ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Введение в конкурентную разведку

Основные методы

Авдюнин Максим

«Перспективный мониторинг»

Перспективный мониторинг

Мониторинг инцидентов ИБ

Тестирование на проникновение

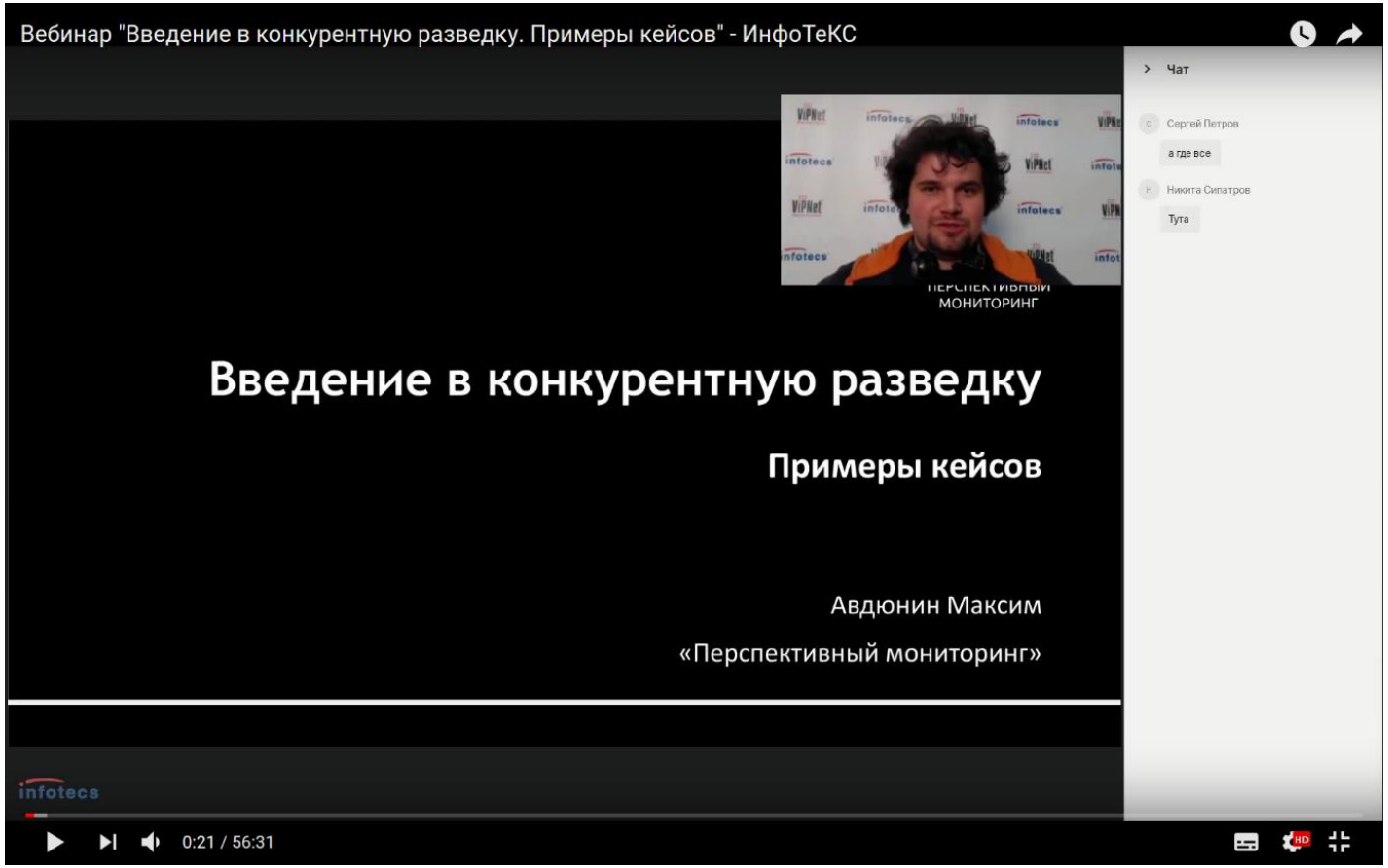
Анализ защищённости ПО

Разработка ПО

Расследование инцидентов ИБ

Конкурентная разведка

Первая часть



- www.youtube.com/watch?v=FzfxGE3i6VE
- www.infotecs.ru/webinars/archive

We are the white hat hackers!

BLACK HAT

vs

WHITE HAT

We are the white hat hackers!

vs

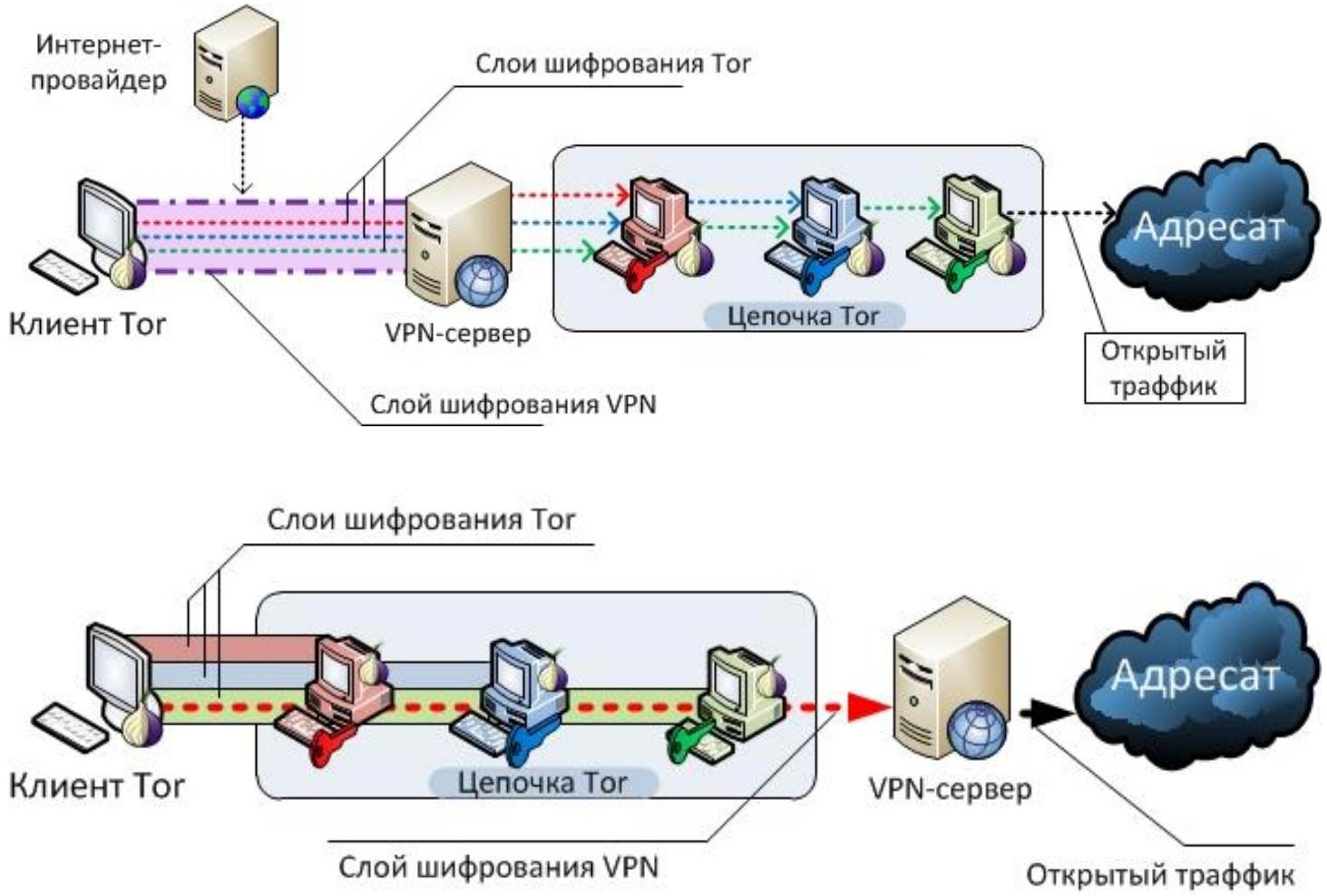
- **Статья 272 УК РФ.** Неправомерный доступ к компьютерной информации
- **Статья 273 УК РФ.** Создание, использование и распространение вредоносных компьютерных программ
- **Статья 274 УК РФ.** Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

Общие методы

Обеспечение невидимости

- Анонимизация
  - Прокси, веб-прокси, плагины-анонимайзеры
  - VPN
  - TOR
  - Прочее (Whonix, I2P, физические средства и т.д.)
- Защита от средств деанонимизации
  - Журналирование
  - IDS/IPS
  - Honeypots

Tor через VPN, VPN через Tor и прочие извращения



Полнота сбора информации

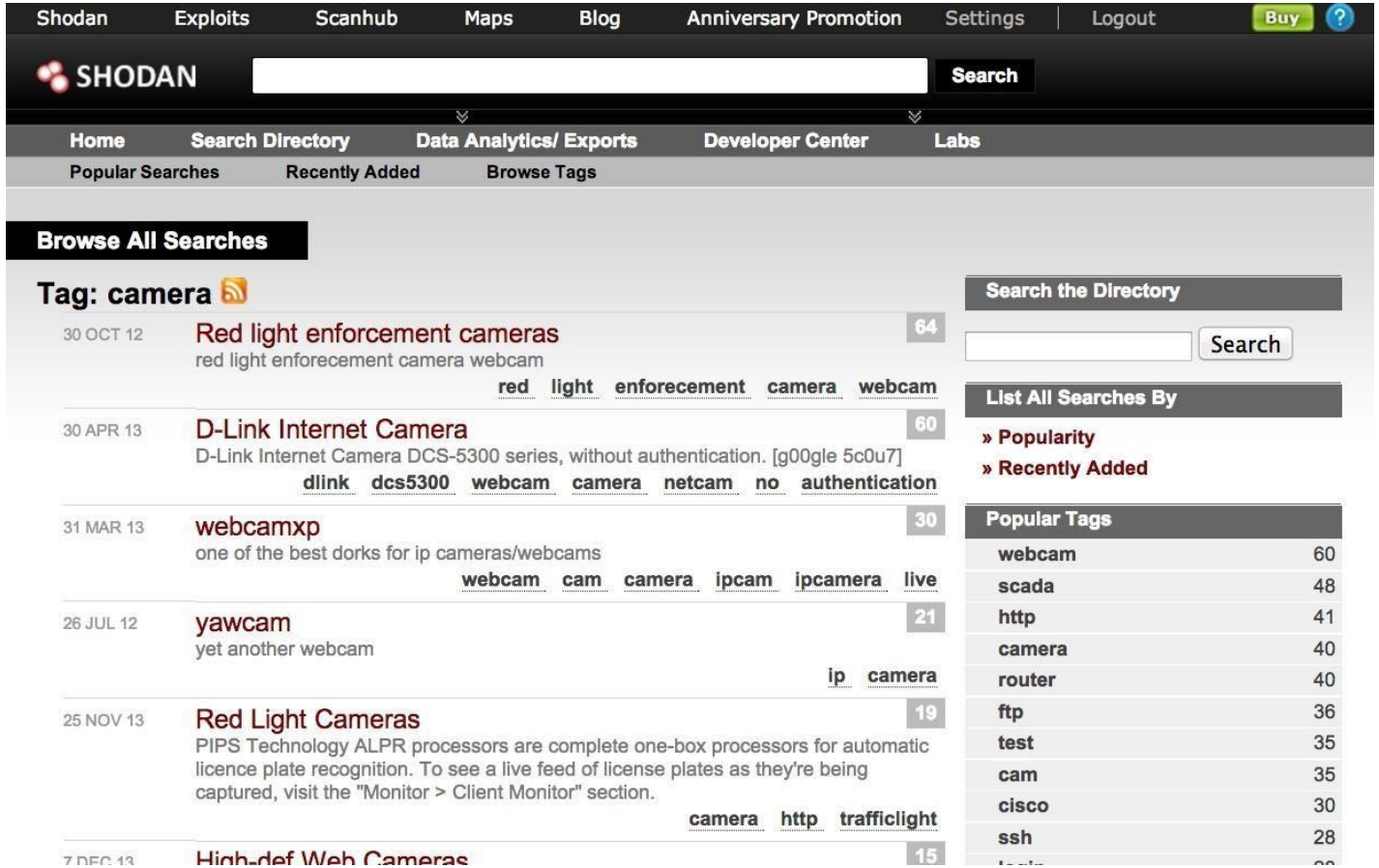
- Аудио-визуальный контент (фотографии, видео, звукозаписи)
- Метаданные
  - EXIF (дата, геолокация)
  - Служебные заголовки e-mail
  - Свойства офисных документов
- Поисковики
  - Метапоисковики
  - Deep Web, Dark Web
  - Региональность
- Мониторинг
  - Ручной
  - Автоматизированный

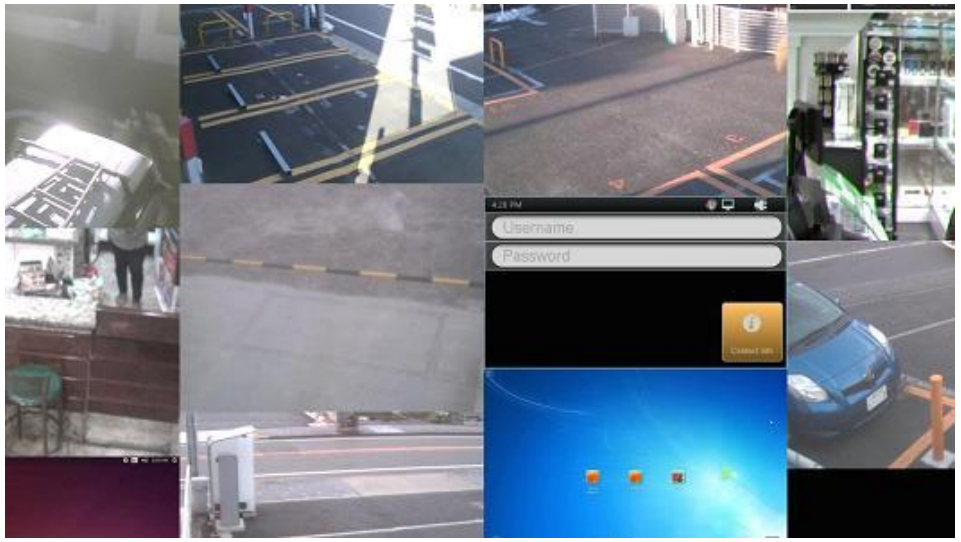
Принц Уильям на базе в Англси

Глубина сбора информации

- Поисковая специфика (Google ≈ Yandex + Bing и т.п.)
- Поисковики изображений (Google-картинки, TinEye и др.)
- Специализированные поисковики (Shodan, Censys)
- Поисковые операторы («INURL:», «FILETYPE:», «SIZE:» и т.п.)
- Google dorks (exploit-db.com/google-hacking-database/)
- Прочие средства (графические редакторы, переводчики, средства распознавания текста)

Веб-камеры и Shodan



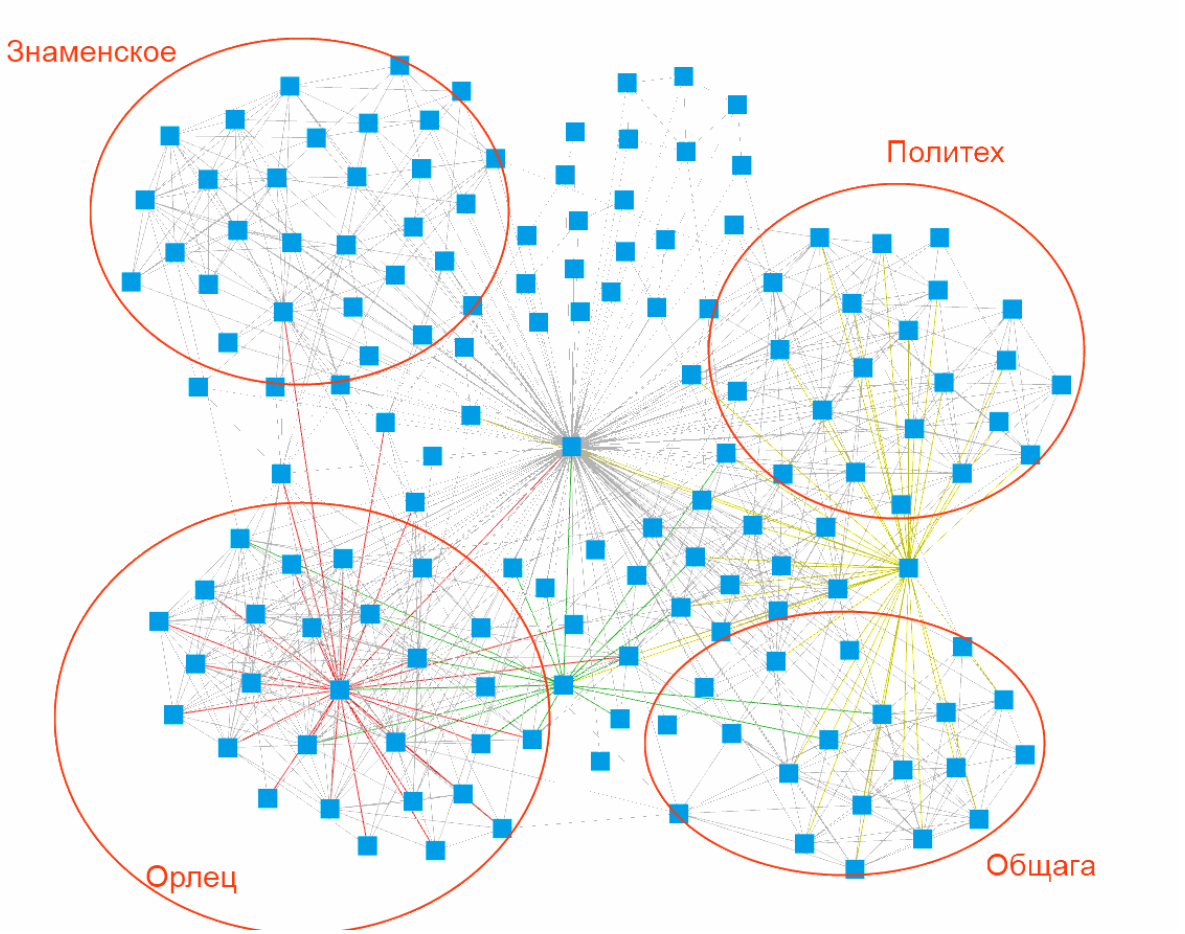


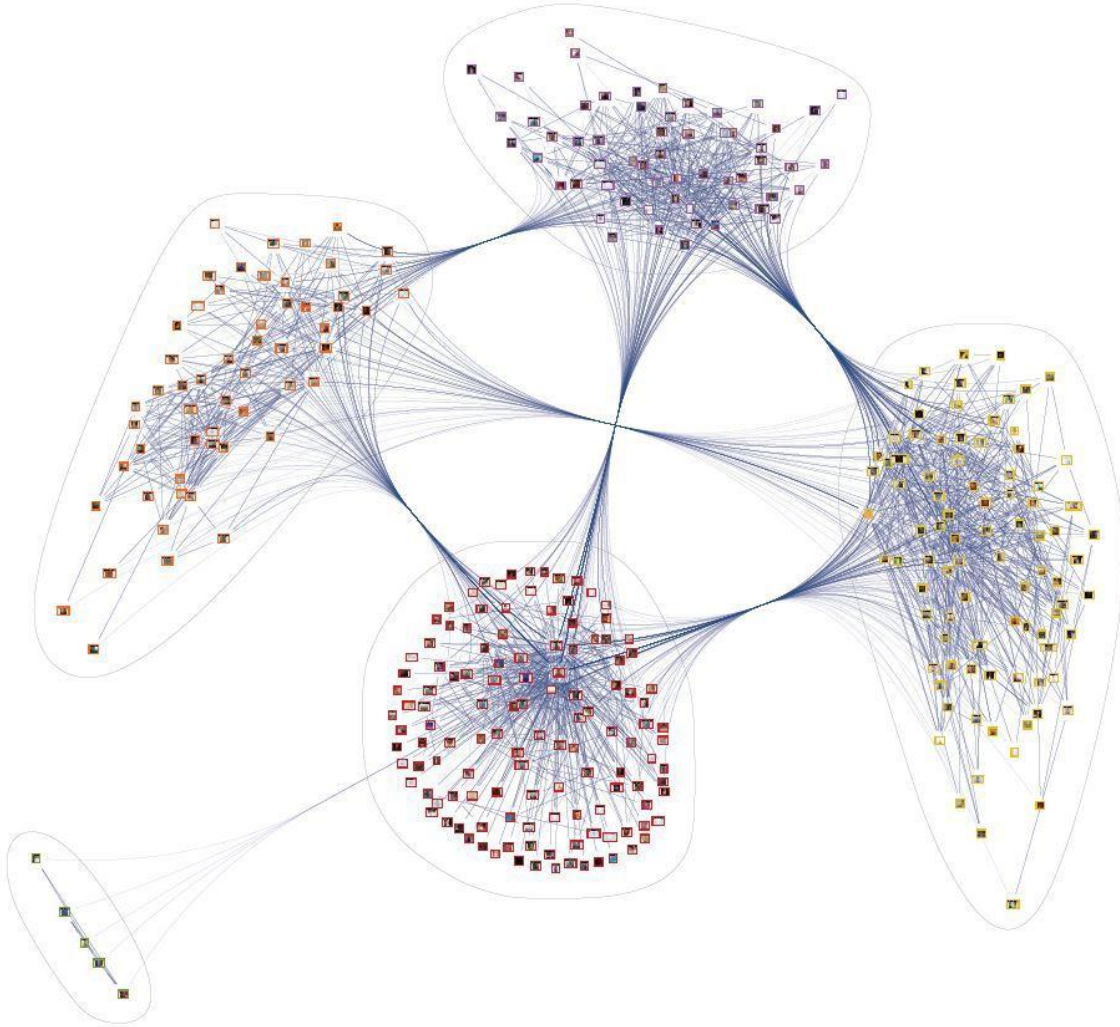
Физические лица

Физические лица

- Открытая информация
  - Официальные источники (например, для США: spokeo.com, whitepages.com, thatsthem.com)
  - Неофициальные источники (phonenumber.to и т.п.)
- Закрытая информация (Deep Web, Dark Web, базы данных)
- Социальные сети и мессенджеры
  - Прямой доступ к информации: ФИО, образование, работа.
  - Косвенные сведения: граф друзей, принадлежность к сообществам, упоминания, история перемещений (Google), геометки (VK, Twitter, Instagram) и т.д.
  - Поиск и получение доступа: findface.ru и google-картинки, восстановление пароля, ip-чекеры.
- Нетрадиционные методы
  - Анализ публикаций, вакансий, материалов СМИ, активности на форумах и т.п.
  - Деанонимизация через средства оплаты: мобильный банк Сбербанка, биткойн-кошельки и т.п.

Социальные графы





Веб-ресурсы

Веб-ресурсы

- Регистрационная информация: WHOIS, история регистрации домена, reverse IP и др.
- История сайта: cache, веб-архивы (archive.org, archive.is)
- Анализ адресной строки
- Технический анализ сайта: перебор директорий (DirBuster) и поддоменов сайта (SubBrute, Knockpy), анализ Robots.txt и т.д.
- Сетевое сканирование (nmap)

Взлом Gartner через адресную строку

Адрес отчёта

http://www.gartner.com/technology/reprints.do?id=1-1FJ5IML&ct=130508

Адрес квадрата

http://imagesrv.gartner.com/reprints/246800/246886/246886_1.png;pv94c471a899798cc3

Упрощённый адрес

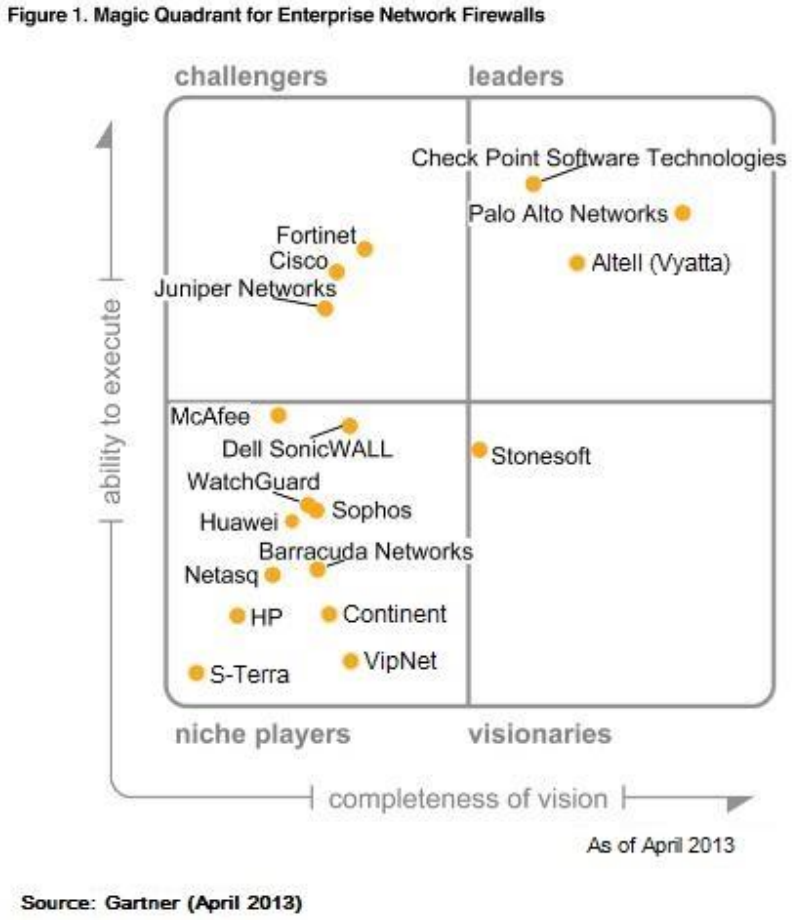
http://imagesrv.gartner.com/reprints/246800/246886/246886_1.png

Формат адреса

http://imagesrv.gartner.com/reprints/[ID00]/[ID]/[ID]_1.png

[ID] — это последние 6 цифр индекса

[ID00] — это [ID], у которого две последние цифры заменены нулями



Получение доступа к ресурсам

Получение доступа к ресурсам

своим

Получение доступа к ресурсам

- Веб-ресурсы
  - Использование сервисов, предоставляющих регистрационные данные аккаунтов закрытых ресурсов (bugmenot.com и т.п.)
  - Авторизация со значениями по умолчанию (admin/admin, user/user и т.п.)
  - Полный перебор паролей в форме авторизации (THC Hydra, Medusa, Ncrack и т.п.)
  - Подбор хеша (hashkiller.co.uk и др.)
  - Восстановление пароля
  - Поиск (и эксплуатация) уязвимостей (Nessus, Metasploit, Acunetix и др.)
- Архивы (атака грубой силой, known-plaintext атака и др.)

Почему перебор работает?

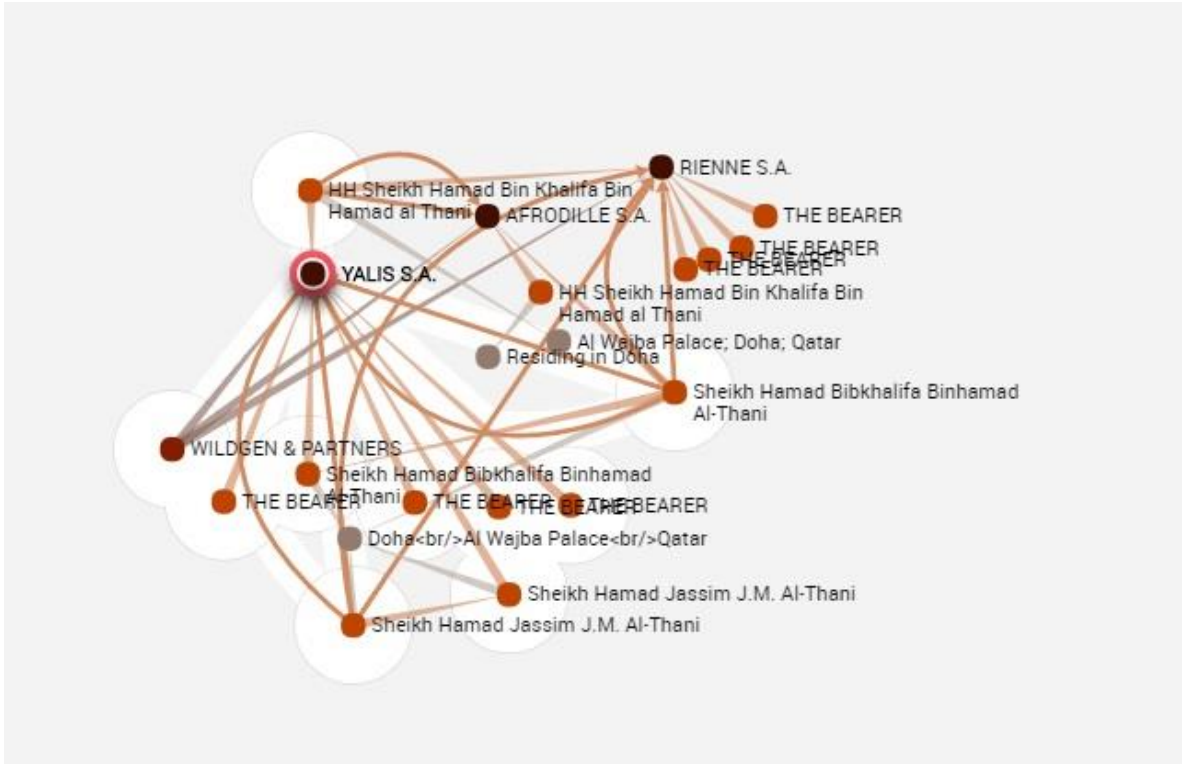
	2012	2013	2014	2015	2016
1	password	123456	123456	123456	123456
2	123456	password	password	password	123456789
3	12345678	12345678	12345	12345678	qwerty
4	abc123	qwerty	12345678	qwerty	12345678
5	qwerty	abc123	qwerty	12345	111111
6	monkey	123456789	123456789	123456789	1234567890
7	letmein	111111	1234	football	1234567
8	dragon	1234567	baseball	1234	password
9	111111	iloveyou	dragon	1234567	123123
10	baseball	adobe123	football	baseball	987654321
11	iloveyou	123123	1234567	welcome	qwertyuiop
12	trustno1	Admin	monkey	1234567890	mynoob
13	1234567	1234567890	letmein	abc123	123321
14	sunshine	letmein	abc123	111111	666666
15	master	photoshop	111111	1qaz2wsx	18atcskd2w
16	123123	1234	16.mustang	dragon	7777777
17	welcome	monkey	access	master	1q2w3e4r
18	shadow	shadow	shadow	monkey	654321
19	ashley	sunshine	master	letmein	555555
20	football	12345	michael	login	3rjs1la7qe

Юридические лица

Юридические лица

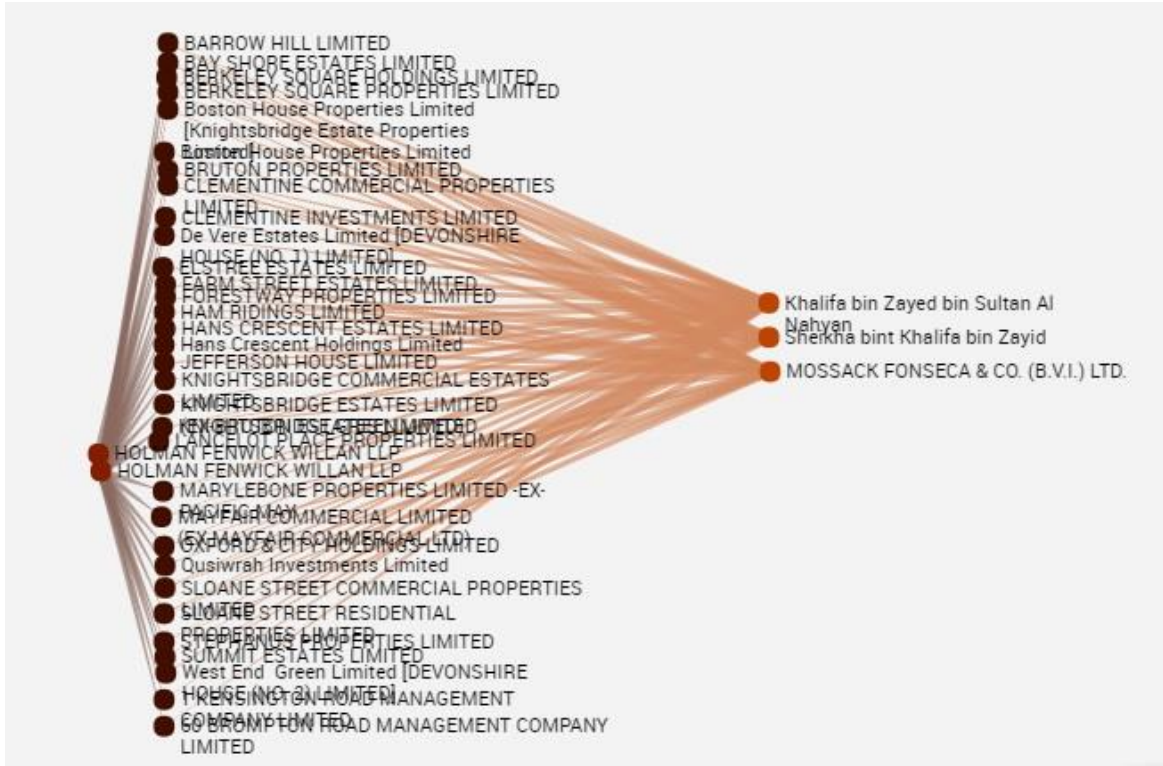
- Информация о компаниях
  - Свободная информация (opencorporates.com, zachestnyibiznes.ru и т.п.)
  - Открытая информация (Сбис, Контур-Фокус, СПАРК, Bureau van Dijk и т.п.)
  - Закрытая информация (Deep Web, Dark Web, базы данных)
- Гос. закупки (zakupki.gov.ru, birja.ru, gostorgi.ru)
- Публикации (СМИ и профильные ресурсы)
- Архив вакансий компании
- Отзывы о компании (antijob.net и т.п.)

Панамский архив



Король Саудовской Аравии

Салман ибн Абдул-Азиз Аль Сауд



Бывший премьер-министр Украины

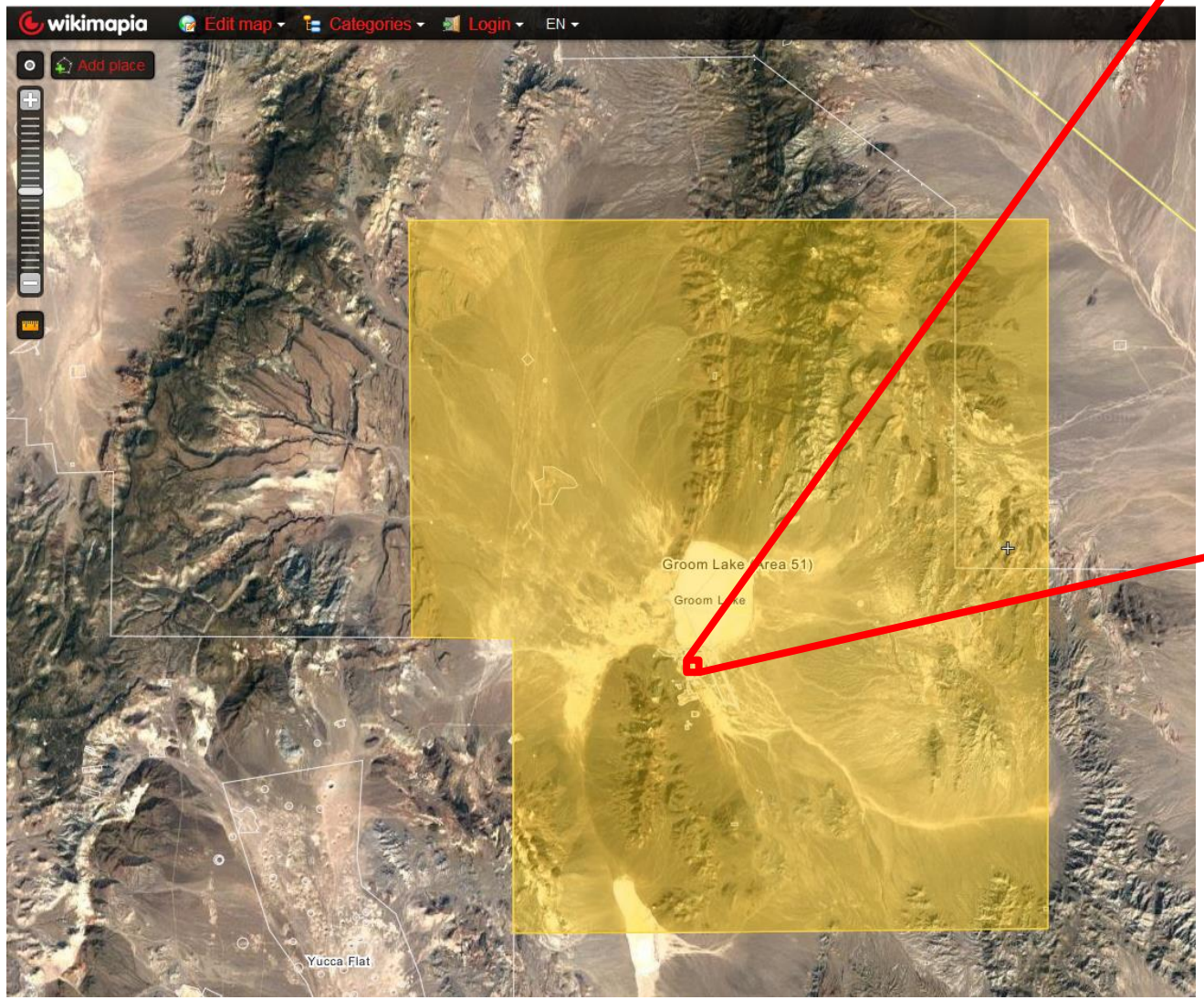
(1996-1997) Павел Лазаренко

Недвижимость

Недвижимость

- Официальная информация
  - ЕГРП, Справочная система по объектам недвижимости и т.д.
  - Кадастровая карта РФ
- Закрытая информация (Deep Web, Dark Web, базы данных)
- Картографические сервисы
  - Яндекс.Карты, Google Maps, 2ГИС, OSM и т.д.
  - Визуальный осмотр: Google Street View, панорамы Яндекс.Карт и т.д.
  - Дополнительная информация (wikimapia.org и т.д.)

Wikimapia — подарок для шпиона



Moscow River Project site

USA / Nevada / Indian Springs /

military Add category

The project is one of the highest air-tight security activities at this base. It does have something to do with recent escalation of Russian air force patrols. This structure is mainly the project's control or administrative center.

Nearby cities: Mesquite, Nevada, St. George, Utah, Washington, Utah
Coordinates: 37°14'32"N 115°48'54"W

Add your comment in english

Comments

Randy613w (guest)
The Moscow River has nothing to do with Russia or Moscow or any river for that effect.
9 years ago | reply

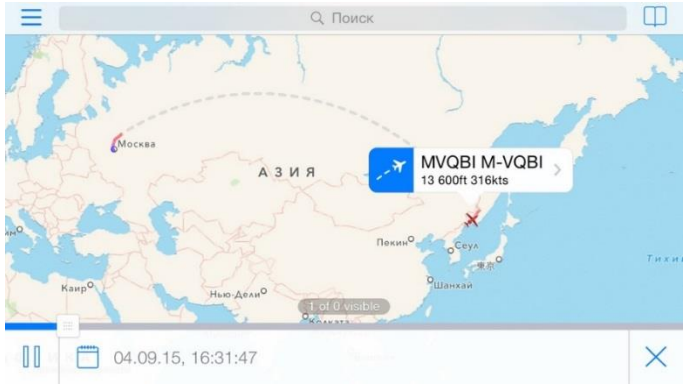
StacheldrahtN01 (guest)
all you armchair mystery professors: MOSCOW is an acronym. "nothing to do with Russia". "Materiel Operations Support Center, Oscar Wiskey..." etc the nearby KUKLA PEN facility owes its name to KUKLA, CIA's crypto name for its internal operations (KU) and KLA, Kampala airport code, and PEN being an acronym for a project.
5 years ago | reply

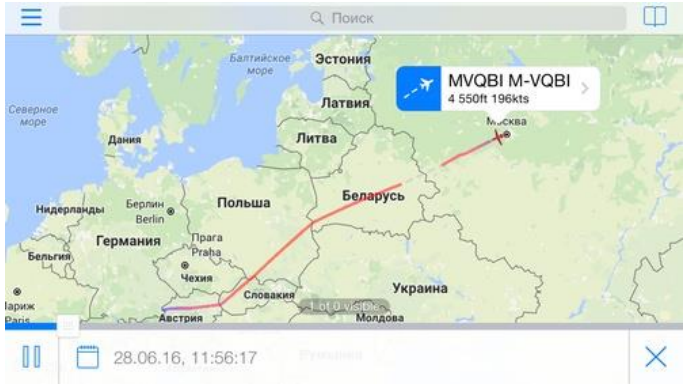
Транспорт

Транспорт

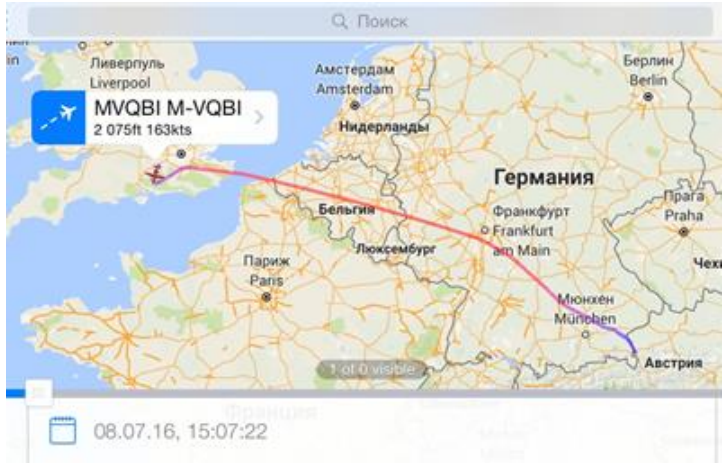
- Регистрационная информация
  - Автотранспорт
    - avtocod.ru, nomerorg.biz/mosgibdd, AVinfoBot (Россия)
    - gov.uk/get-vehicle-information-from-dvla (Великобритания)
    - и т.д.
  - Морской транспорт (vesselfinder.com)
  - Авиатранспорт (airframes.org)
- Информация о перемещении транспортных средств
  - Морской транспорт (marinetraffic.com)
  - Авиатранспорт (planefinder.net, flightradar24.com)
- Закрытая информация (Deep Web, Dark Web, базы данных)

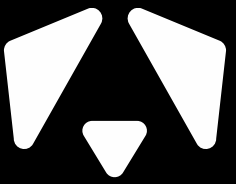
ФБК и корки


Поиск
MVQBI M-VQBI
13 600ft 316kts
Москва
Пекин
Сеул
Шанхай
Нью-Дели
Каир
1 of 0 visible
04.09.15, 16:31:47


Поиск
MVQBI M-VQBI
4 550ft 196kts
Эстония
Латвия
Литва
Дания
Польша
Беларусь
Нидерланды
Германия
Прага
Praha
Чехия
Словакия
Украина
Австрия
Молдова
28.06.16, 11:56:17


9.ANDVOL YA TVOY IDOL- v.p. 1, cw
HAPPY FELLA x Edlen House Ocean of Sharm
ow. Shuvalova O.
ROYAL CANIN
Photo by Elena Ignatova
www.ilen-dream.com.ua


Поиск
MVQBI M-VQBI
2 075ft 163kts
Ливерпуль
Liverpool
Амстердам
Amsterdam
Берлин
Berlin
Нидерланды
Германия
Бельгия
Франкфурт
Frankfurt
am Main
Прага
Praha
Люксембург
Париж
Paris
Мюнхен
München
Австрия
1 of 0 visible
08.07.16, 15:07:22



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Спасибо за внимание!

Максим Авдюнин

Maksim.Avdyunin@amonitoring.ru