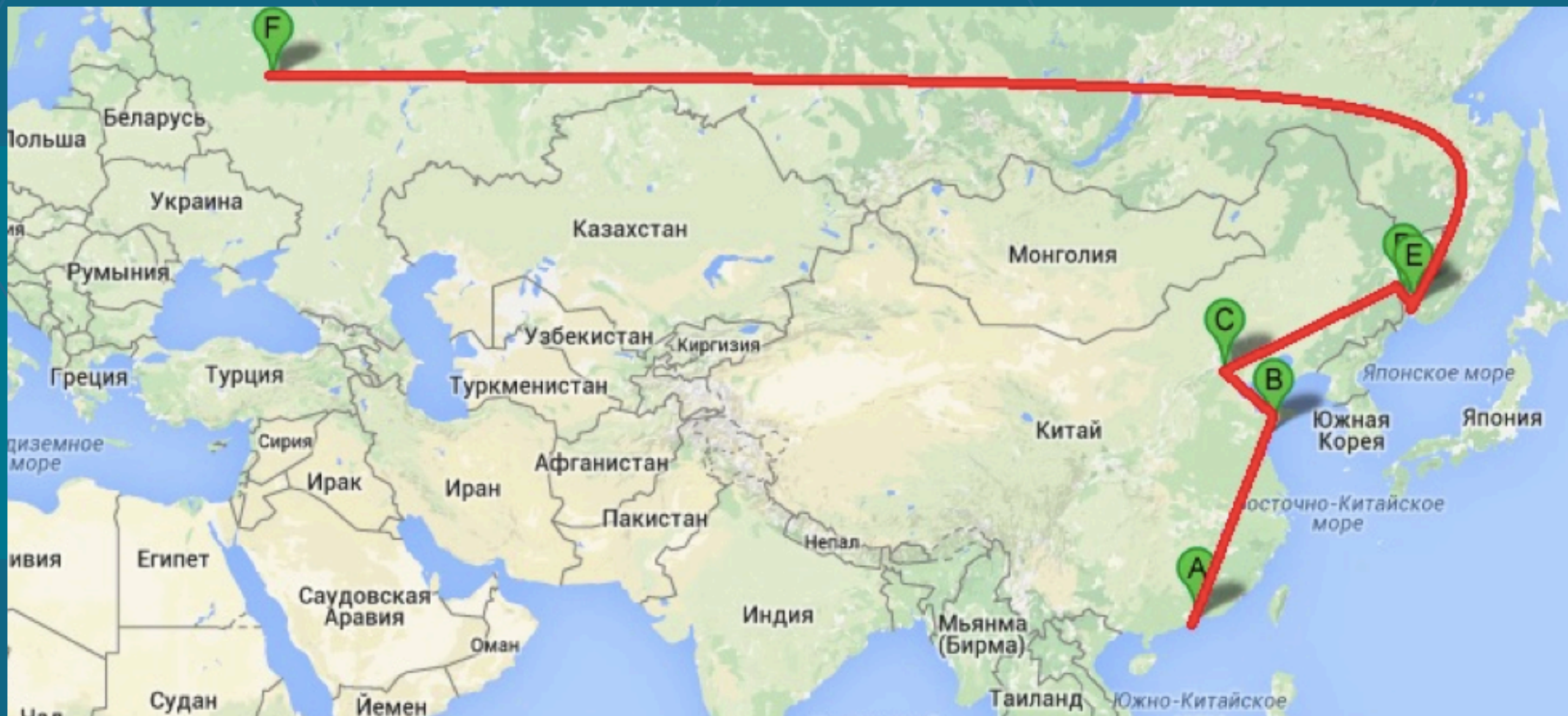
# Money Laundering – Non-Typical Scheme



*Sea-Based Logistics, Warehouse*



# Money Laundering – Non-Typical Scheme



*“Asian” Path*



# QUESTIONS

[ak@intelcrawler.com](mailto:ak@intelcrawler.com)  
[www.intelcrawler.com](http://www.intelcrawler.com)