



# КазХакСтан

Алматы  
5 ОКТЯБРЯ  
2018

Ежегодная практическая конференция  
по вопросам информационной безопасности

conference



# Остаться

# невидимкой

Andrei Masalovich

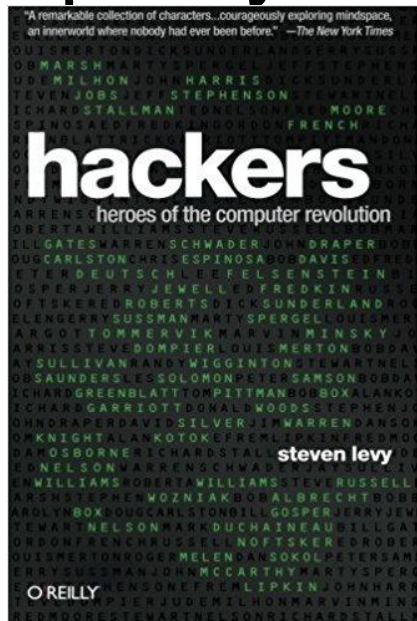
Live smart, live longer

[am@avl.team](mailto:am@avl.team)

# Hackers. Evolution

## Хакеры. Эволюция

Романтики  
Преступники



Heroes



Cyber Crime

Спецназ  
информационной  
ВОЙНЫ



Cyber Army

# Bachosens: Highly-skilled petty cyber criminal with lofty ambitions targeting large organizations



Rdata results for ANY/2a01:4f8:120:8355::

Returned 19 RRs in 0.11 seconds.

akb.md.	AAAA	2a01:4f8:120:8355::
www.akb.md.	AAAA	2a01:4f8:120:8355::
static.akb.md.	AAAA	2a01:4f8:120:8355::
akkumulator.md.	AAAA	2a01:4f8:120:8355::
www.akkumulator.md.	AAAA	2a01:4f8:120:8355::
xxhost.ru.	AAAA	2a01:4f8:120:8355::
www.xxhost.ru.	AAAA	2a01:4f8:120:8355::
ddns.eu.	AAAA	2a01:4f8:120:8355::
bbxapp.com.	AAAA	2a01:4f8:120:8355::
www.bbxapp.com.	AAAA	2a01:4f8:120:8355::
ip2name.com.	AAAA	2a01:4f8:120:8355::
ip2name.net.	AAAA	2a01:4f8:120:8355::
xn--11aj.net.	AAAA	2a01:4f8:120:8355::
lastmd.org.	AAAA	2a01:4f8:120:8355::
www.lastmd.org.	AAAA	2a01:4f8:120:8355::
oyy.name.	AAAA	2a01:4f8:120:8355::
mail.oyy.name.	AAAA	2a01:4f8:120:8355::
noip.name.	AAAA	2a01:4f8:120:8355::
xn--11aj.name.	AAAA	2a01:4f8:120:8355::

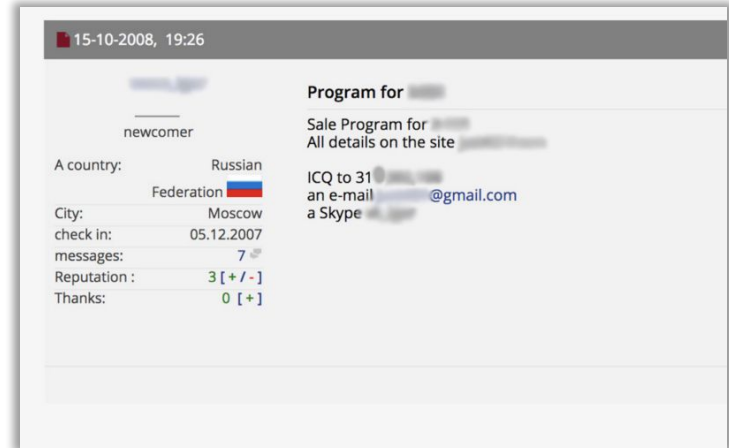


- Сложное заказное malware
- Целевой фишинг
- Эфемерные AES-ключи
- IPv6, DGA, DDNS
- Связь через DNS, ICMP

- Исходный код на VirusTotal
- Распространяется с играми
- Кейлоггер без обфускации
- Менее 20 доменов в год

# Internet Intelligence

## Если использовать методы интернет-разведки...



- Игорь С\*\*\*\*\*
- Тирасполь
- Телефон: \* \*\*\* \*\* \* \*\* \*
- E-mail: \*\*\*\*\*@gmail.com

# Мы – дети в мире умных вещей

## Военные – дети с гранатой



- Высокоточное оружие
- Умное оружие
- Автономное летальное оружие
- Сетецентрическая война

# Honeypots

A **honeypot** is a decoy computer system for trapping hackers or tracking unconventional or new hacking methods.



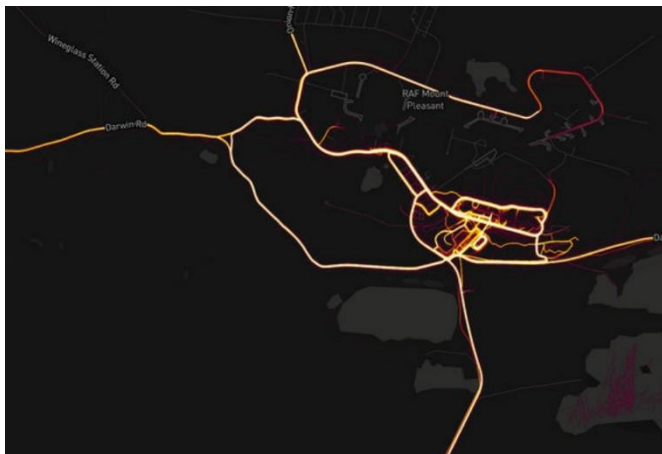
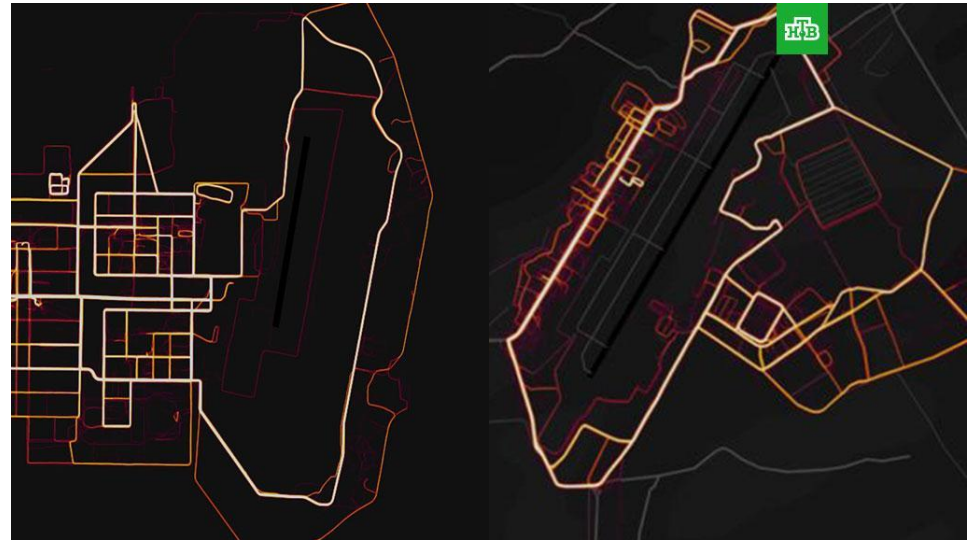
Кто первым клюнул на приманку?

- Министерство обороны одной из стран СНГ
- Антивирусная компания
- Спецслужба одной из стран СНГ

# Fitness app Strava lights up staff at military bases

## Фитнес-трекер Strava

выдал расположение военных баз США

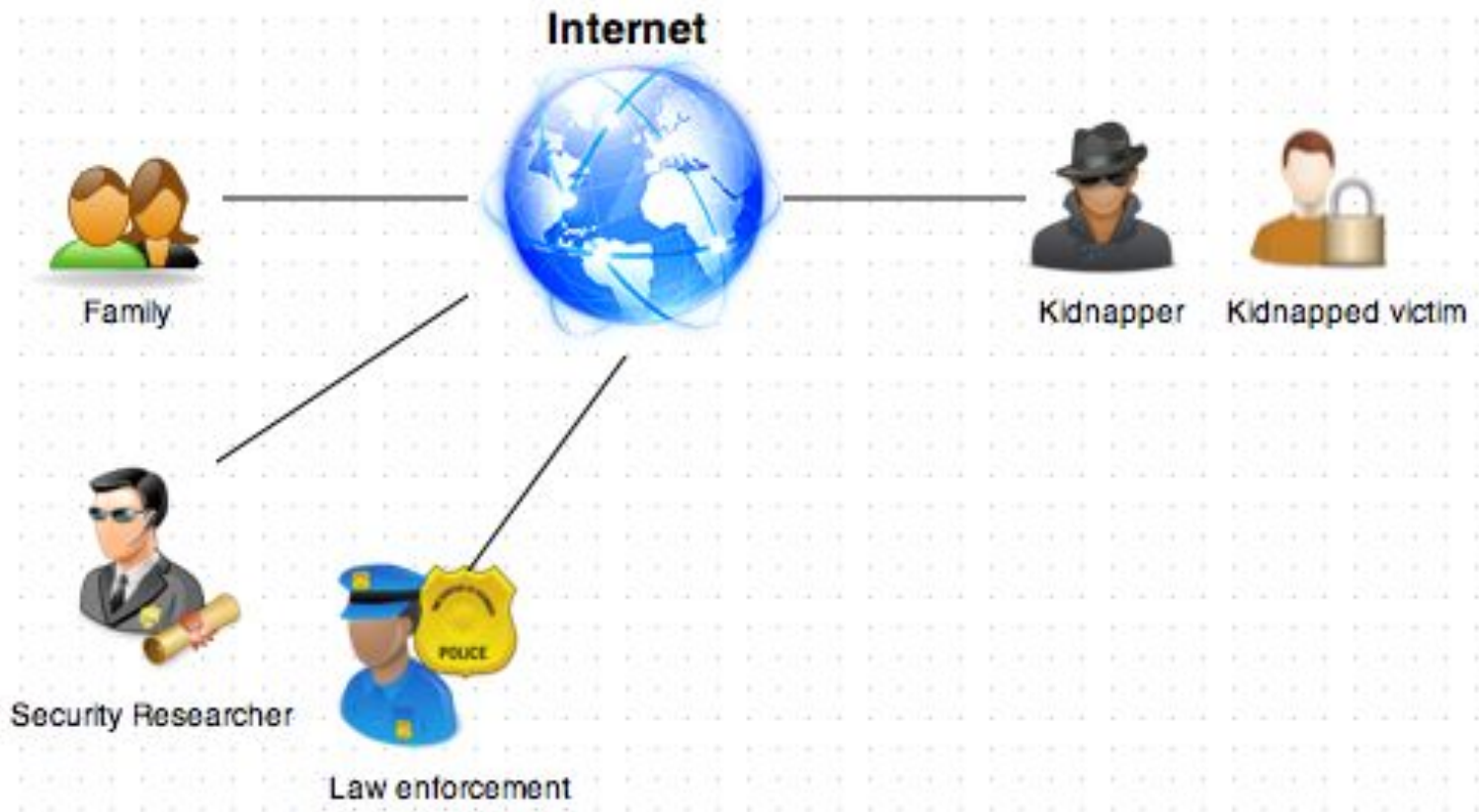


*Working off the IP address, U.S. investigators identified Guccifer 2.0...*  
Скрывайте IP. Всегда.





# «Адресные ловушки»



# Что значит: «Не оставлять следов?»

- Безуликовость
- Недостаточность доказательной базы
- Скрытие присутствия
- Маскировка
- Размывание цели
- Ложный след
- ...
- Легенда прикрытия

# Digital Forensics

**Digital forensics** (sometimes known as **digital forensic science**) is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime.

**Форензика** (компьютерная криминалистика, расследование киберпреступлений) — прикладная наука о раскрытии преступлений, связанных с компьютерной информацией, об исследовании цифровых доказательств, методах поиска, получения и закрепления таких доказательств



Source: Rocky Mountain

# Прячем данные

- Безвозвратное уничтожение
- Невидимые разделы
- TrueCrypt
- Криптоконтейнеры
- Стеганография
- «Двойное дно»

# Digital Footprint Наш цифровой след



Новости



Интернет



Бизнес



Финансы



Недвижимость



Биография



Документы



Семья



Аккаунты



Привычки



Местоположение



Гаджеты



Социальные сети



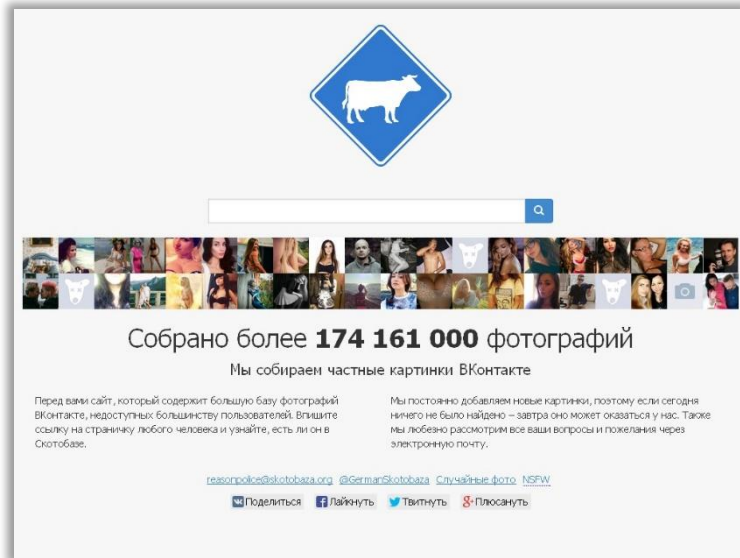
Проблемы с законом



# Using OSINT...



# Источник утечек личной информации – базы удаленных страниц в соцсетях



Собрано более **174 161 000** фотографий

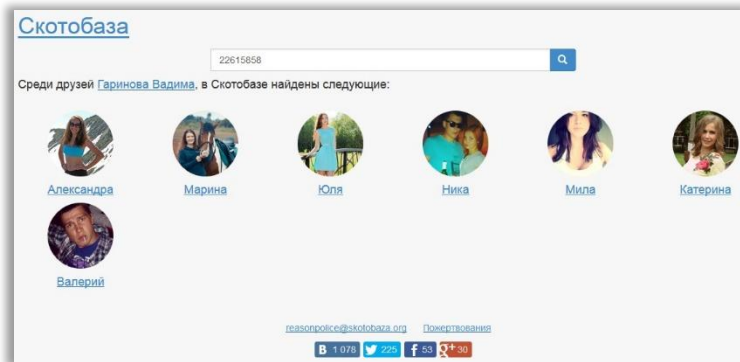
Мы собираем частные картинки ВКонтакте

Перед вами сайт, который содержит большую базу фотографий ВКонтакте, недоступных большинству пользователей. Введите ссылку на страничку любого человека и узнайте, есть ли он в Скотобаза.

Мы постоянно добавляем новые картинки, поэтому если сегодня ничего не было найдено – завтра оно может оказаться у нас. Также мы любим рассматривать все ваши вопросы и пожелания через электронную почту.

[reasonpolice@skotobaza.org](mailto:reasonpolice@skotobaza.org) @GermangSkotobaza Случайные фото NSFW


Поделиться Лайкнуть Твитнуть Плюснуть





Скотобаза


22615856


Среди друзей Гарина Вадима, в Скотобаза найдены следующие:


 **Александра**


 **Марина**

 **Юля**

 **Ника**

 **Мила**

 **Катерина**

 **Валерий**

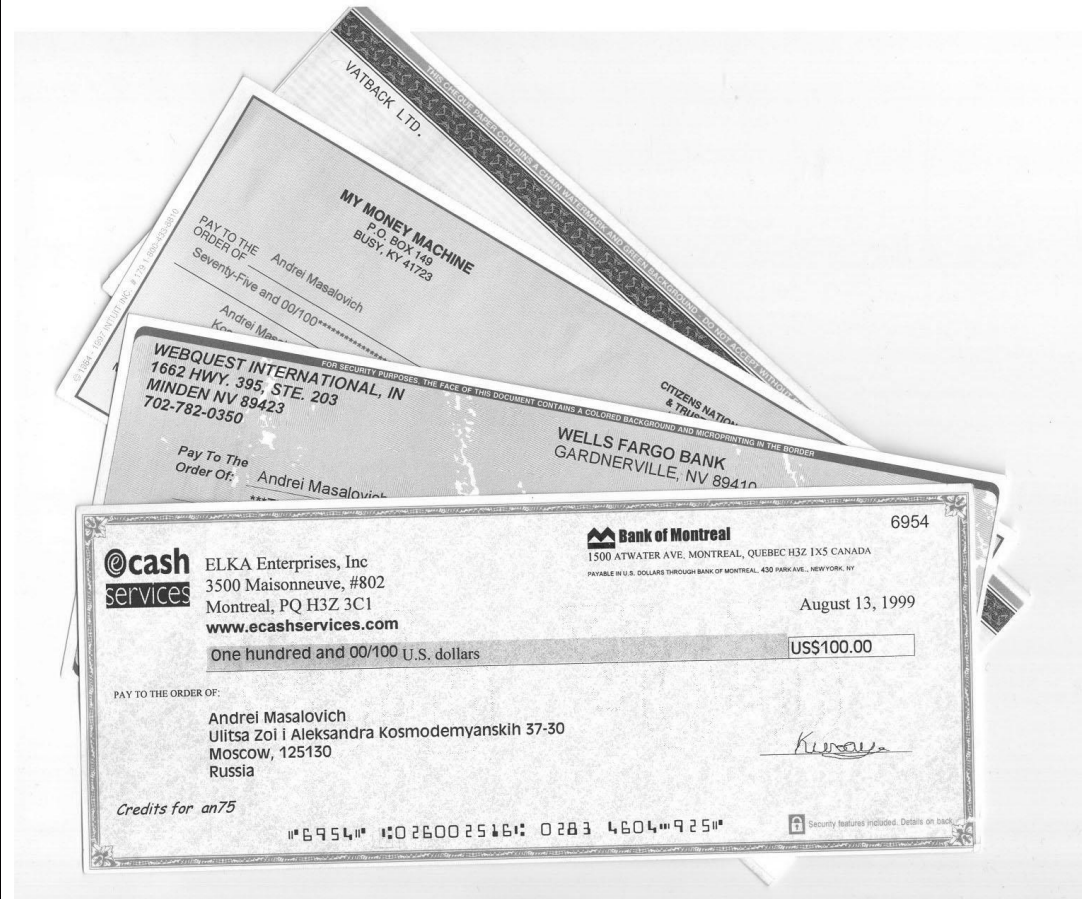
[reasonpolice@skotobaza.org](mailto:reasonpolice@skotobaza.org) [Помощь](#)

1 078 226 53 430





# The Hacker



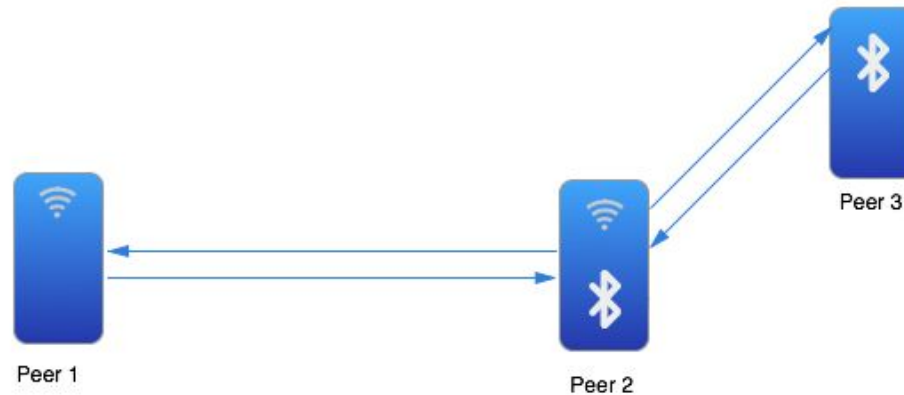
# “Skin”. Кража цифровой личности



Улов на  
[uk.com/docs](http://uk.com/docs)

# Выйти из-под видеокамер

Multipeer connectivity framework в iOS7



# APT – Advanced Persistent Threat



- An **advanced persistent threat (APT)** is a set of stealthy and continuous computer hacking processes, often orchestrated by a person or persons targeting a specific entity.
- АРТ ( «развитая устойчивая угроза»; также целевая кибератака) — противник, обладающий современным уровнем специальных знаний и значительными ресурсами, которые позволяют ему создавать возможности для достижения целей посредством различных векторов нападения

# Advanced Persistent Threat Groups



## **APT37 (Reaper)**

North Korea

Target sectors: Primarily South Korea – though also Japan, Vietnam and the Middle East

– in various industry verticals, including chemicals, electronics, manufacturing, aerospace, automotive, and healthcare

## **APT28 Tsar Team**

Suspected attribution: Russian government

Target sectors: The Caucasus, particularly Georgia, eastern European countries and militaries, North Atlantic Treaty Organization (NATO) and other European security organizations and defense firms

Associated malware: CHOPSTICK, SOURFACE



## **APT33**

Suspected attribution: Iran  
Target sectors: Aerospace, energy. APT33 has targeted organizations, spanning multiple industries, headquartered in the U.S., Saudi Arabia and South Korea.  
Associated malware: SHAPESHIFT, DROPSHOT, TURNEDUP, NANOCORE, NETWIRE, ALFA Shell

# Using Google Translate

## WannaCry:

- Требования о выкупе были написаны на 28 языках
- На трех языках без перевода
- Родной – китайский, второй - английский



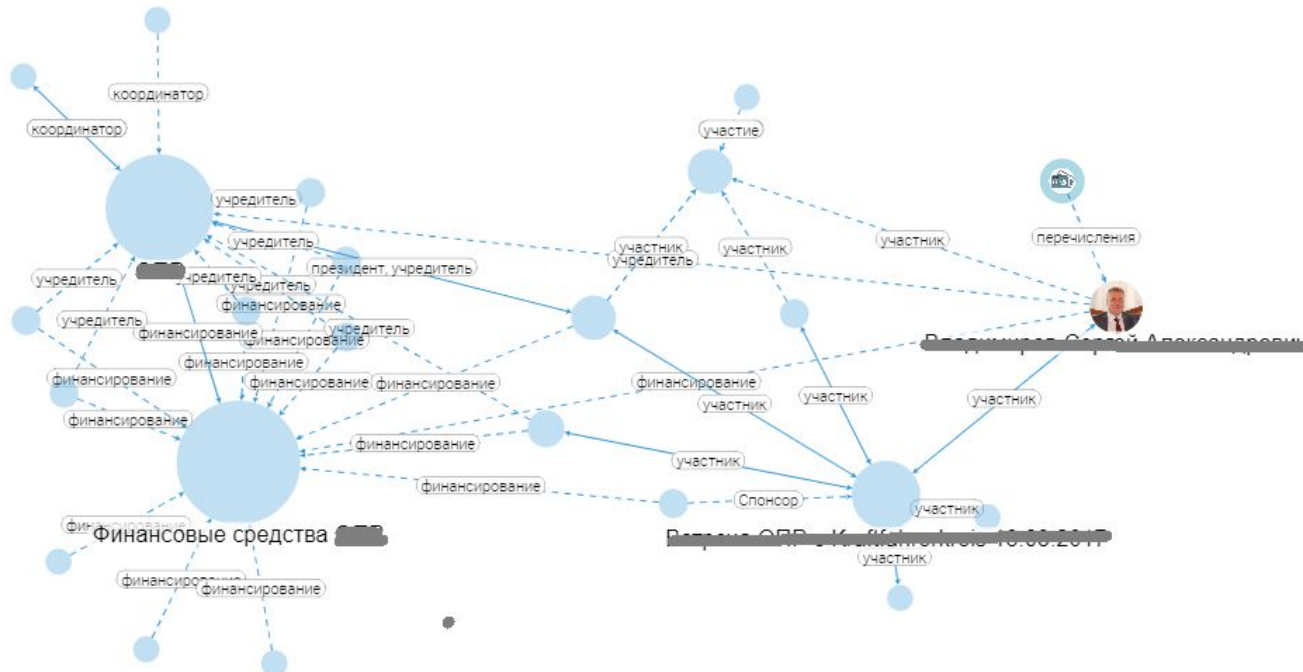
# Анализ графа связей

Счет № 6761-0600-0104  
5200-07  
Банковский счёт

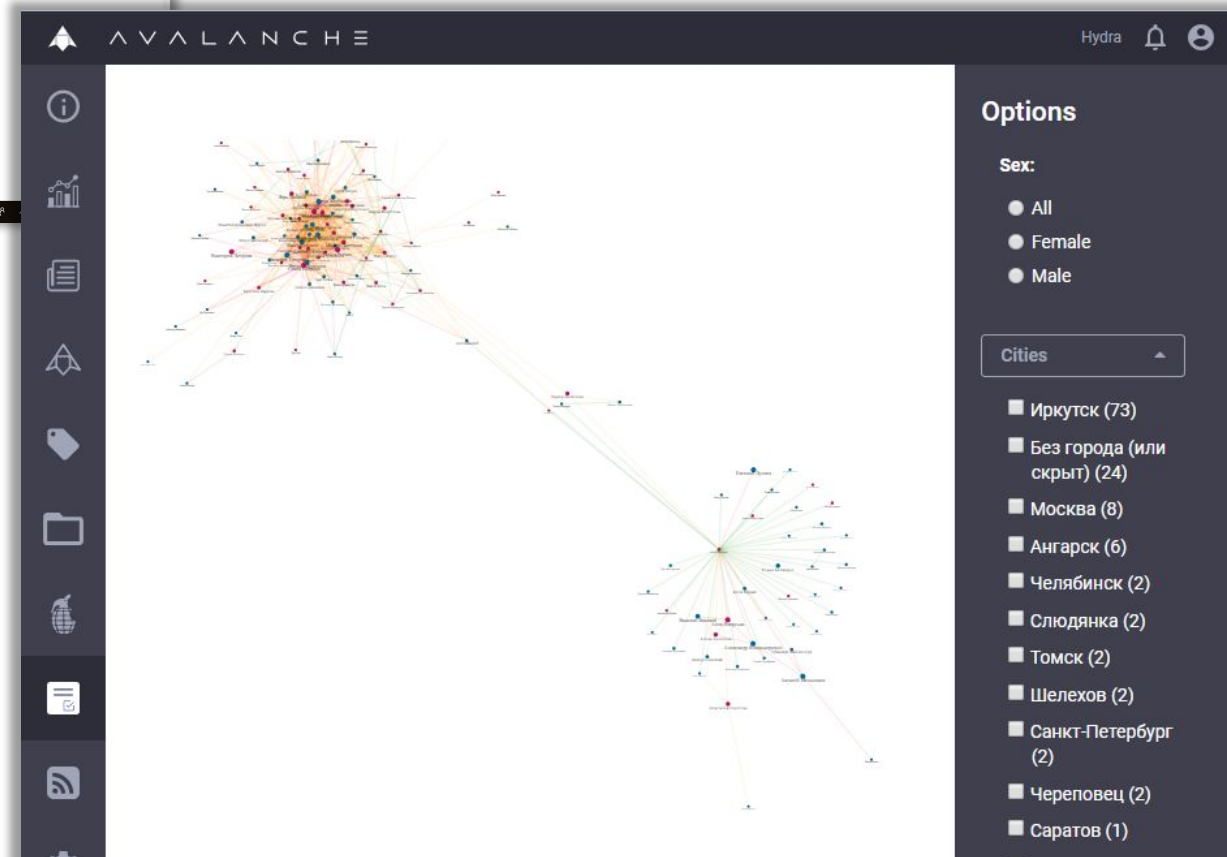
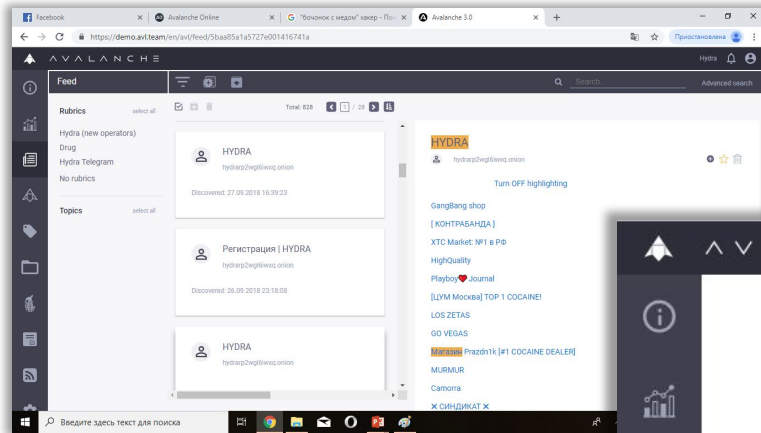
Входящие связи 0  
Исходящие связи 1

Таблица связей

Перейти к -



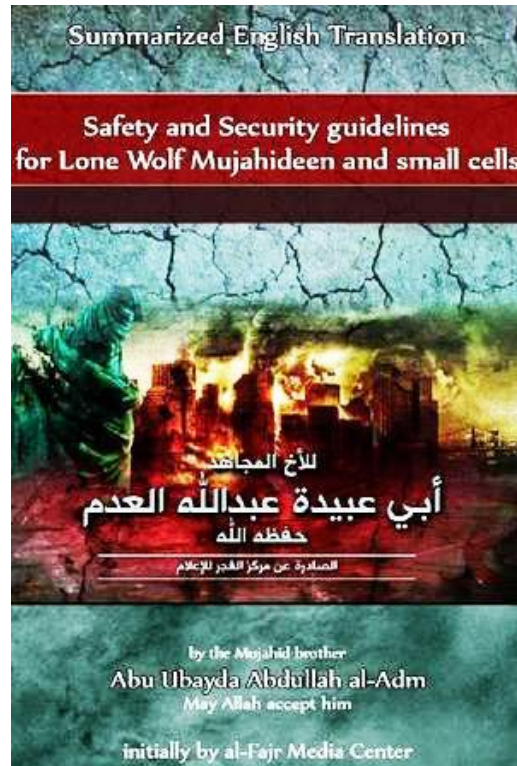
# HYDRA: Outside TOR







# Пример работы в «сером» интернете: Методички террористов по бескомпроматной работе

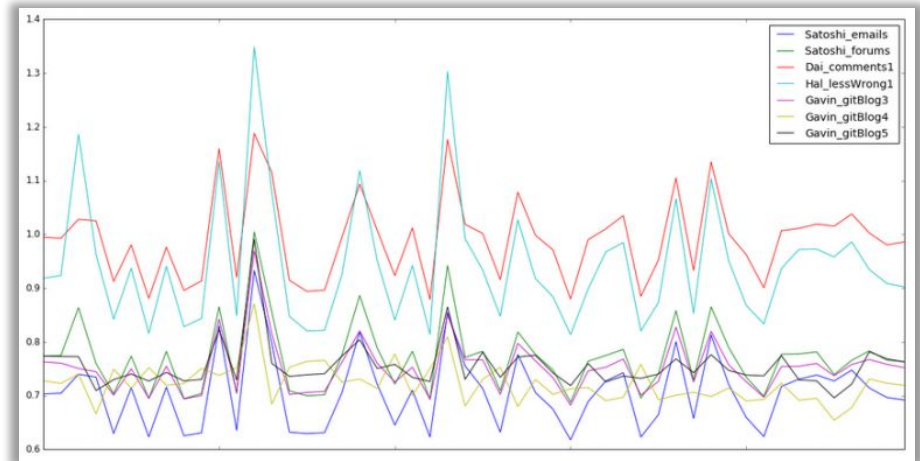


# Stylometry

## Identify Satoshi Nakamoto



- **Stylometry** is the application of the study of linguistic style, usually to written language. Stylometry is often used to attribute authorship to anonymous or disputed documents



Zy Crypto

# ЧТО ДЕЛАТЬ?

- Люди
- Процессы
- Технологии
- Спецназ информационной войны
- Кибероружие

# ЛЮДИ

- Китай открывает 5 учебных центров по кибербезопасности по 10 000 специалистов
- Сингапур оценивает свои потребности в специалистах по ИБ в 15 000 человек



Первый шаг – ЭКСПРЕСС-КУРСЫ

- Для руководителей

- Для специалистов

- Для пользователей

Основам безопасности можно  
научить  
за один день

# ПРОЦЕССЫ

## Контроль обстановки в киберпространстве

Главные новости

Ситуация в стране

Военные конфл...

Чрезвычайные ...

Минобороны

Сопредельные с...

### Киберпространство



#### Сирийские хакеры взломали сайт Forbes

Хакеры из группировки «Сирийской электронной армии» (SEA) взломали сайт американского журнала Forbes и ряд принадлежащих изданию и его сотрудникам аккаунтов в сети микроблога Twitter.

Добавлено 14.02.2014 16:28

[www.vz.ru](http://www.vz.ru)



#### В DARPA разрабатывается система использования смартфонов на поле боя

В управлении перспективных исследовательских программ министерства обороны США (DARPA) пришли к выводу, что привычка постоянно сверяться с мобильным помощником может стать на поле боя преимуществом для американских войск. В среду появились сообщения о начале разработок системы связи, которая бы

Добавлено 14.02.2014 12:00

[www.ci2b.info](http://www.ci2b.info)



#### Белый дом представил госучреждениям США список рекомендаций по защите от

Администрация Белого дома сообщила о выпуске списка рекомендаций для защиты инфраструктуры частных компаний и госучреждений от киберугроз. Президент США Барак Обама приветствовал это нововведение. Около года назад глава государства в своем выступлении, посвященном положению деп в стране,

Добавлено 13.02.2014 14:48

[itar-tass.com](http://itar-tass.com)



#### Администрация США представила новую концепцию кибербезопасности

Президент Обама назвал эту инициативу поворотным моментом в обеспечении защиты от хакерских атак

Добавлено 13.02.2014 14:43

[www.golos-ameriki.ru](http://www.golos-ameriki.ru)

### Во Франции сменился начальник генштаба

Глава генштаба ВС Франции адмирал Эдуар Гийо официально ушел в отставку. В честь него на площади Инвалидов в Париже прошла торжественная церемония, во время которой президент республики Франсуа Олланд лично поблагодарил Гийо за заслуги перед Фра...

AVANCE

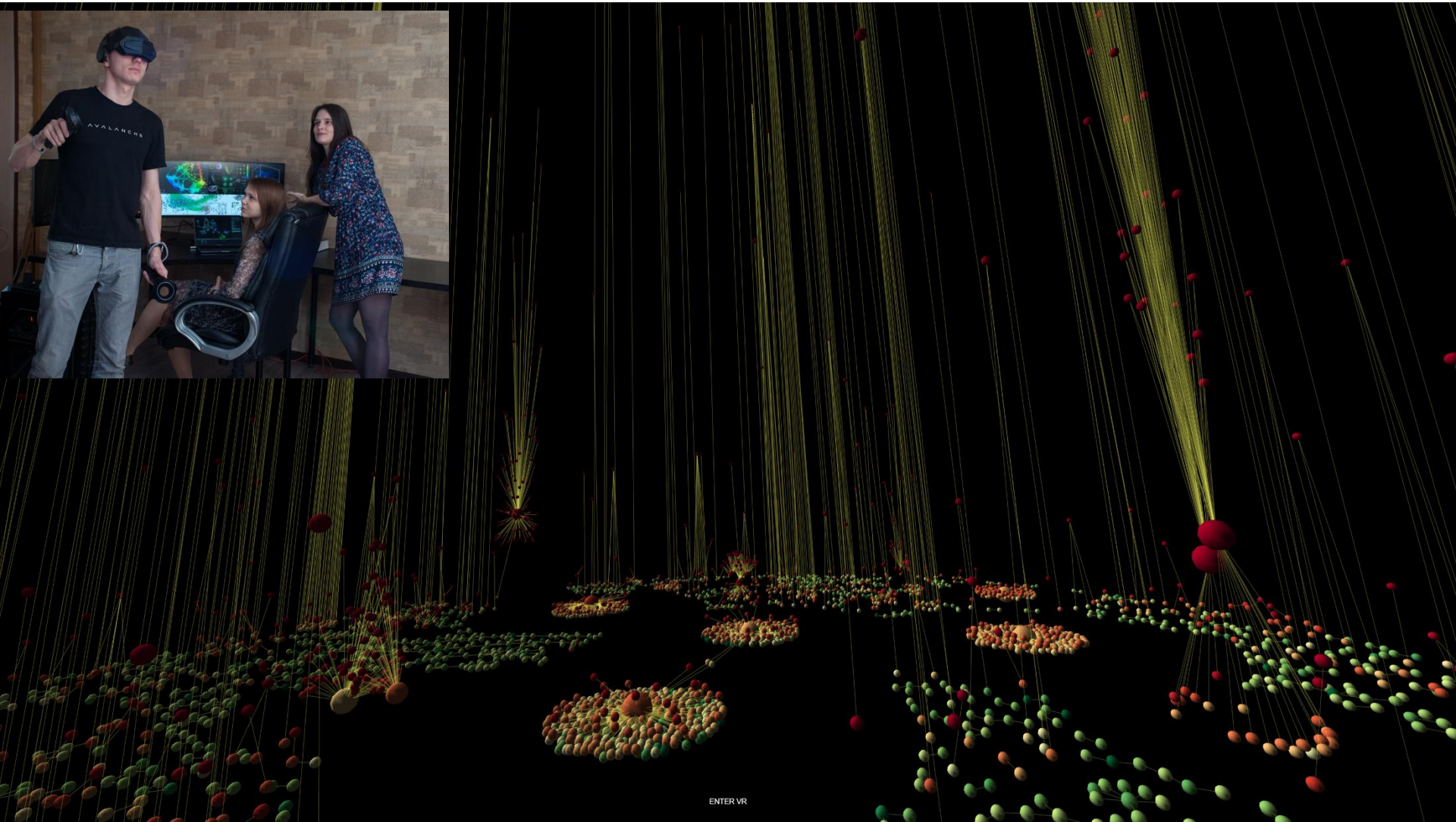
# ТЕХНОЛОГИИ

- Системы контроля оперативной обстановки
- Системы раннего предупреждения
- Аналитическая обработка больших данных
- Ситуационные центры нового поколения



Первый шаг – системы контроля оперативной обстановки

# Step to the Web



ENTER VR

AVALANCHE



# Аналитические технологии на службе разведывательного сообщества США

Infrastructure				Analytics				Applications			
<b>Hadoop On-Premise</b> cloudera, Hortonworks, MAPR, Pivotal, IBM InfoSphere, splice, bluedata, jethro	<b>Hadoop in the Cloud</b> Amazon, Microsoft Azure, Google Cloud Platform, IBM InfoSphere, CAZENA, altiscale, Doble, xplenty	<b>Spark</b> databricks, GridGain, TACHYON NEXUS	<b>Cluster Services</b> Amazon Web Services, Kubernetes, Docker, Mesosphere, Core OS, Pepperdata, StackIQ	<b>Analyst Platforms</b> Palantir, AYASDI, Quid, enigma, Digital Reasoning, ORBITAL INSIGHT	<b>Analytics Platforms</b> Microsoft, guAVUS, Datameer, interana	<b>Data Science Platforms</b> context relevant, DataRobot, Alpine, MODE, ADATA, dataiku, tonian, DOMINO, sense, what, ALGORITHMIA	<b>Visualization</b> Tableau, Roambi, GOMDATA, Oliko, CHARTIO	<b>Sales &amp; Marketing</b> RADIUS, Gainsight, bloomreach, Zeta, blueyonder, livefyre, Lattice, SAILTHRU, kahuna, persado, infer, sense, AVISO, ACTIONIQ, QUANTIFIND, JEN GAGIO	<b>Customer Service</b> MEDALLIA, ATTENSTY, CLARABRIDGE, STELLA Service, NGDATA, Preact, DigitalGenius, Wuseio, appur, fuse:machines	<b>Human Capital</b> gild, Connectifier, textic, entelo, hiQ	<b>Legal</b> RAVEL, JUDICATA, Everlaw, Brevia, PREMIONATION
<b>NoSQL Databases</b> Amazon DynamoDB, Google Cloud Platform, Microsoft Azure, ORACLE, mongoDB, DATASTAX, Couchbase, SEEROSPIKE, SequoiaDB, redislabs, influxdata	<b>NewSQL Databases</b> SAP HANA, Clustrix, Pivotal, memsql, paradigm4, NUODB, MariaDB, VOLTD, CIUTODATA, deepdb, Trafalgar, Cockroach LABS	<b>BI Platforms</b> Power BI, Amazon Web Services, Domo, Wave Analytics, GoodData, birst, platforma, lobker, atscale, MICROSOFT	<b>Statistical Computing</b> SAS, SPSS, MATLAB	<b>Log Analytics</b> splunk, sumologic, kibana, CLOUD PHYSICS, loggly	<b>Social Analytics</b> NETBASE, DATASIFT, tracx, bitly, synthetio, bottlen, simple reach	<b>Ad Optimization</b> MediaMath, Integral Ad Science, OpenX, rocketfuel, Adgorithms, theTradeDesk, Livelihood, distillery, DataXu, Cppier, TAPAD	<b>Security</b> CYCLANCE, CounterTack, cybereason, ThreatMetrix, AREA 1 SECURITY, SentinelOne, Recorded Future, Guardian Analytics, Fortscale, sift science, Kaybase, feedzai, SICNIFYD	<b>Vertical AI Applications</b> Facebook, Clara, KASIST, lumina			
<b>Graph Databases</b> neo4j, OrientDB, InfiniteGraph	<b>MPP Databases</b> TERADATA, VERTICA, NETEZZA, Kognitio, dremio	<b>Cloud EDW</b> Amazon Web Services, Google Cloud Platform, Microsoft Azure, Pivotal, snowflake, WATERLINE, Infoworks	<b>Data Transformation</b> Alteryx, TRIFACTA, MuleSoft, PAXATA, StreamSets, Alation	<b>Data Integration</b> Informatica, MuleSoft, snapLogic, BedrockData	<b>Real-Time</b> Amazon Web Services, METAMARKETS, confluent, DATATOURNEY, dataArtisans	<b>Machine Learning</b> Azure Machine Learning, H2O, SKYTREE, rapidminer, DATAWIP, deepsense, VISENZE, predictionIO, slowfish	<b>Speech &amp; NLP</b> NarrativeScience, apl.ai, NUANCE, Grindspace, semantic machines, cortico, MindMeid, IDIBON, YSCOPE	<b>Horizontal AI</b> IBM Watson, Cortana, sentient, viv, VIVANT, Numenta, MetaMind, clarifai	<b>Publisher Tools</b> Outbrain, mixpanel, Chartbeat, yieldbot, Yieldmo	<b>Govt/ Regulation</b> Socrata, OPENGOV, EN FiscalNote, PREPOL, mark43, OpenDataSoft	<b>Finance</b> Affirm, LendingClub, OnDeck, Kreditech, finance, LendUp, Kabbage, tdemark, FairFi, INSIKT, UORA, Dataminr, Lendio, KENSHC, AIIDYA, iSENTIUM, Quantopian, sentiment
<b>Management / Monitoring</b> New Relic, illumio, APPDYNAMICS, Amazon Web Services, actifio, Numerify, splunk, DATA DOG, TROCAN, Anodot	<b>Security</b> TANIUM, illumio, CODE42, DataGravity, CyberCloud, VECTRA, sqrrl, BlueTalon	<b>Storage</b> Amazon Web Services, Google Cloud Platform, Microsoft Azure, panass, nimblestorage, Qumulo	<b>App Dev</b> Apigee, CASK, Typesafe, CONCURRENT	<b>Crowd-sourcing</b> Amazon Mechanical Turk, CrowdFlower, WorkFusion	<b>Search</b> HP, ELASTIC, ORACLE, INFINEA, Lucidworks, MAANA, swiftype, Algolia, SINEQUA	<b>Data Services</b> LIQ, OPERA, Mu Sigma, DATASOURCE, DATA VALUES, DataKind	<b>For Business Analysts</b> ClearStory, CIRRO, import IO	<b>SMB / Commerce</b> Google Analytics, OrigamiLogic, AMPLITUDE, RJMetrics, BLUECORE, sumAll, granify, Airtable, retention, custora	<b>Education/ Learning</b> KNEWTON, Clever, Declara, PANORAMA, knowTe	<b>Life Sciences</b> 23andMe, Counsyl, RECOMBINE, KYRUS, FLATIRON, zymogen, HealthTap, METABIOTA, ZEPHYR HEALTH, OVI, Gingerio, transcriptic, Glow, entilic, AICure, Atomwise	<b>Industries</b> OPOWER, eHarmony, RetailNext, duetto, STITCH FIX, WorkFusion, BLUE RIVER, TACHYUS, SwiftKey, Seeq, FarmLogs, HowGood, collect, STATMUSE, BOEVEER
<b>Cross-Infrastructure/Analytics</b> Amazon Web Services, Google, Microsoft, IBM, SAP, SAS, HP, Autodesk, vmware, talend, TIBCO, TERADATA, ORACLE, NetApp											
<b>Framework</b> Hadoop, HADOOP, YARN, Spark, MESOS, TEZ, Flink, CDAP	<b>Query / Data Flow</b> SLAMDATA, DRILL, Google Cloud Dataflow	<b>Data Access</b> HBASE, accumulo, mongoDB, cassandra, kafka, CouchDB, riak, OPENTSDB, nifi	<b>Coordination</b> talend, Apache Ambari	<b>Real-Time</b> STORM, Spark, APEX, TACHYON, druid	<b>Stat Tools</b> Scala, NumPy, SciPy	<b>Machine Learning</b> mlilib, Aerolve, Apache, SINGA, MADlib, Caffe, CNTK, TensorFlow, WEKA, FeatureFu, DIMSUM, VELES, jupyter, DL4J	<b>Search</b> elasticsearch, Solr, Lucene	<b>Security</b> Apache Ranger, Visualization, Zepalin			
<b>Data Sources &amp; APIs</b>											
<b>Health</b> Apple, JAWBONE, GARMIN, practicefusion, fitbit, Withings, VALIDIC, relatmo, kinsa, Human API	<b>IOT</b> UPTAKE, ThingWorx, helium, samsara	<b>Financial &amp; Economic Data</b> Bloomberg, DOW JONES, YDLEE, PREMISE, S&P CAPITAL IQ, Quandl, xignite, CB INSIGHTS, mattermark, estimize, FLAID	<b>Air / Space / Sea</b> PLANET LABS, WINDWARD, spire, CRUISE, SKYCATCH, Airware, DroneDeploy	<b>Location/People/Entities</b> GARMIN, foursquare, InsideView, esri, STREETLINE, CARTOBB, factual, PlaceIQ, Crismon Hexagon, placemeter, BASIS, Sense	<b>Other</b> qualtrics, panjiva, DATA.GOV	<b>Incubators &amp; Schools</b> GA, DataCamp, INSIGHT, DataElite, METIS, The Data Incubator					

# Дополнительная информация



**Forbes** 22.04.2018 10:51 Ресурсы | Везде

Разведка сетью: как система Avalanche помогает спецслужбам и бизнесу

Подполковник спецслужб в отставке Андрей Масалович создал программу Avalanche для борьбы с сетевыми угрозами. За что власти и корпорации ценят разработку?

«Русские, интервь» — десктоп-версия в массах выискивает двери торговых центров «Барнесс» и «Биржевик». Их разработал один из самых ярких и успешных людей бизнеса и науки. Предприниматель изобрел, который позволил ему увидеть до сих пор закрытый код, который не смел, пока информация о нем была. «За три часа до начала беспорядков у меня в ноутбуке зашифрованная информация — список телефонов», — вспоминает со слов Андрей Масалович, президент холдинга «Информ» и разработчик новаторской аналитической системы Avalanche. — Мы заметили, что в группе «Суровое Барнесс» и оспаривать в на ресурсе «Ф-Руссия» начались прямые угрозы жизни протестов.

После событий в Барнессе система раннего предупреждения на базе Avalanche «Лавина Пульс» — использовалась в МВД, в управлении авиационной разведкой информации (УВРИ). От государства не отстал и бизнес — банки и

ПРОВЕРЬТЕ, ЕСТЬ ЛИ У ВАС ПРИКЛЮЧЕН

Журнал Forbes

Оборвать подписку на журнал

КОГДА РОЖДАЮТСЯ УДОБНОСТИ НЕ СА РИДЕТ

200 БОГАТЕЙШИХ БИЗНЕСМЕНОВ РОССИИ

# Спасибо за внимание 😊

## Questions?



Masalovich Andrei  
Масалович Андрей  
Игоревич  
Специалист по связям с  
реальностью  
+7 (964) 577-2012  
[am@avl.team](mailto:am@avl.team)

[iam.ru/tipaguru.htm](http://iam.ru/tipaguru.htm)