

Расширенное руководство по онлайн-камерам

v0.2.4

2017

Содержание

| | |
|---|-----------|
| 1. Введение | 3 |
| 2. Терминология | 5 |
| 3. Поиск онлайн-камер | 6 |
| 3.1. Сетевые адреса | 6 |
| 3.1.1. IP-адреса | 6 |
| 3.1.2. Порты | 8 |
| 3.2. Клиентский софт | 9 |
| 3.2.1. Nmap | 9 |
| 3.2.2. VNC | 11 |
| 3.2.3. KPortScan | 12 |
| 3.2.4. Angry IP Scanner | 13 |
| 3.2.5. Advanced IP Scanner | 15 |
| 3.2.6. Nesca | 16 |
| 3.2.7. RouterScan | 18 |
| 3.2.8. Другие инструменты | 19 |
| 3.3. Онлайн-софт | 20 |
| 3.3.1. Онлайн-базы камер | 20 |
| 3.3.2. Google Search | 22 |
| 3.3.3. Shodan | 26 |
| 4. Получение доступа | 30 |
| 4.1. Логины и пароли | 30 |
| 4.1.1. Онлайн-базы логинов, паролей и URL | 30 |
| 4.1.2. Статистика | 30 |
| 4.1.3. Логины и пароли по умолчанию | 32 |
| 4.2. Инструменты | 34 |
| 4.2.1. hikka | 34 |
| 5. Просмотр онлайн-камер | 35 |
| 5.1. Форматы трансляции | 35 |
| 5.1.1. Обновление изображения | 35 |
| 5.1.2. Потоковое видео | 36 |
| 5.1.3. MJPEG | 37 |
| 5.2. Браузерные плагины | 38 |
| 5.2.1. Java-апплеты | 39 |
| 5.2.2. QuickTime Player | 43 |
| 5.2.3. ActiveX | 45 |
| 5.2.4. Разнообразные плагины | 49 |
| 5.3. Софт для камер | 52 |

1. Введение

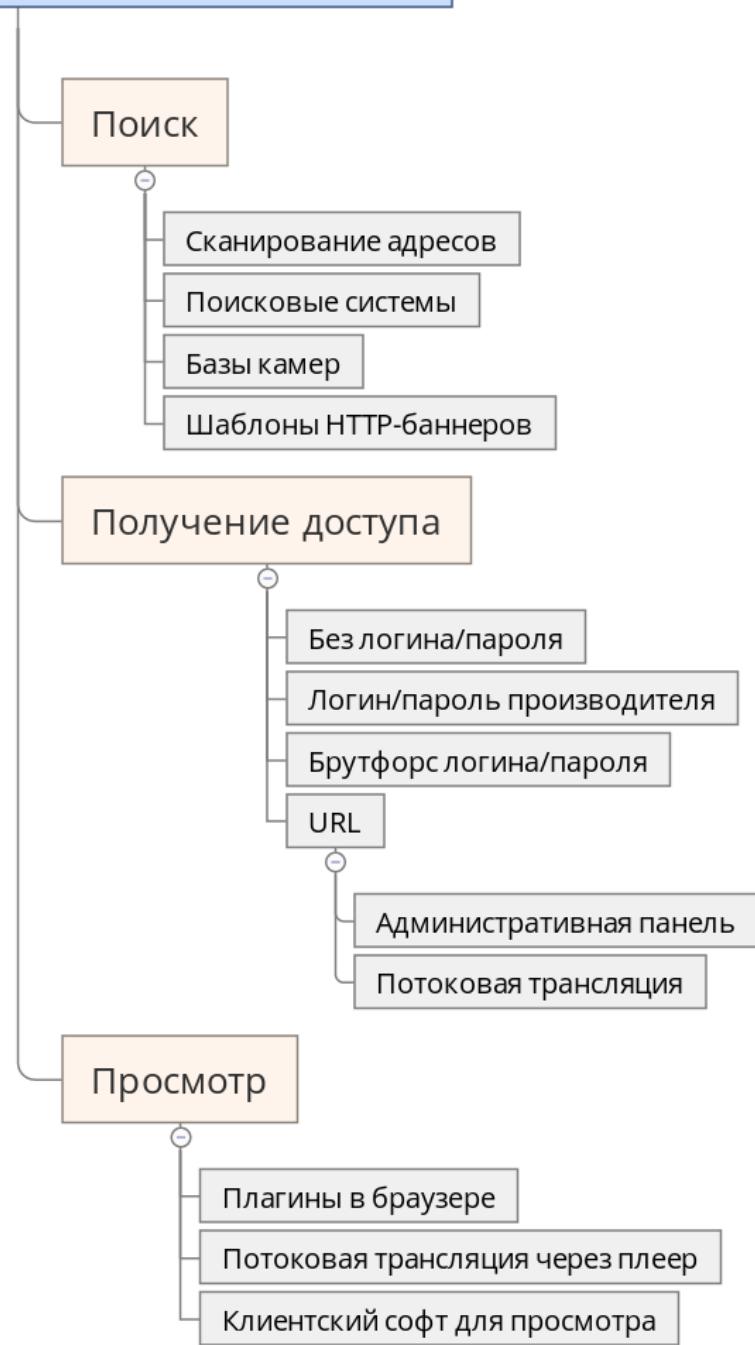
Безусловно, просмотр онлайн-трансляций – одно из важнейших преимуществ развития World Wide Web. Зрение является основным процессом человеческого восприятия, а наиболее информативно привлекательной для человека есть и останется картина окружающего мира, представленная в визуальном виде – наиболее приближенном к реальному восприятию.

Предназначение данного руководства – дать информацию читателям, заинтересованным в поиске и просмотре непубличных онлайн-трансляций. В этом контексте будут рассматриваться онлайн-камеры – устройства, предназначенные для частного использования, но доступные извне, для всей остальной Сети. Далее в разделах будут освещены вопросы поиска камер, доступа к ним, а также особенности тех или иных видов видеотрансляций.

Следует отметить, что при работе с камерами и, в частности, при следовании данному руководству рекомендуется проявлять осторожность и не выполнять действий, в последствиях которых вы не уверены. Ответственность за несанкционированный доступ к сетевым устройствам возлагается на читателей, а авторы напоминают, что в общем случае вся информация о доступе к камере сохраняется для её владельца.

Условно работу с онлайн-камерами можно разделить на стадии поиска, получения доступа и просмотра (изобр. 1). В соответствии с этими стадиями выстроена структура данного руководства, поэтому рекомендуется обращаться к произвольному интересующему вас разделу вместо последовательного чтения.

Работа с онлайн-камерами



Изображение 1 — Работа с онлайн-камерами

Приведённые в тексте программы, примеры возможных ошибок и способы их решения по умолчанию относятся к операционной системе *Windows 7*, если не указано обратное.

2. Терминология

ActiveX – платформа для подключения программных компонент, используемая в ОС Windows, в частности, в Internet Explorer. Не поддерживается в других браузерах, но для Firefox есть плагины, например, ff-activex-host¹.

DVR (Digital Video Recorder) – цифровой видеорегистратор: устройство для записи, хранения и воспроизведения видео.

HTTP (Hypertext Transfer Protocol) – протокол передачи данных (изначально гипертекстовых), используется в браузерах. Стандартный порт – 80.

Iris – регулировка количества света, попадающего на матрицу камеры. От этого зависит резкость изображения и его освещённость.

NPAPI (Netscape Plugin Application Programming Interface) – устаревшая платформа для разработки плагинов к браузерам. Не поддерживается Internet Explorer с 5.5, Google Chrome с 40, Mozilla Firefox с 43, однако используется во множестве камер.

NVR (Network Video Recorder) – сетевой видеорегистратор: аппаратура, предоставляющая возможность просмотра и управления подсоединенными к ней камерами.

RTSP (Real Time Streaming Protocol) – потоковый протокол реального времени, предназначен для передачи мультимедийных данных.

PTZ (Pan, Tilt, Zoom) – аббревиатура, означающая возможность управления камерой (соответственно, панорамирование, наклон, зум).

¹<https://github.com/leeor/ff-activex-host>

3. Поиск онлайн-камер

Условно выделим три группы способа поиска онлайн-камер:

- Ручное сканирование адресного пространства;
- Использование поисковых систем с указанием текстовых шаблонов;
- Поиск в готовых базах данных камер с фильтрацией по характеристикам.

Инструменты для сканирования в основном представлены клиентскими программами, т.к. большинство онлайн-сканеров обладают либо урезанной функциональностью, либо доступны только за абонентскую плату. К клиентским инструментам относятся широко известные **Nmap**, **ZMap**, **Masscan** и другие. Описание подобных инструментов представлено в разделе Клиентский софт.

При использовании поисковых систем необходимо использовать специальные запросы – **dorks**, представляющие собой фильтры поиска с указанием точного текста и/или других параметров в контенте страницы. Напомним, что индексируемый поисковиками контент является *HTTP-баннером*, текстом web-страницы сервера, которой в случае с камерами является административная панель. Таким образом, при известных заголовке HTTP-страницы камеры, части соответствующего URL и других параметров возможен поиск экземпляров таких камер через индексирующие системы. Примеры запросов в поисковых системах общего назначения на примере Google приведены в разделе Shodan.

Готовые базы данных, как правило, являются либо специализированными развлекательными сайтами, напрямую выводящими видеотрансляцию на свою страницу, либо интерфейсами поисковиков специального назначения (например, Shodan), имеющих категоризацию по типам устройств и производителям. Список подобных сервисов приведён в разделе Онлайн-базы камер.

3.1. Сетевые адреса

3.1.1. IP-адреса

Предположим, что читающий ознакомлен с понятием IP-адреса как такового. Здесь лишь напомним, что IP адрес стандарта IPv4 состоит из 4 чисел от 0 до 255, разделённых точкой. Общее количество таких адресов – 4 294 967 296. Для реальных хостов 0 и 255 адреса резервируются, также некоторые диапазоны резервируются для использования

в локальных сетях. Это означает, что общее количество реальных IP несколько ниже.

Следует отметить, что в настоящее время активно продвигается стандарт IPv6, предоставляющий намного большее адресное пространство и, соответственно, более широкие перспективы для развития IoT (интернета вещей) и для камер в частности. Аспекты сканирования диапазона IPv6 будут рассмотрены в следующих версиях руководства.

Также напомним, что в пределах одного адреса могут существовать различные порты (от 1 до 65535). Грубо говоря, если вы знаете адрес дома, то это ещё не значит, что он открыт для вас – необходимо найти открытую дверь, но дверей потенциально могут быть тысячи. В общем случае, за каждым портом закреплена определённая функция/приложение.

Отметим, что могут существовать различные форматы записи адресов, которые могут использоваться при сканировании.

CIDR (Classless Inter-Domain Routing) – нотация, которая позволяет записать целую подсеть. Стока при этом состоит из самого адреса и *битовой маски*, которая показывает, сколько первых битов адреса должны оставаться неизменными.

Битовая маска может иметь значение от 0 до 32. Таким образом, *адрес 123.56.78.9/0* означает все возможные адреса (так как 0 битов фиксированы, меняются все биты адреса),

адрес 123.56.78.9/24 означает адреса диапазона 123.56.78.0-123.56.78.255 (так как 24 бита фиксированы, меняются последние 8 бит = байт = число от 0 до 255),

адрес 123.56.78.9/32 означает один адрес - 123.56.78.9 (так как все 32 бита адреса фиксированы, то адрес может быть записан только в одном варианте).

Понимание формата необходимо в случае, когда нужно просканировать сеть организации/города/государства/etc, но она (в общем случае) представляет собой не последовательный диапазон адресов, а набор различных подсетей. Понимание количества затрагиваемых адресов позволяет спланировать время и ресурсы.

Для работы при необходимости доступны онлайн-калькуляторы² и конвертеры³.

Простые диапазоны IP-адресов означают последовательное перечисление с первого до последнего с учётом формата записи. Таким образом, диапазон 123.56.78.9-123.56.79.10 будет включать в себя адреса 123.56.78.9-123.56.78.255 и 123.56.79.0-123.56.78.10.

Сложные диапазоны IP-адресов означают видоизменение отдельных байт в записи адреса. Например, диапазон 123.56.78-79.9 будет

²<http://www.subnet-calculator.com/cidr.php>

³<http://www.ipaddressguide.com/cidr>

включать в себя только два адреса, но эти адреса будут непоследовательны.

Это формат может быть полезен, но не является общеиспользуемым.

Доменные имена используются повсеместно и также могут быть использованы для сканирования. Стоит упомянуть, что IP-адресу имя не только может не быть сопоставлено, но и может быть сопоставлено несколько имён. В данном руководстве особенности сетевой адресации рассматриваться не будут.

Откуда брать сетевые адреса для сканирования? Ниже представлен список некоторых сервисов:

- CIPRG⁴ – Country IP Ranges Generator, генератор IP-диапазонов по странам с регулярно обновляемой базой;
- 4it.me⁵ – популярный в Рунете сервис, предоставляет IP диапазоны городов (диапазоны/CIDR, два варианта базы: мировая и Ru-center). В комментариях можно встретить адреса и советы;
- ipaddresslocation.org⁶ – получение IP по стране (диапазоны/CIDR);
- countryipblocks.net⁷ – получение диапазонов IP в 12 разных форматах;
- IPdeny⁸ – готовые для скачивания файлы со блоками IP по странам.

3.1.2. Порты

Порт - число от 0 до 65535, используемое для уточнения параметров подключения по IP-адресу. Таким образом, каждое соединение (подразумевается протоколы TCP и UDP) характеризуется не только двумя адресами, но и соответствующими портами.

Есть стандартные порты⁹, которые используются по историческим причинам и/или официально закреплены в документации программ. Один из таких портов – **80**, по умолчанию используемый для доступа к сайтам по протоколу HTTP. Большая часть онлайн-камер, имеющих web-интерфейс, доступны именно через этот порт.

⁴<http://services.ce3c.be/ciprg/>

⁵<https://4it.me/getlistip>

⁶http://www.ipaddresslocation.org/ip_ranges/get_ranges.php

⁷https://www.countryipblocks.net/country_selection.php

⁸<http://www.ipdeny.com/ipblocks/>

⁹https://ru.wikipedia.org/wiki/Список_портов_TCP_и_UDP

Другие наиболее часто используемые порты для web-интерфейсов камер (по данным Casca, 12.2015): **81, 8080, 82, 8081, 8888, 8000, 8082, 8001, 9000, 83, 88, 8083, 85, 8008**.

3.2. Клиентский софт

3.2.1. Nmap

В качестве инструмента сканирования IP-адресов в первую очередь следует рассмотреть Nmap. Это широко используемая консольная утилита, которая поддерживает множество возможностей. Здесь не будет рассматриваться весь их спектр, а только минимально необходимые параметры поиска. Полное руководство можно прочесть на официальном сайте¹⁰, начинающим рекомендуется ознакомиться с вольным переводом англоязычного руководства от нетсталкинг-группы DWR¹¹. Рекомендуется использовать консольный интерфейс, однако, доступен и официальный графический: **Zenmap**¹².

```
:-$ nmap -T5 -n -Pn -p 80,8080 --open --script http-title --stats-every 1s 121.148.233.229/31

Starting Nmap 6.47 ( http://nmap.org ) at . MSK
Stats: 0:00:01 elapsed; 0 hosts completed (2 up), 2 undergoing Connect Scan
Connect Scan Timing: About 62.50% done; ETC: 01:04 (0:00:01 remaining)
Stats: 0:00:02 elapsed; 0 hosts completed (2 up), 2 undergoing Script Scan
NSE Timing: About 0.00% done
Stats: 0:00:03 elapsed; 0 hosts completed (2 up), 2 undergoing Script Scan
NSE Timing: About 0.00% done
Nmap scan report for 121.148.233.229
Host is up (0.26s latency).
Not shown: 1 closed port
PORT      STATE SERVICE
80/tcp    open  http
|_http-title: NETSurveillance WEB

Nmap done: 2 IP addresses (2 hosts up) scanned in 3.51 seconds
```

Изображение 2 — Nmap – определение HTTP-заголовка

Запускать инструмент желательно от имени администратора, так как низкоуровневый доступ к сетевому адаптеру будет недоступен простому пользователю. В случае ошибки доступа (изобр. 3) в некоторых случаях достаточно дописать опцию **--unprivileged**, однако перезапуск под администратором может быть единственным выходом. То же относится и к запуску графической оболочки.

¹⁰<https://nmap.org/man/ru/>

¹¹<https://github.com/deep-web-research/ultimate-netstalking-guide/blob/master/nmap-guide.md>

¹²<https://nmap.org/zenmap/>

```

Starting Nmap 6.46 < http://nmap.org > at 2015-12-03 16:36 RTZ 2
Error in OpenService
Initiating Ping Scan at 16:36
Only ethernet devices can be used for raw scans on Windows. Use
the --unprivileged option for this scan.
QUITTING!

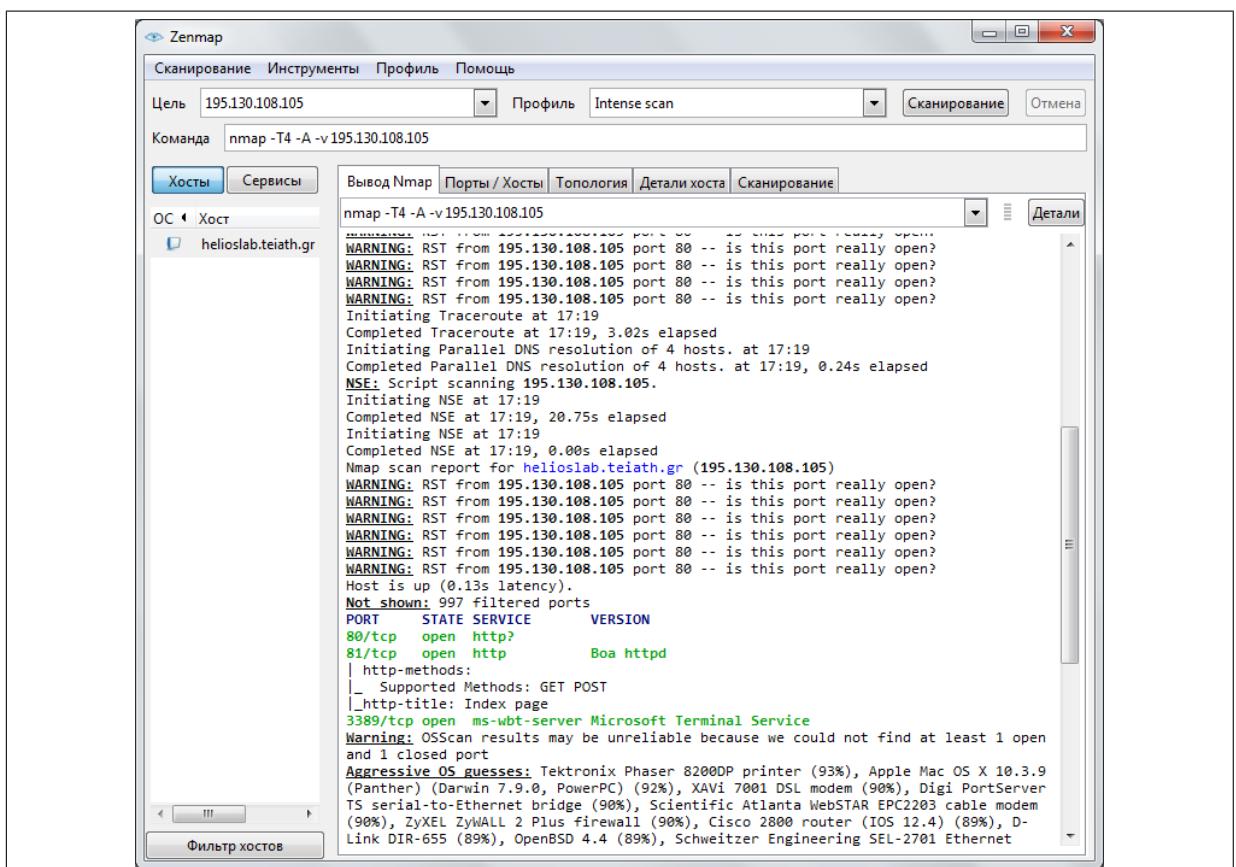
```

Изображение 3 — Nmap – ошибка при запуске

Для запуска в консоли начинающему рекомендуются следующие опции: **-T5 -n -Pn -p 80,8080 --open --script http-title --stats-every 5s**

При этом каждые 5 секунд будут выводиться найденные хосты с заголовками HTTP-страниц, по которым можно вручную опознать камеры (см. шаблоны поиска в разделе Shodan). Указанные порты 80 и 8080 являются одними из самых популярных HTTP-портов (статистику по камерам см. в разделе Статистика).

Те же опции можно использовать и для графической оболочки Zenmap, вводя их в поле "команда"(изобр. 4), также там уже есть предустановленные профили сканирования, на которые можно ориентироваться.

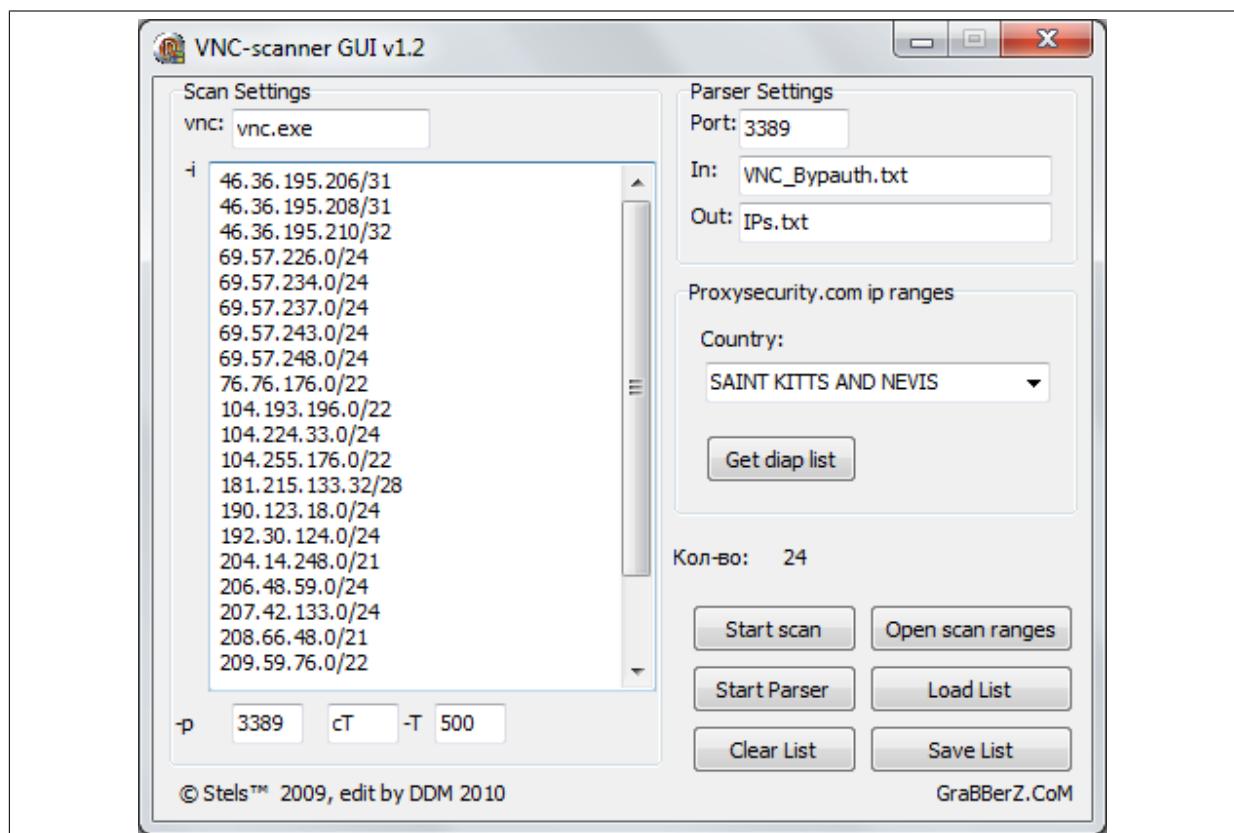


Изображение 4 — Графический интерфейс Zenmap

3.2.2. VNC

VNC (RealVNC Bypass Authentication Scanner) – консольный сканер, используемый в основном для скана IP-адресов с открытым портом 3389 (удалённый рабочий стол ОС Windows). Сайт разработчиков¹³ по состоянию на 05.2016 не работает.

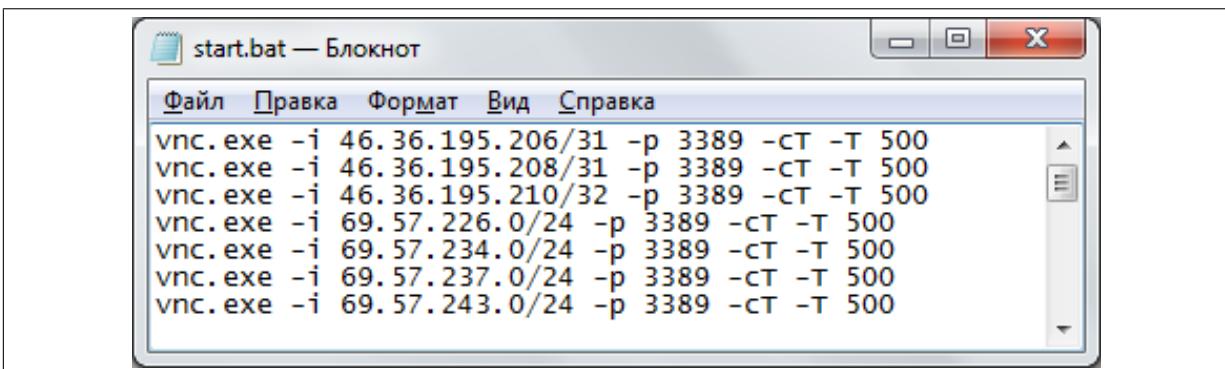
Широко распространена графическая версия сканера VNC-scanner GUI. Настройки и использование далее будут рассматриваться для этой версии.



Изображение 5 – VNC scanner GUI

Для запуска необходим лишь один exe-файл, сама консольная утилита запакована в нём, а используемые параметры наглядно отображаются в графическом интерфейсе. После нажатия на кнопку **Start scan** создаётся и запускается файл **start.bat**, в который записывается список команд для консольной утилиты с параметрами.

¹³<http://heapoverflow.com/>



Изображение 6 — Скрипт для запуска VNC

Параметры сканера:

vnc – запускаемый файл;

-i – IP-адреса для сканирования (используются CIDR и простые диапазоны) через переносы строк;

-p – порты для сканирования, допускается перечисление через запятую или диапазоны;

-cT – использование метода TCPconnect для проверки портов;

-T – количество потоков для сканирования, по умолчанию 500.

Результаты сканирования дописываются в файл **VNC_bypauth.txt** в виде *<IP>:<port>*. Для получения чистого списка IP можно воспользоваться парсером: в поле **Port** следует ввести порт, по которому нужно отсеять список из файла результатов, в поля **In** и **Out** можно ввести имена файлов, если необходимо использовать файлы не по умолчанию. После нажатия кнопки **Start Parser** сформируется текстовый файл со списком IP без портов.

Загрузка диапазонов IP с сайта Proxysecurity.com по состоянию на 12.2015 не работает.

Также следует отметить полезные служебные функции: **Open scan ranges** – загрузка встроенного диапазона IP-адресов; **Load List** и **Save List** – загрузка и сохранение введённых диапазонов соответственно; **Clear List** – очистка введённых диапазонов.

3.2.3. KPortScan

Простой сетевой сканер с графическим интерфейсом и минимумом настроек (изобр. 7). Быстрее VNC, но результаты сканирования хуже. Принимает только простые диапазоны. Имеется визуальное отображение прогресса сканирования.

Описание полей ввода:

threads – количество потоков сканирования;

port – искомый порт;

Способ сохранения файла результата results.txt:

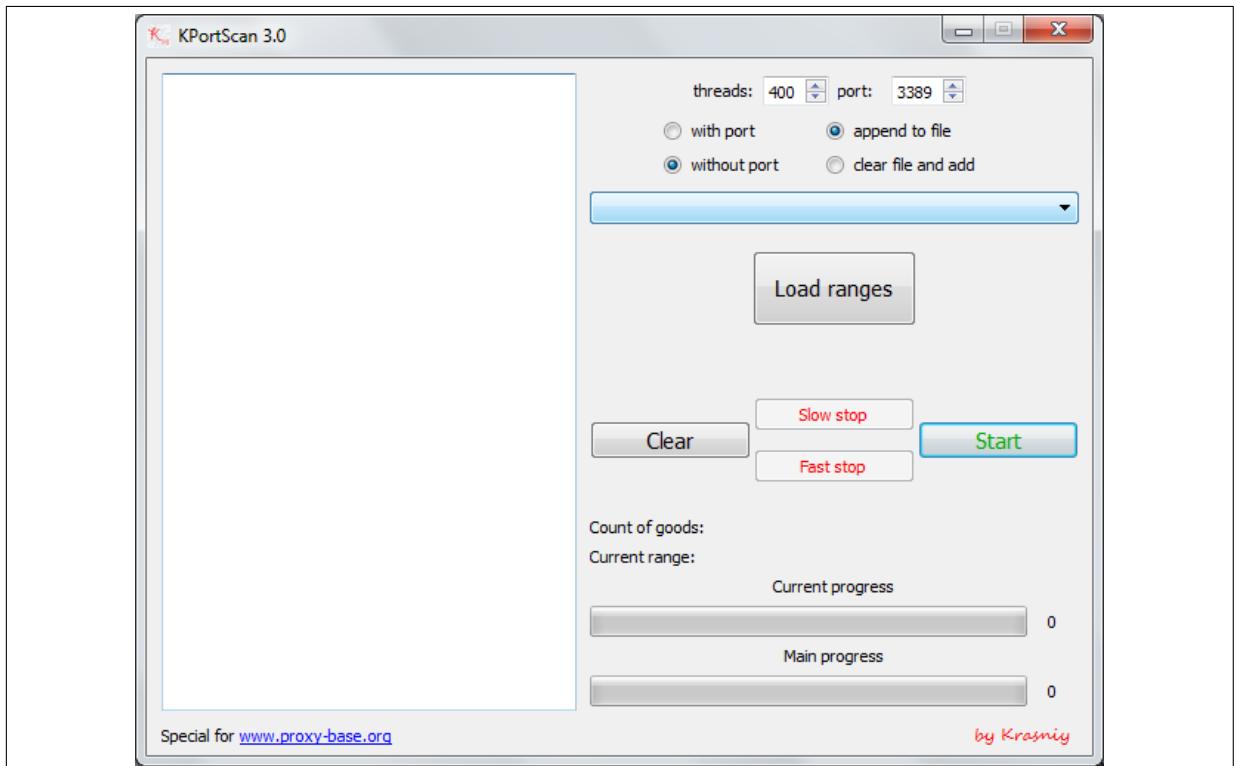
without port - сохраняет без порта;

with port - сохраняет с портом в виде `<IP>:<port>`;
append to file - добавляет новые результаты к предыдущим результатам, находящимся в файле;

clear file and add - удаляет предыдущие результаты, сохраненные в файле, и записывает новые результаты в чистый файл.

Загрузка диапазонов IP (**Load ranges**) с сайта Proxysecurity.com по состоянию на 12.2015 не работает.

Остановить сканирование можно двумя способами: быстрым (**fast**) и медленным (**slow**). В первом случае сканирование прервётся мгновенно, а во втором программа завершит работу с текущим диапазоном (удобно при наличии большого количества диапазонов).



Изображение 7 — KPortScan

3.2.4. Angry IP Scanner

Angry IP Scanner¹⁴ – инструмент для сканирования, чрезвычайно удобный возможностями кастомизации, хоть и имеющий баги.

Для сканирования можно использовать как диапазон IP (возможно определение адреса по известному имени хоста), так и случайные адреса и списки IP.

Далее будет рассматриваться настройка программы для версии 3.4. Открываем *Tools – Preferences*. Во вкладке *Scanning* выставляем *Pinging method* **Combined UDP+TCP** – более продуктивный метод

¹⁴<http://angryip.org/>

сканирования. Количество портов можно установить выше, ориентируясь на загрузку процессора при сканировании. Во вкладке *Ports* вставляем в многострочное поле ввода список необходимых портов (можно использовать порты из раздела Статистика). Во вкладке *Display* выставляем отображение только хостов с открытыми портами (Hosts with open ports only).

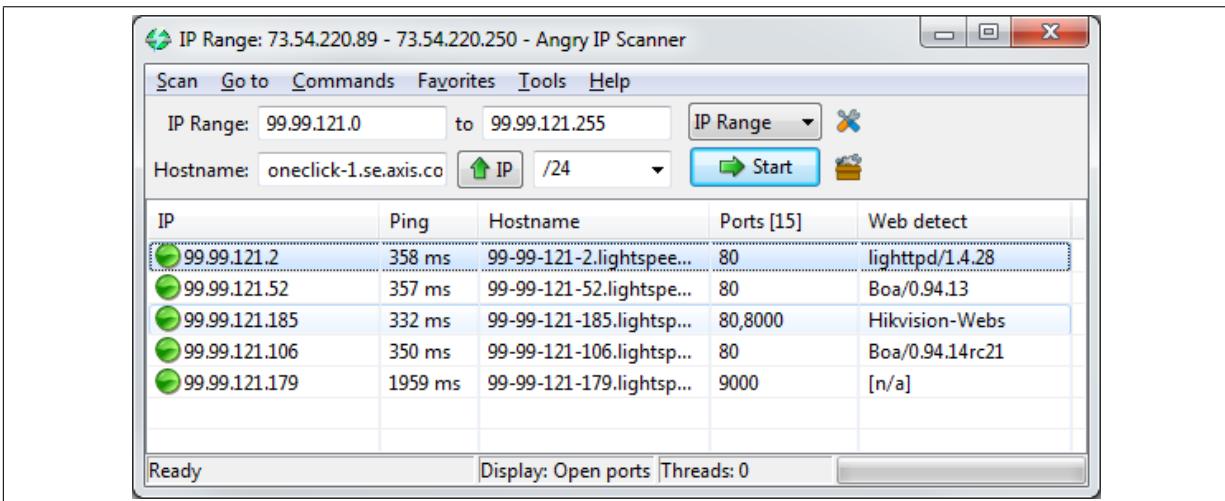
Открываем *Tools – Fetchers*. Колонка **IP** будет отображаться в любом случае, а из других полей необходимо только **Web detect** (определение имени сервера).

Открываем *Command – Open – Edit openers*. Здесь находятся настраиваемые команды, которые можно выполнить для каждого из найденных результатов. Для сканирования камер очень полезна опция открытия браузера с найденным IP, а также геолокация (заданная по умолчанию ссылка не работает). Ниже в таблице приведены примеры полезных команд. Необходимо отметить, что горячие клавиши Ctrl+1... Ctrl+9 для команд не будут обновлены непосредственно после редактирования команд, надо будет перезапустить программу.

Таблица 1 — Команды для Angry IP Scanner

| Opener name (menu item) | Run program in the terminal | Execution string | Описание |
|------------------------------------|--|---|--|
| Internet Explorer | Выставить | start iexplore \${fetcher.ip} | Запуск Internet Explorer с выбранным IP |
| Google Chrome | Выставить | start chrome \${fetcher.ip} | Запуск Google Chrome с выбранным IP |
| Mozilla Firefox | Выставить | start firefox \${fetcher.ip} | Запуск Mozilla Firefox с выбранным IP |
| Браузер по умолчанию | Не выставлять | http:// \${fetcher.ip}/ | Запуск браузера по умолчанию с выбранным IP |
| Геолокация | Не выставлять | http:// www.infosniper.net/index.php?ip_address= \${fetcher.ip} | Запуск браузера по умолчанию с геолокацией для выбранного IP |

Пример результатов сканирования приведён на изобр. 8.



Изображение 8 — Angry IP Scanner

3.2.5. Advanced IP Scanner

Advanced IP Scanner¹⁵ – популярная удобная программа для сканирования, анализа и управления компьютерами как в локальной, так и глобальной сети.

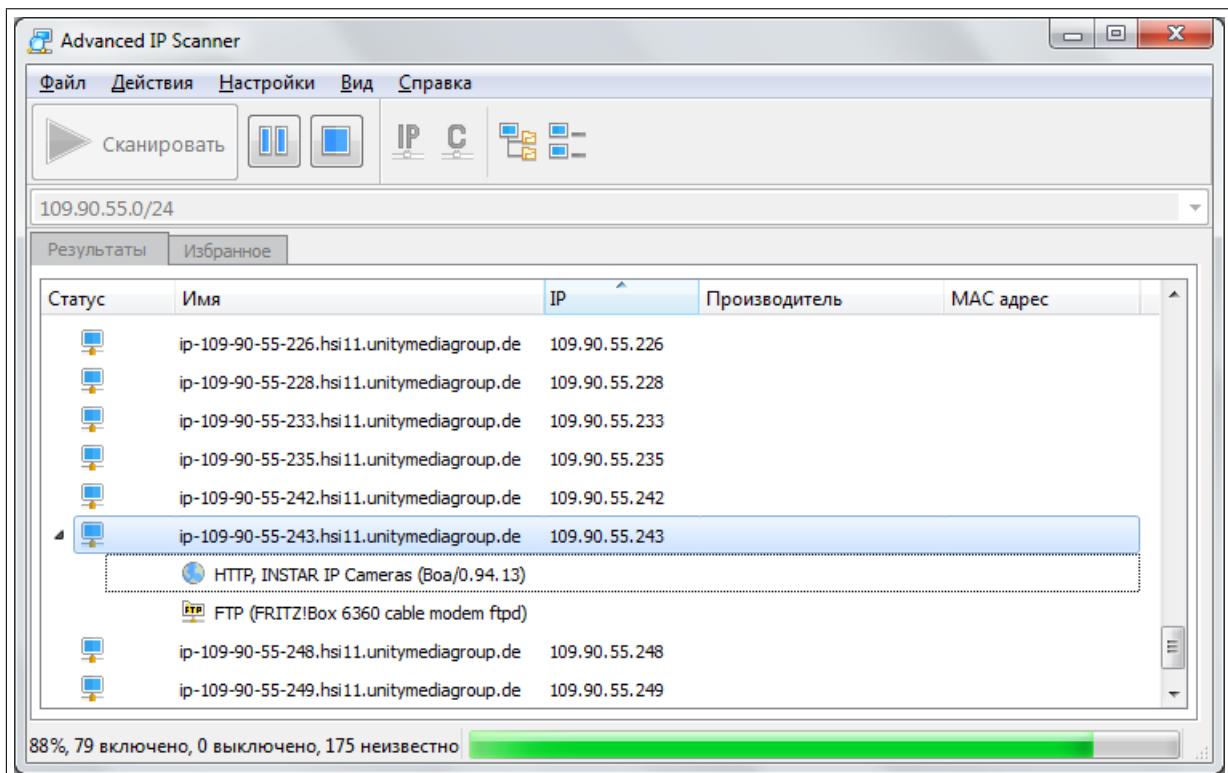
Доступны действия для портов по умолчанию (просмотр HTTP, FTP, RDP), интеграция с Radmin для удалённого управления.

В качестве аргументов принимает обычные записи IP-адресов, CIDR и простые диапазоны.

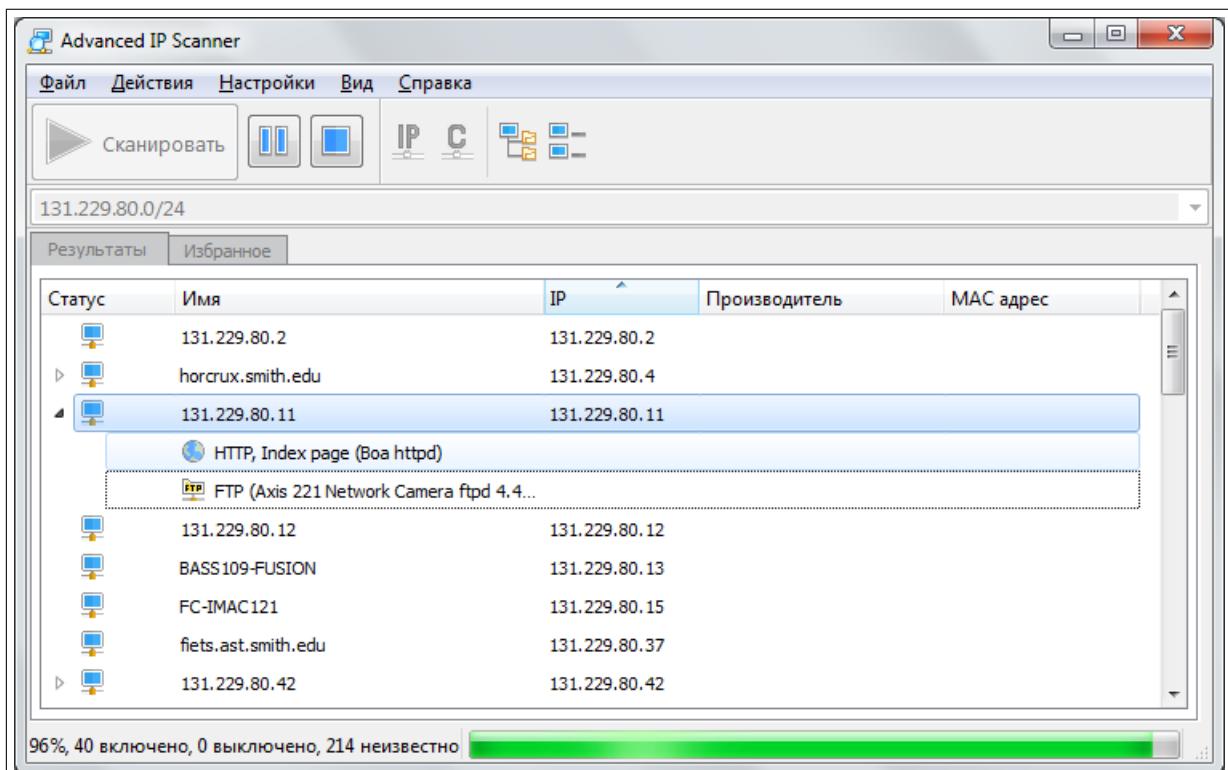
Перед поиском камер рекомендуется поставить опцию «Высокая точность сканирования» в разделе «Производительность», а также оставить только «HTTP» во вкладке «Ресурсы».

Характеристика ресурса может прямо содержать надпись «IP Camera» (изобр. 9) или содержать имя производителя, например, AXIS (изобр. 10).

¹⁵<http://www.advanced-ip-scanner.com/ru/>



Изображение 9 — Advanced IP Scanner

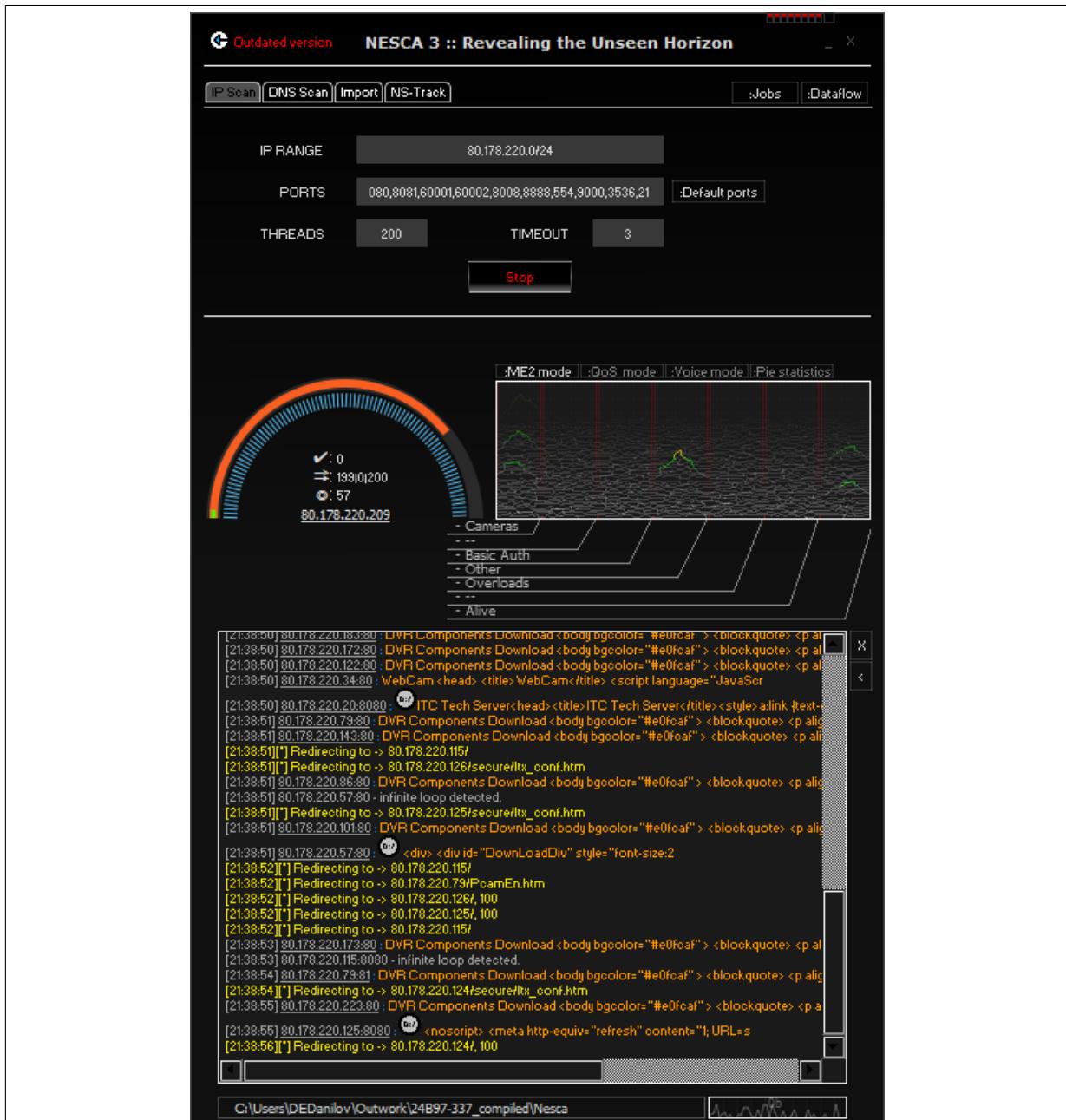


Изображение 10 — Advanced IP Scanner

3.2.6. Nesca

Nesca – один из самых известных «элитных» самописных сканеров, созданный для командной работы по сканированию Сети в поисках

различных устройств. Обладает пафосным «хакерским» графическим интерфейсом (изобр. 11). Часть функционала на данный момент не реализована, однако, программа позволяет удобно и быстро сканировать любые диапазоны адресов (обычные и CIDR), а также диапазоны доменных имён (DNS-режим, подробнее в do_not_read.txt), задавая при этом количество потоков, таймаут и проверяемые порты. Найденные сервисы программы также пытается пробрутьть, подбирая логин и пароль.



Изображение 11 — Nesca

Для сканирования в предыдущих версиях программы требовался личный ключ, который позволял включиться в сообщество Nesca и посыпать результаты на сервер. В последних версиях для отключения

проверки по ключу можно перейти на вкладку *NS-Track* и снять галку *Send results to public NescaDatabase*.

Доступен старый репозиторий¹⁶ исходного кода программы и актуальный¹⁷.

Ссылка на скомпилированную под Windows версию 24D87-801¹⁸, пароль 24D87-801.

3.2.7. RouterScan

Программа Router Scan была создана на форуме Antichat¹⁹ для поиска и определения роутеров в Сети, а также для извлечения из них системной информации и получения доступа, но при этом также определяются и многие DVR/NVR устройства. Получение информации происходит по двум возможным путям: программа попытается подобрать пару логин/пароль к маршрутизатору из списка стандартных паролей, в результате чего получит доступ. Также есть возможность использовать неразрушающие уязвимости (или баги) для конкретной модели маршрутизатора, позволяющие получить необходимую информацию и/или обойти процесс авторизации. На основе собранных данных энтузиастами собрана карта роутеров²⁰ с SSID и паролями.

Актуальная версия – 2.53, скачивать рекомендуется с официального сайта²¹, пароль Stas'M Corp.. Исходный код самой программы закрыт, открыты исходники модулей для эксплуатации уязвимостей.

¹⁶<https://bitbucket.org/emopidor/nesca/>

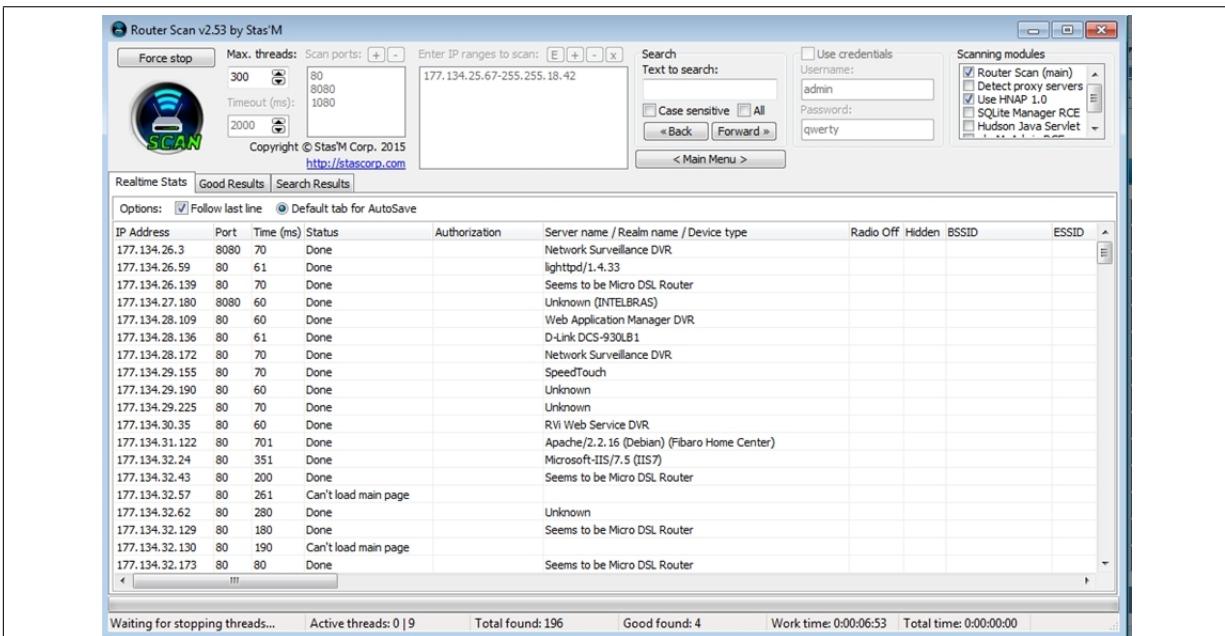
¹⁷<https://bitbucket.org/cora32/nesca>

¹⁸https://mega.nz/#!yZV3UDpY!6D5k-Dd1amF0i_rzIhFM-WU7cdN3pxR2mwsYiIqedtU

¹⁹<https://forum.antichat.ru/>

²⁰ <http://3wifi.stascorp.com/>

²¹<http://stascorp.com/load/1-1-0-56>



Изображение 12 — Router Scan

3.2.8. Другие инструменты

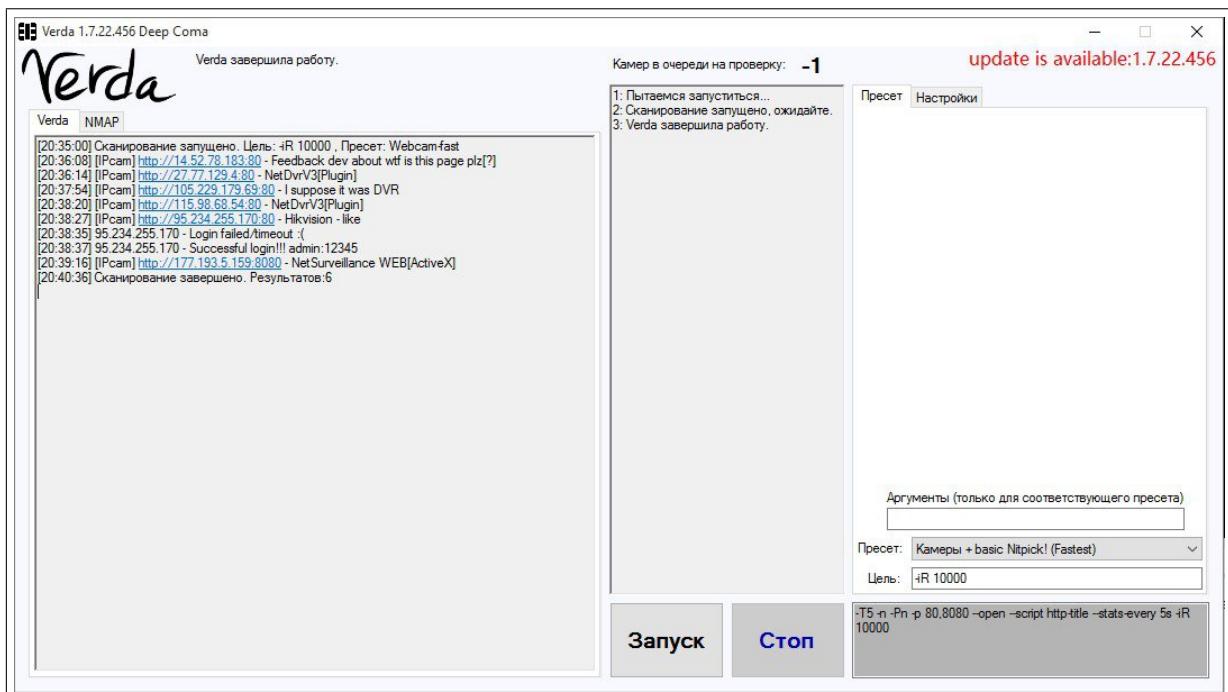
Существуют специализированные утилиты для поиска камер в локальной сети. Как правило, они создаются производителями конкретно для своих камер. Пример: SADP IP-finder (Search Active Device Protocol)²² – утилита для обнаружения, настройки и сброса пароля устройств Hikvision (только для локальной сети).

Из самописных утилит для поиска камер также можно выделить **Verda** – графическая надстройка над Nmap (изобр. 13) (необходим также .Net), определяющая камеры по шаблонам заголовков и адресов, а также посылающая запросы на хосты для уточнения информации. На 5.2016 доступна версия 1.7.32.249²³. Открыт исходный код на Github²⁴. Из минусов следует отметить отсылку программой отчётов о найденных результатах на сайт автора.

²²<http://www.hikvision.msk.ru/index/download/0-14>

²³<http://verda-dl.zz.mu/>

²⁴<https://github.com/sedmoy/verda-v1>



Изображение 13 — Verda

3.3. Онлайн-софт

3.3.1. Онлайн-базы камер

Ниже в таблице приведены ссылки на информационные ресурсы с базами онлайн-камер. Как правило, доступен и просмотр камеры онлайн. Информация действительна на 12.2015.

Таблица 2 — Базы онлайн-камер

| Ссылка | Описание |
|-------------------------------|---|
| Insecam ²⁵ | Каталог камер с публичным доступом, категории по странам и местоположению. Доступно около 20000 камер. |
| EarthCam ²⁶ | Популярный сервис для просмотра камер, имеются возможности расширенного поиска. |
| Camscape ²⁷ | Простой сайт-база камер с минимальным описанием и категоризацией по географическому положению. Доступно около 1400 камер. |
| AtenLabs Camwar ²⁸ | Сборник камер с тривиальным интерфейсом для их переключения, большая часть базы недействительна. |

Продолжение на следующей странице

²⁵<http://www.insecam.org/>

²⁶<http://www.earthcam.com/>

²⁷<http://www.camscape.com/>

²⁸<http://www.atenlabs.com/camwar/index.php>

Таблица 2 – Продолжение

| Ссылка | Описание |
|---|--|
| goandroam ²⁹ | Простой сервис просмотра камер с возможностью комментирования для зарегистрированных пользователей. Доступна возможность поиска камер по географическому положению/близости. |
| World Wide Livecams ³⁰ | Простой сервис с базой адресов камер с географической информацией и сохранёнными скриншотами. Доступно около 1300 камер. |
| AMOS (the archive of many outdoor scenes) ³¹ | Научный проект по сбору и исследованию изображений камер по всему миру. Доступна история снимков и их архивы, географическая информация и теги, однако, прямых трансляций нет. |
| ip Cams Live ³² | Сайт производителя одноимённого софта с трансляциями в различных форматах. Доступно около 600 камер. |
| mjpeg.net ³³ | Сервис для хранения камер со скриншотами и описанием, есть возможность определения географического положения и ближайших камер. Заброшен с 2010 года. Доступно около 6000 камер. По состоянию на 09.2016 недоступен, вместо него вирусные страницы. |
| tvway.ru ³⁴ | Русскоязычный каталог камер в разных точках мира, есть теги по географическому положению и открывающимся видам. |
| TV Joy ³⁵ | Русскоязычный каталог камер в разных точках мира, есть категоризация по открывающимся видам. Заброшен с 2014 года. |
| webcamplaza ³⁶ | Проработанный каталог камер с различными категориями |
| Opentopia ³⁷ | Каталог открытых камер с категоризацией, возможностью просмотра в различных режимах, комментариями. Хранятся скриншоты за 5, 8, 11, 14 часов назад. |

²⁹<http://www.goandroam.com/>

³⁰<http://camelize.info/>

³¹<http://amosweb.cse.wustl.edu/>

³²<http://www.ipcams.ch/>

³³<http://www.mjpeg.net/>

³⁴<http://tvway.ru/>

³⁵<http://tvjoy.ru/>

³⁶<http://www.webcamplaza.net/>

³⁷<http://www.opentopia.com/>

3.3.2. Google Search

Процесс поиска в Google достаточно тривиален (необходимо лишь напомнить, что при частых запросах появляется капча). Приведённые ниже шаблоны поиска (*dorks*) также могут быть использованы в любой другой индексирующей системе в соответствующей для неё нотации или для ручного поиска при наличии заголовков/текстов страниц (полученных с помощью софта).

Разумеется, нижеуказанные шаблоны не исчерпывают все возможные камеры – они лишь отражают наиболее часто искомые и доступные в данное время (актуально на 12.2015). При желании можно провести анализ рынка онлайн-камер, выявив новые/приобретающие популярность, а затем, пользуясь справочниками ссылок (см. раздел Онлайн-базы камер) и другими материалами (возможно, руководствами по конкретной модели или демо-камерами), подобрать шаблон, не используемый никем ранее, что гарантирует более высокую вероятность нахождения не попадавшихся другим камер.

Пояснение по операторам поиска:

intitle: – поиск подстроки в заголовке страницы (тег <title>);

inurl: – поиск подстроки в адресе страницы (URL, путь);

intext: – поиск подстроки в тексте страницы (видимая часть);

all – ставится перед указанными выше выражениями, после этого поиск будет производиться по каждой подстроке;

" (двойные кавычки) – означают поиск по целому выражению, если оно состоит из нескольких подстрок; подстроку без пробелов нет смысла окружать кавычками;

- (минус) – ставится перед указанными выше модификаторами запроса, инвертирует результат (показывает страницы, НЕ содержащие подстроки).

Active WebCam Page

"Active WebCam Page"

AXIS

inurl:axis-cgi
inurl:axis-cgi/jpg
inurl:axis-cgi/mjpg
inurl:axis-cgi/mjpg/video.swf
inurl:mjpg/video.mjpg
inurl:mjpg/video.cgi
inurl:video.cgi?resolution=
inurl:indexFrame.shtml "AXIS Video Server"
inurl:view/view.shtml AXIS
inurl:view/index.shtml
inurl:view/indexFrame.shtml
"Live web imaging unleashed"
intitle:"Live View / - AXIS <номер модели камеры>"
<номер модели камеры> можно не вписывать, используется для уточнения. Примеры: 205, 206, 207, 211, M1114, P5534-E, etc.
inurl:axiscam.net AXIS
inurl:axiscam.net intitle:Camera
inurl:axiscam.net "Live view"
inurl:dyndns.org AXIS
"Live View is the default page"
inurl:view/ctl.shtml
inurl:netw_tcp.shtml
inurl:/mpeg4/video.sdp
inurl:cgi-bin/push.html
inurl:"axis-cgi/motion/motiondata.cgi"
intitle:axis intitle:"video server"

Bironsoft

intitle:"Bironsoft WebCam" -4.0 -serial -ask -crack -software -a -the
-build -download -v4 -3.01 -numrange:1-10000

Canon

inurl:lvappl
inurl:sample/LvAppl
intitle:liveapplet inurl:LvAppl
inurl:sample/Others/SvrPush.htm
inurl:viewer/live/en/live.html

Cisco (Linksys)

inurl:"/main.cgi?next_file=index.htm"
camera linksys inurl:main.cgi
intitle:"Linksys Web Camera" "ver"
inurl:/img/vr.htm

Convision

inurl:pictype=jpegserverpush

D-Link

inurl:"top.htm?Currenttime"

EvoCam

intitle:" EvoCam" inurl:" webcam.html"

FlexWATCH

inurl:viewash.html
inurl:/app/idxas.html
inurl:/app/sample/ab1.asp
intitle:flexwatch intext:"Home page ver"

i-Catcher

intitle:"i-Catcher Console - Web Monitor"
intitle:"i-Catcher Console - Web Playback"

INTELLINET

intitle:"::::: INTELLINET IP Camera Homepage :::::"
inurl:/main_activex.asp
inurl:/main_applet.asp

IQeye

intitle:"IQeye302 | IQeye303 | IQeye601 | IQeye602 | IQeye603"
intitle:"Live Images"
inurl:"appletvid.html"

MOBOTIX

inurl:cgi-bin/guestimage.html
inurl:control/userimage.html
intext:"MOBOTIX" inurl:"userimage.html"
"Kamerainformationen anzeigen"
(intitle:MOBOTIX intitle:PDAS) | (intitle:MOBOTIX intitle:Seiten) |
(inurl:/pda/index.html +camera)
inurl:dyndns.org MOBOTIX

NetCam

liveapplet
intitle:"netcam live image"
Configuration "Pop-up Live Image"
Display Cameras intitle:"Express6 Live Image"

NuSpectra

inurl:snap.html +intitle:"SiteCam"
intitle:"SiteCam Video Snapshot"

Panasonic

inurl:/cam_portal.cgi
"ViewerFrame?Mode="
inurl:ViewerFrame?Mode=Motion
-inurl:htm -inurl:html inurl:ViewerFrame
inurl:MultiCameraFrame?Mode=
inurl:MultiCameraFrame?Mode=Motion
site:.viewnetcam.com -www.viewnetcam.com
allintitle:Network Camera NetworkCamera
inurl:portal_main.html intitle:Panasonic
inurl:CgiStart intitle:Camera
intitle:"WJ-NT104 Main"
inurl:".viewnetcam.com"

QuickCam

intitle:"QuickCamPro WebCam" inurl:webcam

Sony

inurl:home/homeJ.html
intitle:snc-rz30
intitle:snc-cs3 inurl:home/
intitle:"sony network camera snc-p1"

SupervisionCam

intitle:"supervisioncam protocol"

TOSHIBA

"TOSHIBA Network Camera - User Login"
intitle:toshiba inurl:user_single_view.htm
inurl:/user_view_M.htm

VisionGS

intitle:"VisionGS Webcam Software"

webcam XP

"Powered by webcamXP"
intitle:my webcamXP server!
"powered by webcamXP" "Pro|Broadcast"
inurl:"pocketpc?camnum=1"

WebGate

"Webthru User Login"

Другое

-inurl:htm -inurl:html inurl:webcam.php
inurl:Remote/index.php3
inurl:/Aview.htm
inurl:chconv?CH=
inurl:Ctl/index.htm?Cus
intitle:"SiteZAP WebCam Control"
inurl:webcam.asp
inurl:ViewerFrame?Mode=
inurl:ViewerFrame?Mode=Refresh
inurl:dyndns intitle:Network Camera
inurl:toolam.html
inurl:Camera.aspx?ServerID
inurl:next_file=main_fs.htm
"Live video"

3.3.3. Shodan

Shodan³⁸ - сервис для поиска различных устройств, подключённых к сети. Запущен в 2009 году. Для получения результатов больше одной страницы требуется регистрация, для работы с большим количеством данных - оплата.

По состоянию на январь 2017, запросы для поиска онлайн-камер являются наиболее популярными в поисковике.

Одним из преимуществ Shodan перед Google является возможность поиска по заголовкам ответа, т.е. данным сервера, авторизационного запроса, специфичных служебных данных. Таким образом, становится легко отсеять устройства, использующие специфичные сервера для видеотрансляции.

³⁸<https://shodan.io>

Другим из преимуществ является возможность поиска с фильтрами (указание нестандартного порта, страны, города). Для использования этой возможности необходима регистрация, также необходимо учесть, что Shodan в отношении специфичных портов уступает Google в покрытии устройств (последний может проиндексировать и запомнить ссылку на камеру с портом, который никогда не будет обрабатываться краулерами Shodan в силу нестандартности). Приведённые ниже шаблоны поиска (dorks) частично пересекаются с теми, что могут быть использованы в Google, но из-за более широких возможностей индексации некоторые в Google не могут быть использованы.

Пояснение по операторам поиска:

Поисковые фильтры, в терминологии Shodan, это специальные ключевые слова для поиска в метаданных ответа.

hasScreenshot:true – фильтр для поиска результата со скриншотами (применим не только к камерам, также к VNC, RTSP, X Windows, для поиска только камер со скриншотами можно указать протокол http);

port – указание проиндексированного порта устройства;

city – указание города;

country – указание двухбуквенного кода страны;

title – поиск в заголовке страницы;

html – поиск в HTML-ответе сервера;

" (двойные кавычки) – означают поиск по целому выражению, если оно состоит из нескольких подстрок; подстроку без пробелов нет смысла окружать кавычками;

- (минус) – ставится перед фильтрами или строками, исключая их из результата.

Любое проиндексированное устройство, имеющее скриншот на веб-интерфейсе

hasScreenshot:true http

AXIS

axis camera Content-Length: 695

Bosch

Server: VCS-VideoJet-Webserver

Canon

Server: VB100

Cisco

title:'+tm01+' title:"WVC210 Wireless-G PTZ Internet Camera with Audio"

D-Link

title:"DCS-5300G"Server: D-Link Internet Camera D-Link Internet Camera, 200 OK title:"DCS" title:"IP camera"

Hikvision

hikvision Content-Length: 1341

Hipcam

Server: Hipcam RealServer/V1.0

i-Catcher

Server: i-Catcher Console

Lorex

LNE3003 Wireless IP Camera

MayGion

maygion

MJPEG Streamer

title:"MJPEG-Streamer"

Netwave

Netwave IP Camera

Panasonic

Server: U S Software Web

P2P Network Camera

wificam

Samsung

title:"Web Viewer for Samsung DVR" Content-Length: 2524

StarDor NetCam XL

title:"NetCamXL"

TP-LINK

title:"IP CAMERA Viewer" Content-Length: 703

TRENDnet

Auther: Steven Wu

Vivotek

Vivotek Network Camera -401

VMAX Web Viewer

title:"Login cgicc form"

webcamXP/webcam7

webcamXP webcam 7

Другое

Server: SQ-WEBCAM

IPCamera_Logo

"webcamlast-modified"

Android Webcam Server -Authenticate

yawcam

Boa ipcam

imaginek ipcam

ADH-web

AbelCam

Brickcom

4. Получение доступа

4.1. Логины и пароли

4.1.1. Онлайн-базы логинов, паролей и URL

Ниже в таблице приведены ссылки на информационные ресурсы по моделям камер и доступу к ним. Информация действительна на 12.2015.

Таблица 3 — Онлайн-базы реквизитов камер

| Ссылка | Описание |
|---------------------------|---|
| CAMURL.RU ³⁹ | Справочник ссылок доступа для камер по поставщику/модели |
| ISPYCONNECT ⁴⁰ | Справочник ссылок доступа для камер по модели |
| Art-Of-War ⁴¹ | Список паролей по умолчанию для оборудования от различных поставщиков |
| zee:cure ⁴² | Пароли по умолчанию и дефолтные IP для разных типов камер |

4.1.2. Статистика

В следующих колонках отражены наиболее часто используемые для сетевых устройств логины и пароли (по данным Nesca, 12.2015).

³⁹<https://www.camurl.ru/>

⁴⁰<http://www.ispyconnect.com/sources.aspx>

⁴¹<http://art-of-war.ru/0500-it/0600-hardware/passwords>

⁴²<http://zeecure.com/free-cctv-and-security-tools/complete-list-of-every-ip-camera-default-username-password-and-ip-address/>

Логины:

| | | |
|---------|---------------|----------|
| admin | test | telecom |
| root | ftp | dreambox |
| 123123 | 1234 | master |
| 123456 | administrator | Admin |
| 12345 | qwerty | guest |
| cisco | recovery | backup |
| super | Polycom | cgadmin |
| meinsm | system | 0000 |
| monitor | naadmin | 1111 |

Пароли:

| | | |
|----------|-----------|---------------|
| root | test | 0000 |
| admin | sysadm | 000000 |
| password | admin123 | master |
| 123456 | Admin | 12345678 |
| 1234 | 123321 | 666666 |
| 12345 | 12344321 | 123123123 |
| ADMIN | toor | 123454321 |
| cisco | qwerty123 | 0123456789 |
| ftp | 1q2w3e4r | qqqqqq |
| ROOT | 987654321 | administrator |
| 123123 | system | sys |
| pass | telecom | guest |
| passwd | dreambox | backup |
| qwerty | 111111 | fujiyama |
| meinsm | 1111 | super |
| monitor | 654321 | P@ssw0rd |
| user | !@#\$%^ | passw0rd |

4.1.3. Логины и пароли по умолчанию

В следующей таблице отражены дефолтные (по умолчанию) логины/пароли для доступа к некоторым видам камер. Выделенные полужирным названия являются ссылками на описания визуальных интерфейсов камер в разделе Разнообразные плагины.

Таблица 4 — Логины/пароли к камерам по умолчанию

| Название | Логин | Пароль | Примечание |
|------------------|----------------|---------------|--|
| ACTi | admin Admin | 123456 | |
| Arecont Vision | (нет) | (нет) | |
| Avigilon | admin | admin | |
| Axis | root | pass | У новых моделей нет пароля по умолчанию. Пароль задаётся во время первой настройки |
| Basler | admin | admin | |
| Bosch | (нет) | (нет) | |
| Brickcom | admin | admin | |
| Cisco | (нет) | (нет) | Нет пароля по умолчанию. Пароль задаётся во время первой настройки |
| | admin | 123456 | IE. Доступна выгрузка записей |
| Dahua | admin | admin | |
| Digital Watchdog | admin | admin | |
| DRS | admin | 1234 | |
| DVTel | Admin | 1234 | |
| | admin | (нет) | IE. Вход с выставленным типом сети «Wan». Доступна выгрузка записей |
| DynaColor | Admin | 1234 | |
| FLIR | admin | fliradmin | |
| Foscam | admin | (нет) | |
| GeoVision | admin | admin | |
| Grandstream | admin | admin | |

Продолжение на следующей странице

Таблица 4 – Продолжение

| Название | Логин | Пароль | Примечание |
|---------------------|--------------|----------------|---|
| | admin | 12345 | Через встроенный софт или браузер после установки плагина из инсталлятора |
| Honeywell | admin | 1234 | |
| | root | system | |
| IPX-DDK | root | admin Admin | |
| JVC | admin | jvc | |
| Mobotix | admin | meism | Пароль по умолчанию встречается чрезвычайно редко |
| | admin | (нет) | |
| | admin | (нет) | IE |
| Panasonic | admin | 12345 | |
| Pelco Sarix | admin | admin | |
| Pixord | admin | admin | |
| Samsung Electronics | root | root | |
| | admin | 4321 | |
| Samsung Techwin | admin | 111111 | Старая модель |
| | admin | 4321 | Новая модель |
| Sanyo | admin | admin | |
| Scallop | admin | password | |
| Sentry360 | admin | 1234 | Модель mini |
| | (нет) | (нет) | Модель pro |
| Sony | admin | admin | |
| Stardot | admin | admin | |
| Starvedia | admin | (нет) | |
| Trendnet | admin | admin | |
| Toshiba | root | ikwd | |
| Vacron | admin | (нет) | |
| VideoIQ | supervisor | supervisor | |
| Vivotek | root | (нет) | |
| Ubiquiti | ubnt | ubnt | |
| Wodsee | admin | (нет) | |

4.2. Инструменты

В данном разделе будут освещены особенности использования следующих инструментов для подбора логинов/паролей к камерам:

- Hydra
- Burp Suite
- Bruter
- hikka

Доработка раздела ожидается в следующей версии документа.

4.2.1. hikka

Инструмент для подбора паролей к камерам типа Hikvision. Интересен тем, что сохраняет найденные камеры в файл в таком виде, в котором можно затем вставить прямо в программу для просмотра (iVMS, см. подраздел Софт для камер)

Ссылка на GitHub для текущей версии⁴³ софта, для предыдущей⁴⁴ (более не поддерживается). Компилировать рекомендуется самому, предварительно установив дистрибутив языка программирования Go.

Принимает только список одиночных IP, брутит только по одному порту (по умолчанию 8000, возможно задать опцией **port**).

Для запуска в консоли рекомендуется следующая команда:

hikka -threads 100 -shoots screens/ -csv results.csv

где 100 – количество потоков сканирования, **screens/** – папка, в которую будут сохраняться скриншоты.

⁴³<https://github.com/superhacker777/hikka>

⁴⁴<https://github.com/superhacker777/ivms-bf>

5. Просмотр онлайн-камер

5.1. Форматы трансляции

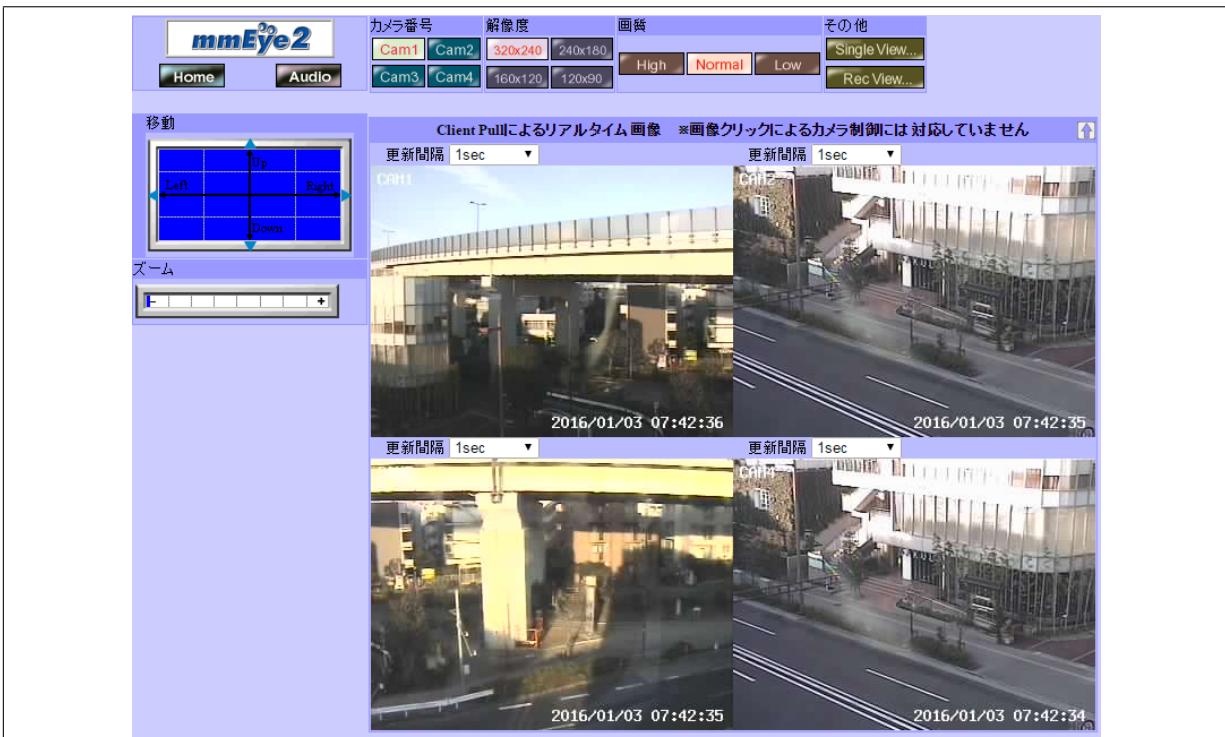
5.1.1. Обновление изображения

Самый простой формат трансляции с онлайн-камер – это отображение обновляющейся картинки. Реализаций такого механизма достаточно много, при этом зачастую трансляция может быть неотличима от передачи видео (при широком канале и частом обновлении картинки). Иногда же бывает наоборот – предлагаются фиксированные «большие» промежутки времени обновления картинки.

Примеры: MOBOTIX (изобр. 14), mmEye2 (изобр. 15).



Изображение 14 — MOBOTIX



Изображение 15 — mmEye2

5.1.2. Потоковое видео

Потоковое вещание, как правило, является основным каналом передачи аудиовидеотрансляции владельцу камеры. Оно может быть доступно как непосредственно с камеры, так и с видео-сервера, позволяющего транслировать видео множеству пользователей без потери производительности камеры.

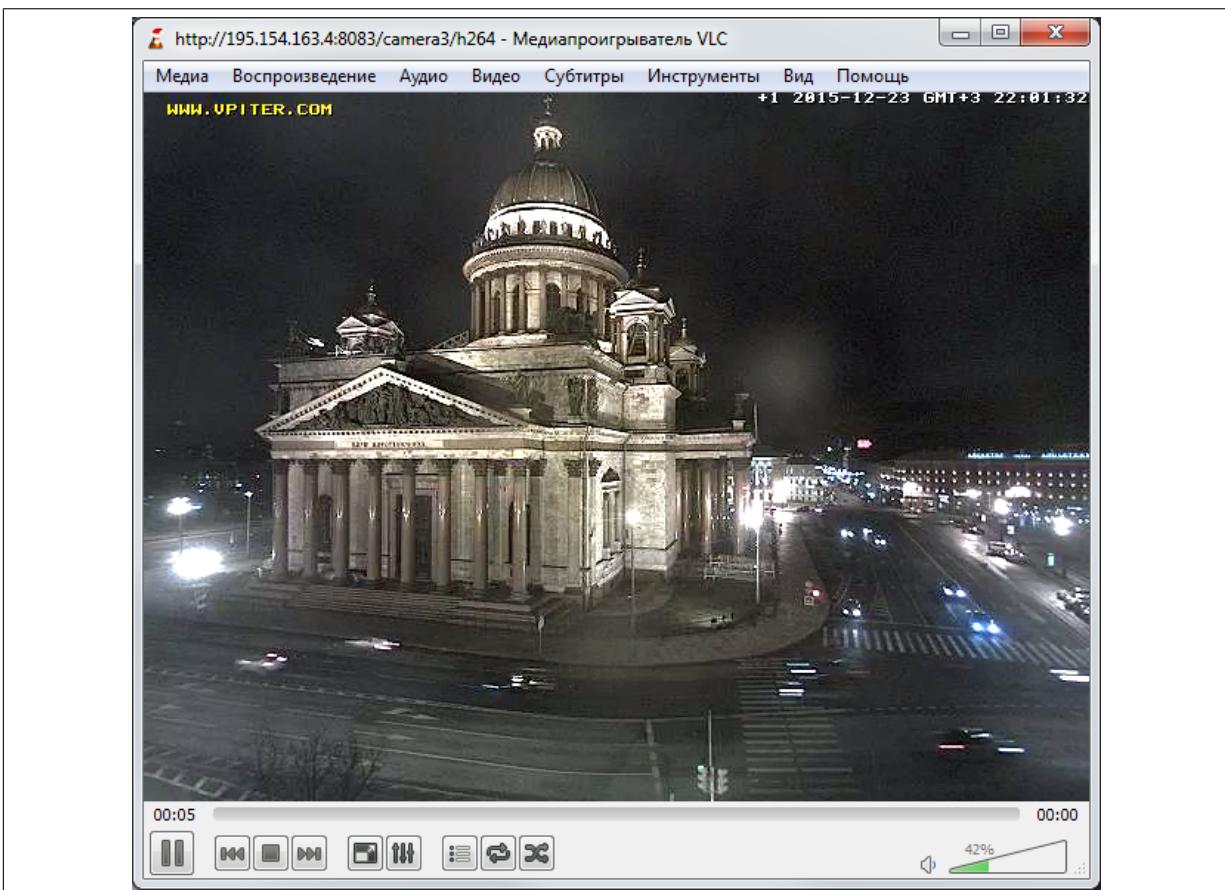
Доступ к каналу потокового вещания предоставляется по URL (см. раздел «Онлайн-базы логинов, паролей и URL»), которые можно определить для конкретной модели камеры или получить путём анализа трафика при воспроизведении такого видео в плеере на стороннем сайте.

Протоколом передачи обычно является RTSP. Примеры форматов: MPEG4, H.264.

Для просмотра потоковых трансляций рекомендуется VLC Player⁴⁵.

Пример: сервер трансляций онлайн-камер Санкт-Петербурга (изобр. 16)

⁴⁵<http://www.videolan.org/vlc/>



Изображение 16 — VLC-плеер

5.1.3. MJPEG

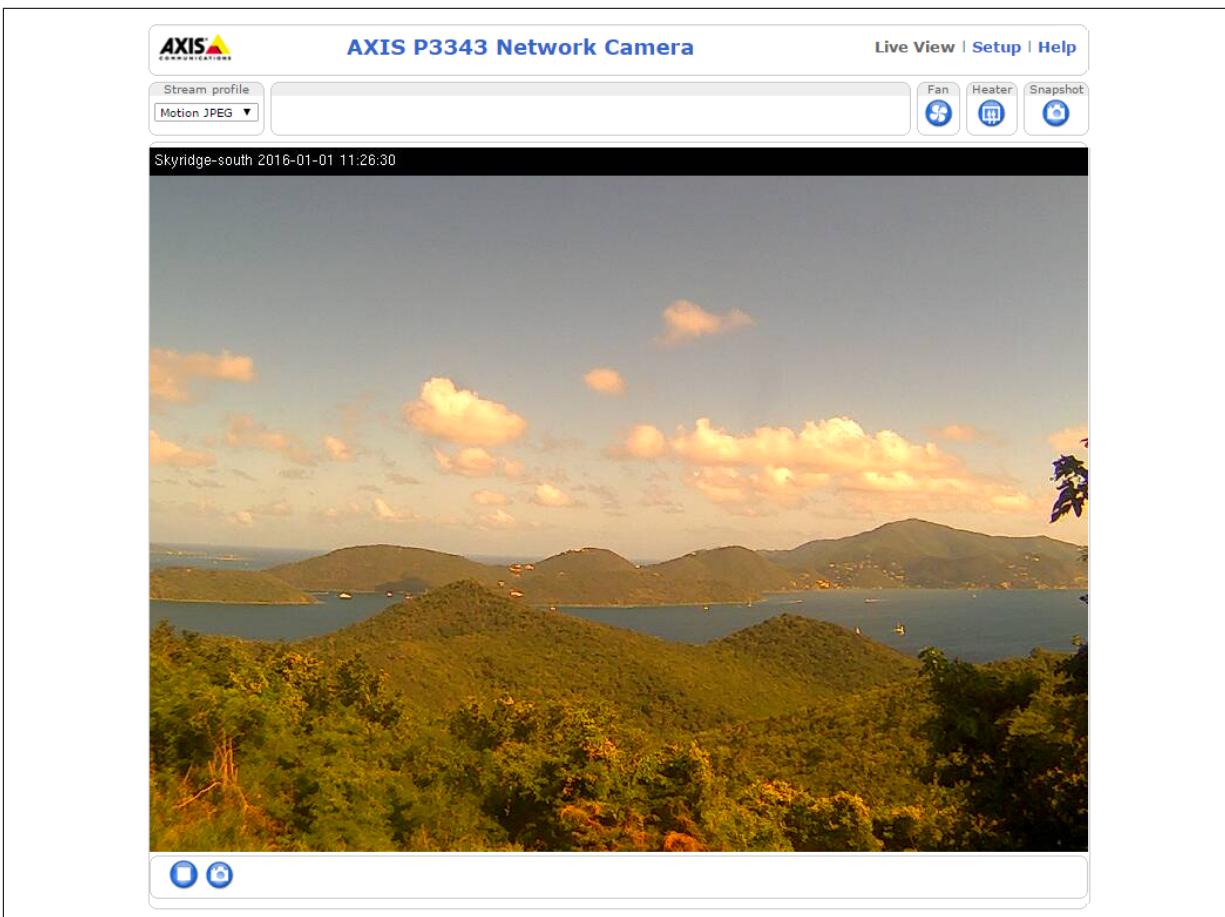
MJPEG (Motion JPEG) является, по сути, потоковой трансляцией. Отличие заключается в передаче в одном потоке одиночных полноценных JPEG-изображений, с которыми возможна дальнейшая работа. Каналы передачи: HTTP, RTSP.

Для работы с MJPEG в настоящее время не требуется дополнительный софт, основные браузеры его поддерживают.

Примеры: **AXIS** (изобр. 17, изобр. 18). Доступ к просмотру по умолчанию **не запаролен**.



Изображение 17 – AXIS с MJPEG-трансляцией, интерфейс 1



Изображение 18 – AXIS с MJPEG-трансляцией, интерфейс 2

5.2. Браузерные плагины

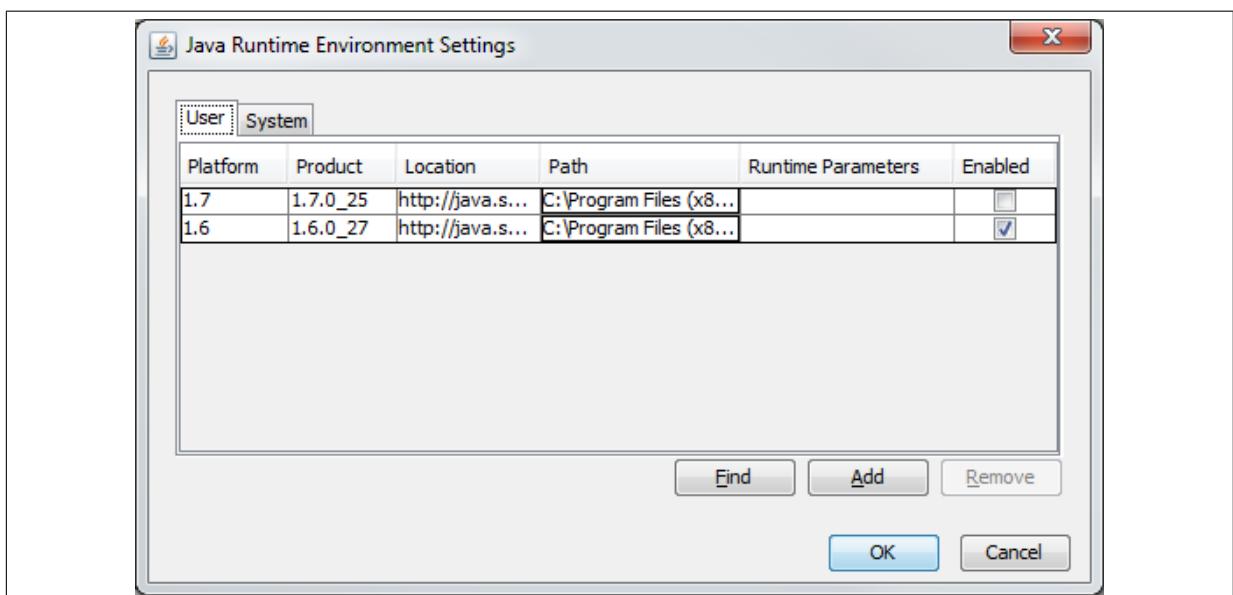
В этой секции будут рассмотрены варианты трансляции с камер через браузер. Для каждого вида приведена базовая информация, а

также примеры камер от различных производителей со скриншотами и описанием дефолтных реквизитов доступа (логины и пароли по умолчанию доступны в разделе Получение доступа).

Иногда при установке плагинов возможна и установка соответствующего софта вне браузера (например, при использовании ActiveX), но, как правило, специализированный софт для просмотра должен устанавливаться пользователем вручную. Список такого софта доступен в соответствующем подразделе Софт для камер.

5.2.1. Java-апплеты

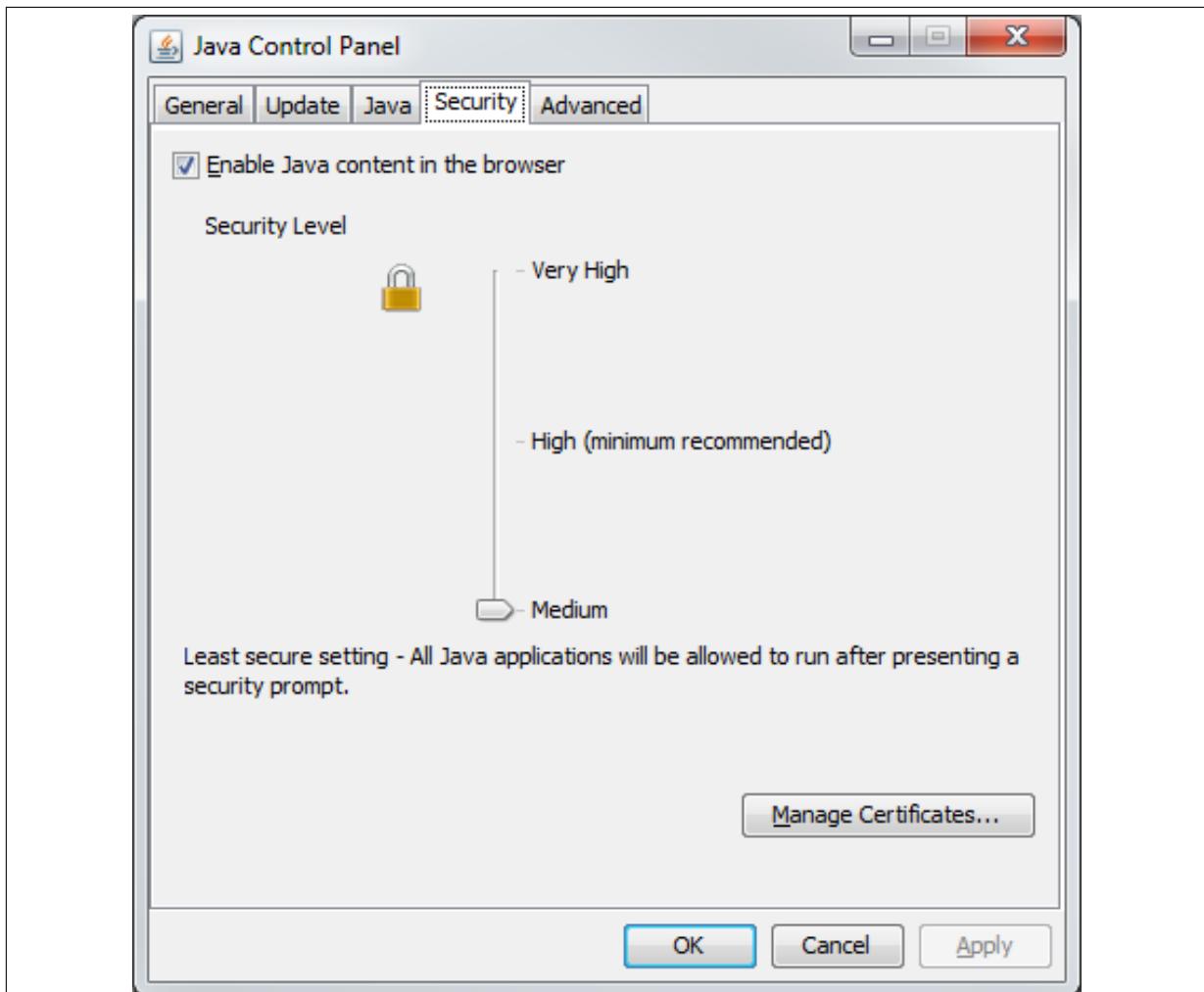
Java-апплеты – плагины, написанные на языке Java для выполнения в браузерах. Не поддерживаются в последних версиях Chrome, для Firefox необходим плагин. Для них необходима установленная среда JRE (JavaRuntime Environment). Следует отметить, что большинство апллетов требует Java версии 1.6.0, однако, на компьютере уже может быть установлена более поздняя версия. Узнать установленные версии и актуальную можно в панели управления Java: *Панель управления\Все элементы панели управления\Java*. Версии находятся во вкладке Java, кнопка View:



Изображение 19 — Список установленных версий Java

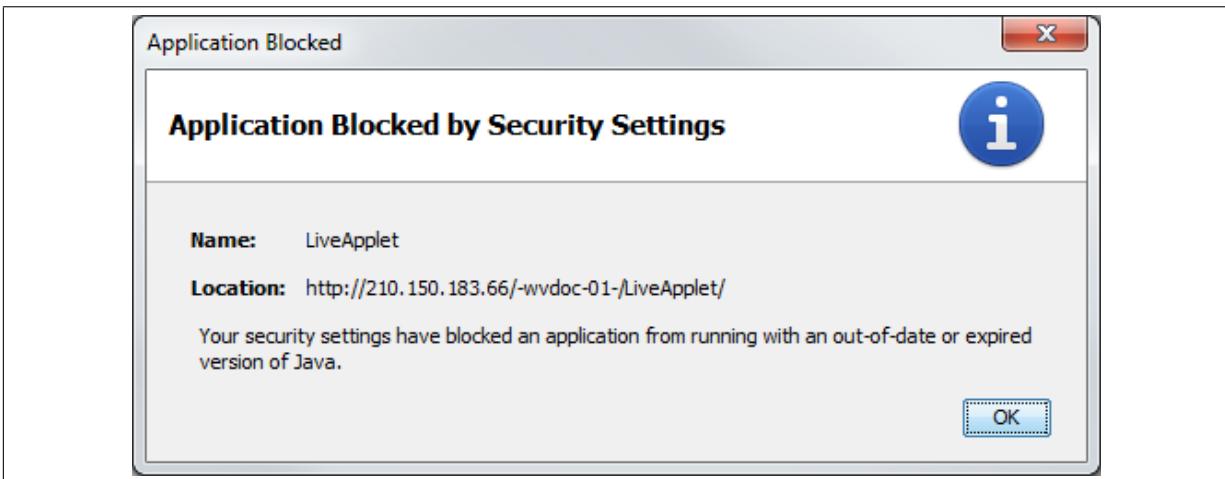
Включаем необходимую нам, но учитываем, что параметры безопасности определяются последней установленной версией. Переходим на вкладку Security. Если отображается окно настроек с бегунком (см. следующий скриншот), то версия Java ниже 1.8.0_20 и допускается установить средние (Medium) настройки безопасности, что нам и необходимо сделать. Если доступны только две радиокнопки High и Very

High, то среду выполнения (предположительно, «Java 8 ...») следует удалить через «Программы и компоненты».



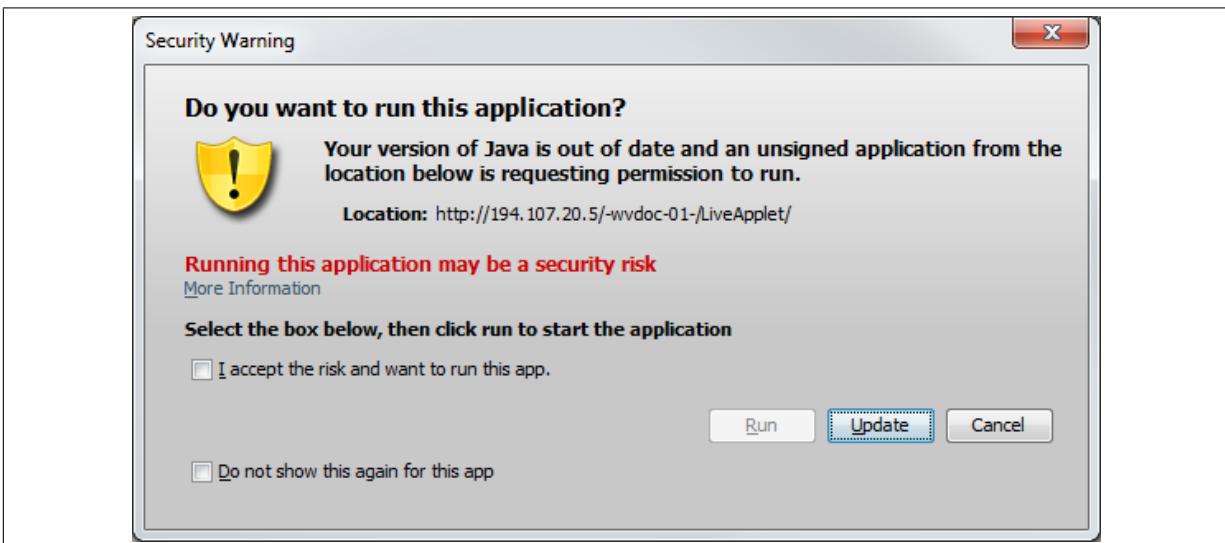
Изображение 20 — Настройки безопасности версии Java

Далее будут рассмотрены примеры ошибок при попытке просмотреть апплет, их анализ и решение проблем. Не рассматриваются ошибки вида «Этот плагин является уязвимым/опасным, вы должны его обновить», так как при них всегда предоставляется возможность запустить плагин.



Изображение 21 — Запуск блокирован из-за устаревшей Java

Версия Java подходит для выполнения апплета, но настройки безопасности не позволяют ей запуститься. Следует изменить настройки безопасности на Medium (см. выше).



Изображение 22 — Версия Java устарела

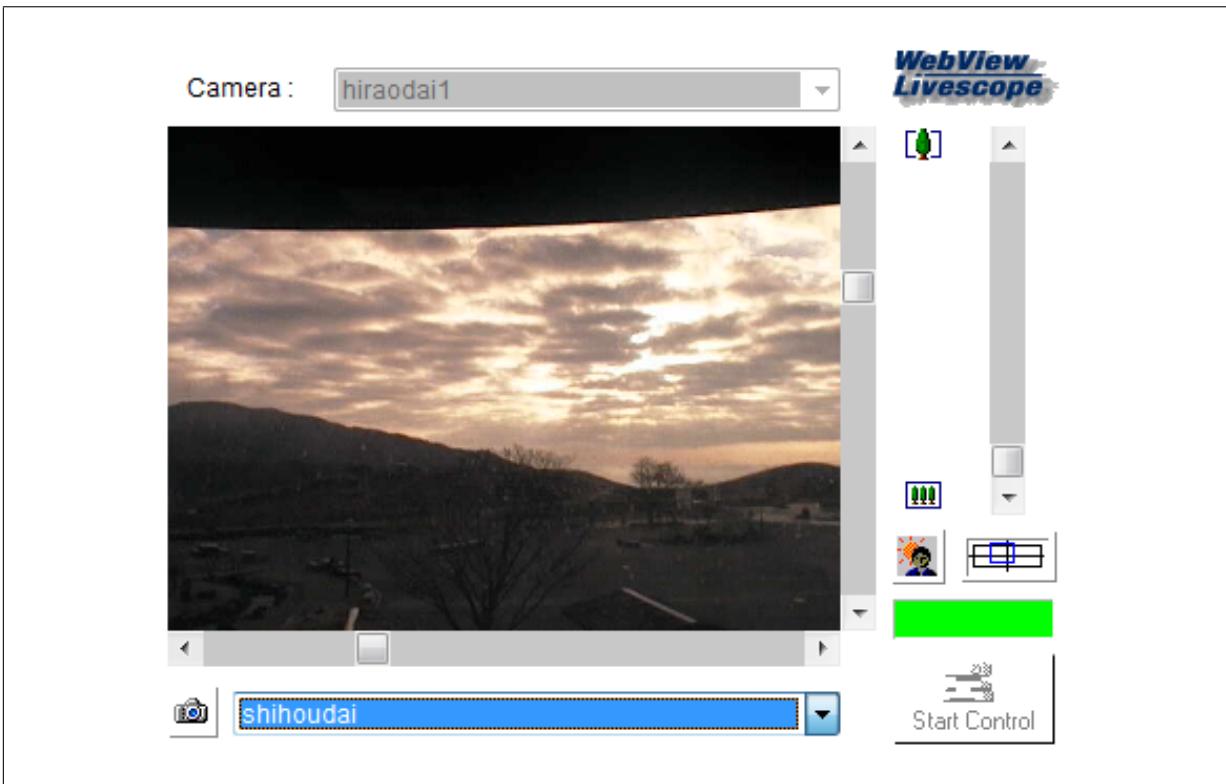
Версия Java подходит для выполнения апплета, просто требуется подтвердить согласие с рисками. Устанавливаем оба чекбокса, нажимаем Run.



Изображение 23 — Запуск блокирован из-за настроек безопасности Java

Настройки безопасности запрещают выполнение аплетов. Следует удалить текущую версию Java и поставить версию ниже (< 1.8.0_20).
Примеры:

- **Canon** (изобр. 24). В большом количестве встречается по Японии
- **IQinvision** (изобр. 25). по умолчанию используются аплеты Java, но доступен и ActiveX-интерфейс



Изображение 24 – Canon



Изображение 25 – IQinvision

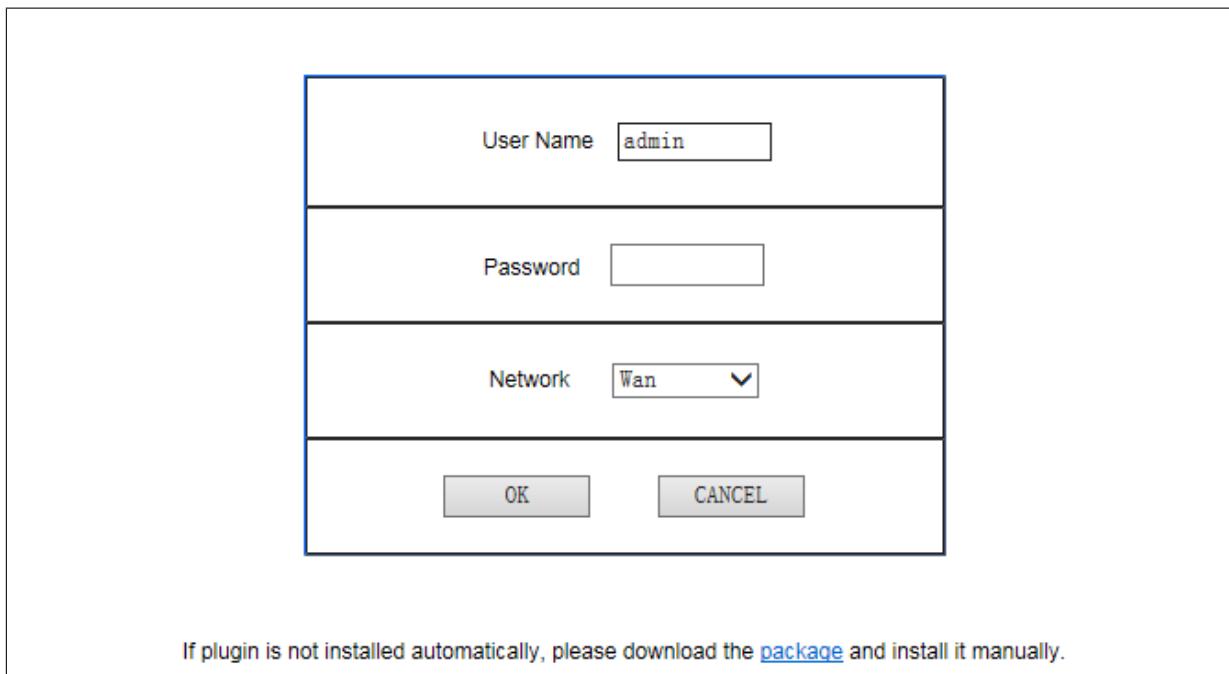
5.2.2. QuickTime Player

Реализует протокол передачи видео одноимённой технологии от Apple. Распространён как в интерфейсах непрофессиональных онлайн-камер, так и в виде альтернативного режима просмотра для камер AXIS. Для работы необходимы плагины.

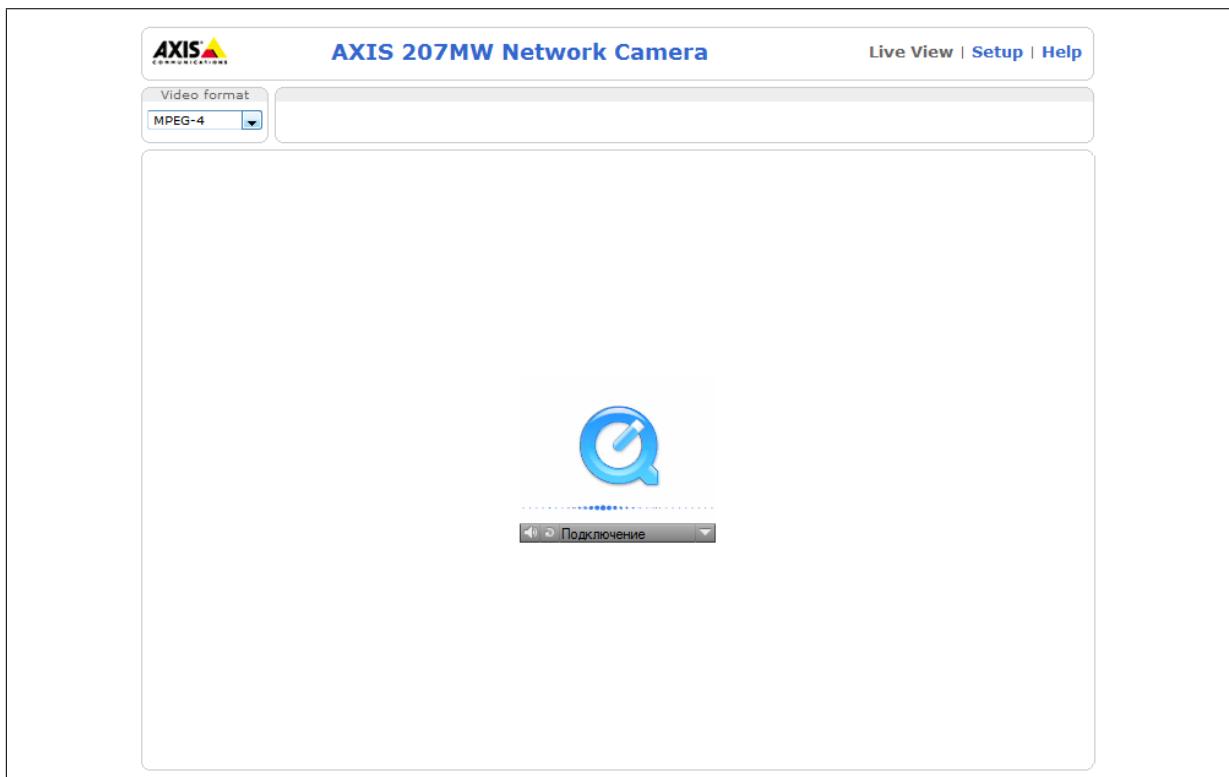
Примеры:

- **NetSurveillance** (изобр. 26). Дефолтный доступ: **admin** без пароля.

- **AXIS** (изобр. 27). Доступ к просмотру по умолчанию **не запаролен**.



Изображение 26 – NetSurveillance



Изображение 27 – AXIS с QuickTime

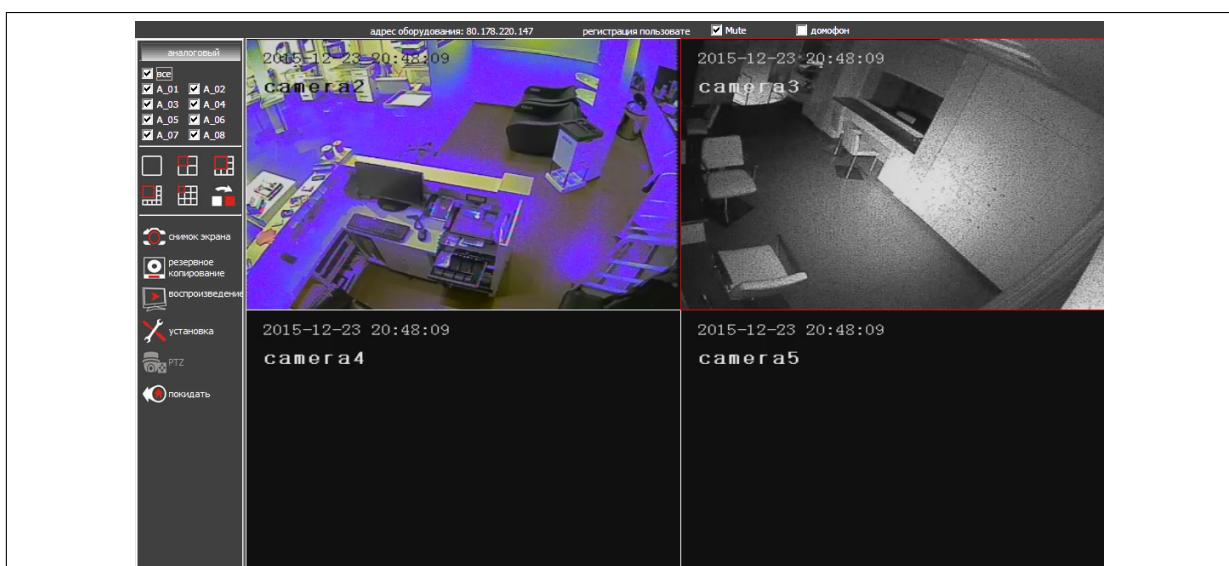
5.2.3. ActiveX

В данную категорию входит довольно большое количество самых разнообразных камер. ActiveX-компоненты предназначены для работы только в Internet Explorer, однако доступны плагины для эмуляции ActiveX в Firefox.

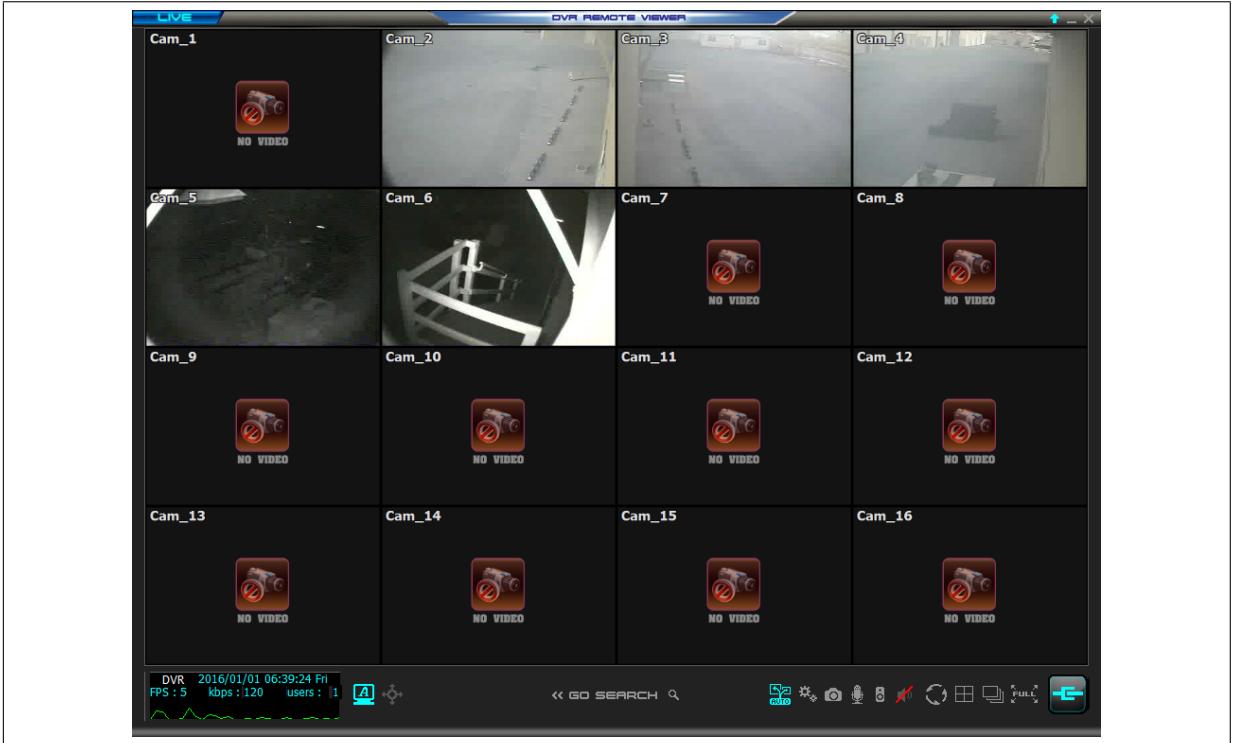
Для запуска плагина браузер скачивает архив вида ***.cab** (может быть локализован по исходному коду страницы) и устанавливает его содержимое в систему. Следует отметить, что в этом архиве иногда также находятся программы для просмотра конкретного вида камер, которые затем можно использовать отдельно от браузера, подключаясь к любой камере этого вида.

Примеры:

- **264 DVR** (изобр. 28)
- **DVR REMOTE VIEWER**. Дефолтный доступ: *Administrator* без пароля. Из cab-пакета с помощью ActiveX устанавливается клиентская программа, отображающая подробную информацию и позволяющая настраивать отображение различных каналов, вывод звука (изобр. 29)
- **DVR WebViewer** (изобр. 30)
- **DVR remote management system (TLNetDvr)**. Дефолтный доступ: *admin* без пароля, вход с выставленным типом сети «Wan» (изобр. 31, изобр. 32)
- **NetDvrV3**. Дефолтный доступ: *admin* без пароля. Интерфейс клиента интересен возможностями подключения камер по списку IP и их поиска (изобр. 33, изобр. 34)



Изображение 28 — 264 DVR



Изображение 29 — Окно программы DVR REMOTE VIEWER



Изображение 30 — DVR WebViewer

User Name

Password

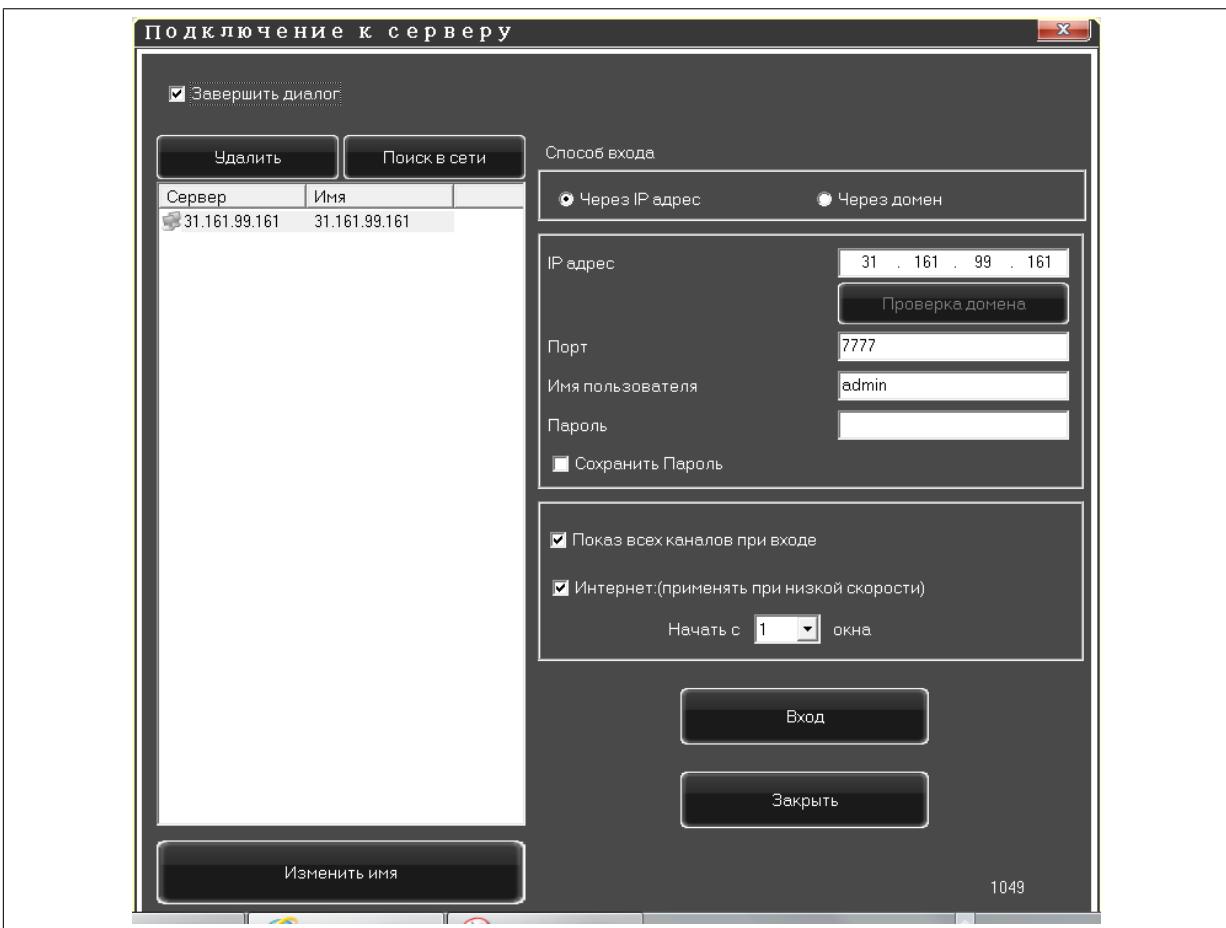
Network

If plugin is not installed automatically, please download the [package](#) and install it manually.

Изображение 31 — Окно авторизации TLNetDvr



Изображение 32 — Основной интерфейс TLNetDvr



Изображение 33 – Окно подключения камеры NetDvrV3



Изображение 34 – Основной интерфейс NetDvrV3

5.2.4. Разнообразные плагины

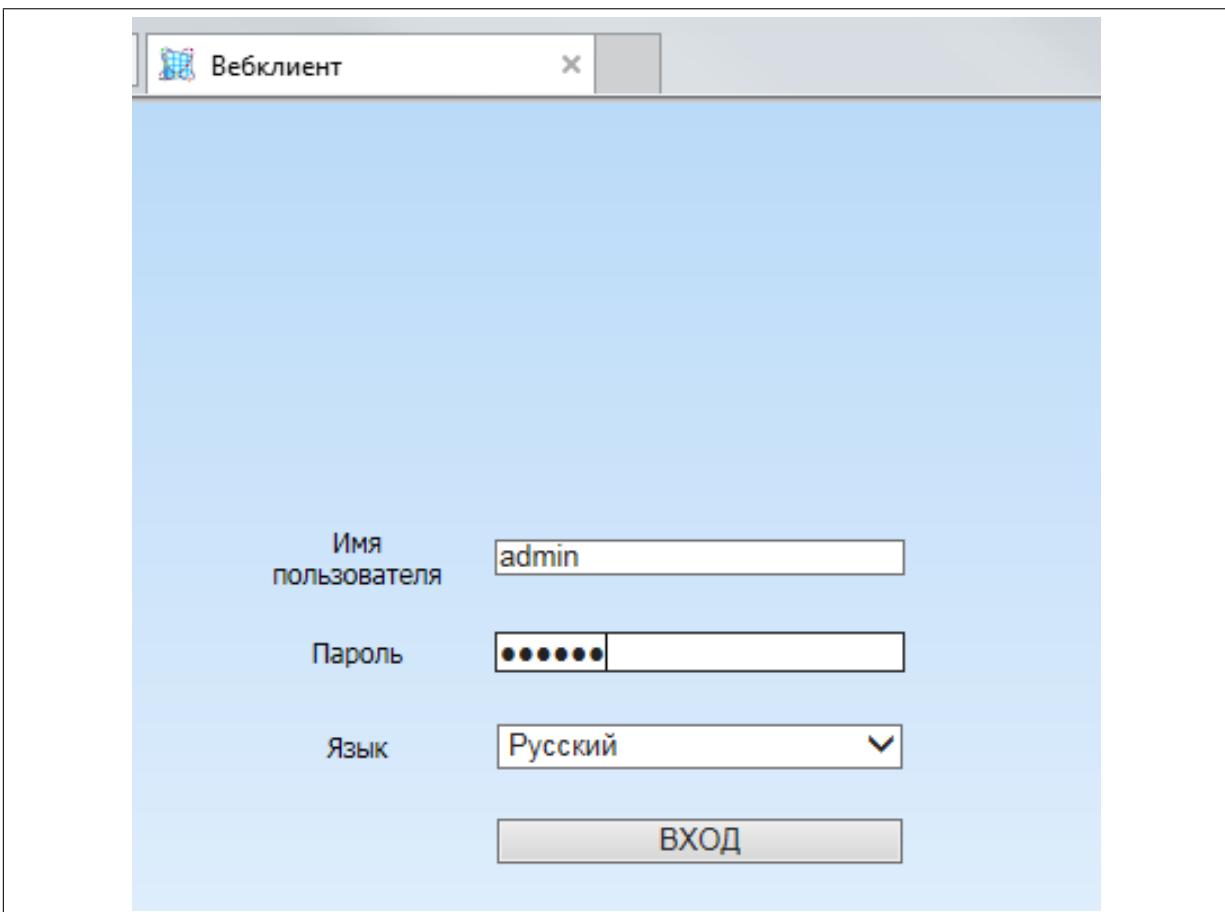
Существует масса других различных плагинов для просмотра и управления камерами, для которых не нашлось места в данном руководстве. Всегда важно помнить, что плагины устаревают, значит, не на всех браузерах и не во всех их версиях определённый плагин может работать.

Ниже приведён список некоторых системных названий плагинов, не упомянутых в руководстве.

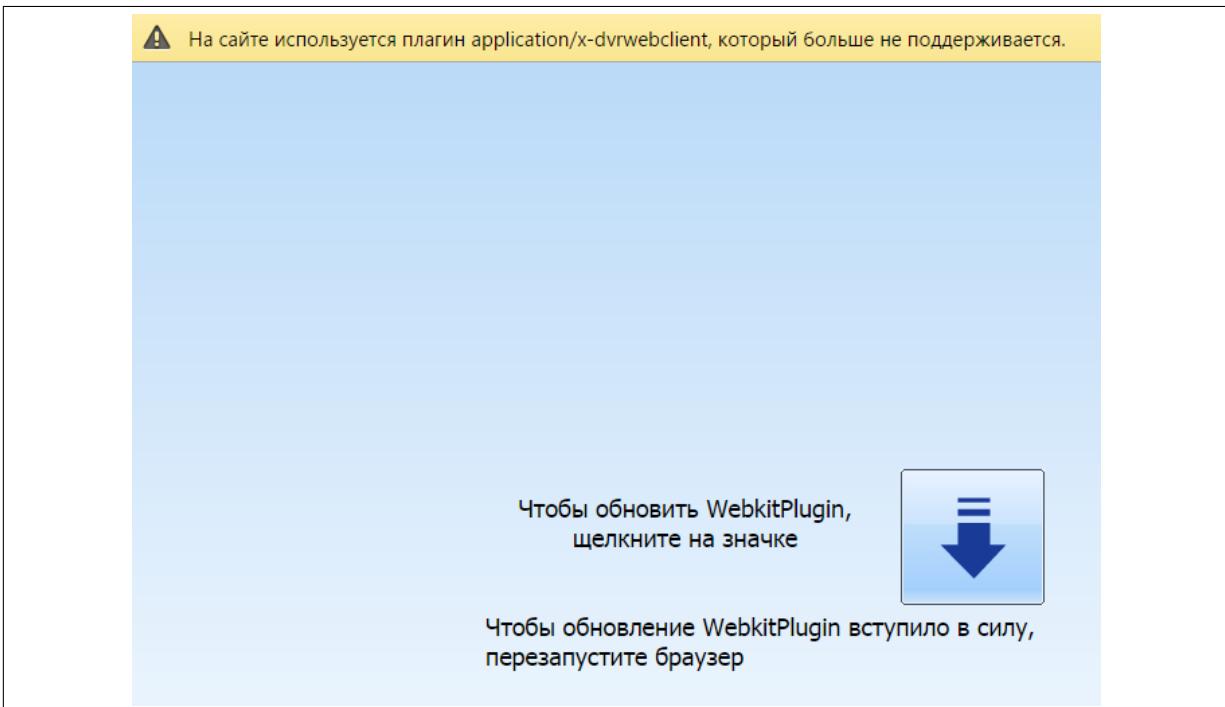
- application/x-cmsplugin (CMS Plugin_x86_64)
- application/x-dvrwebclient (npwebclient)
- application/mozilla-dvrclient-plugin
- application/npguide-plugin
- application/nptest-plugin
- application/nbr/nvrviewer
- application/chwp-webvideo-plugin (npUSSCWebVideoPlugin: rts)
- application/hwp-webvideo-plugin (npWebVideoPlugin: rts)

Примеры:

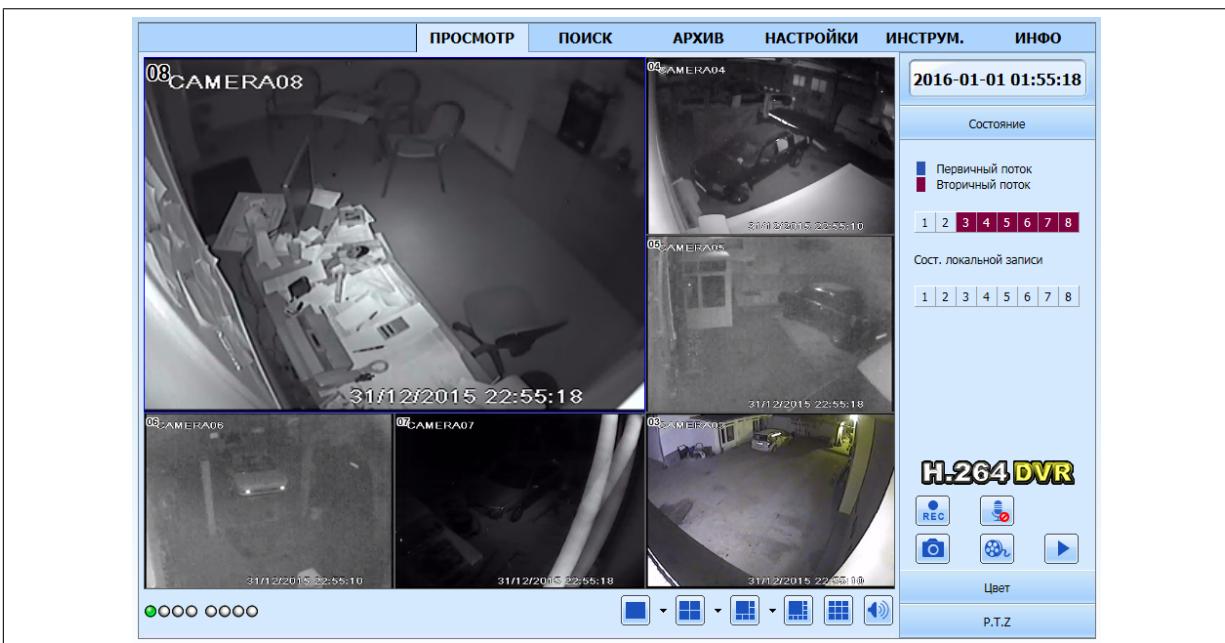
- **Chipspoint Electronics.** Дефолтный доступ: **admin/123456**. Скриншоты : окно авторизации (Internet Explorer, изобр. 35), уведомление о том, что плагин (application/x-dvrwebclient) не поддерживается (Google Chrome, изобр. 36), интерфейс после авторизации (изобр. 38).
- **Hikvision.** Дефолтный доступ: **admin/12345**. Скриншоты: окно авторизации (изобр. 39), основной интерфейс (изобр. 40).



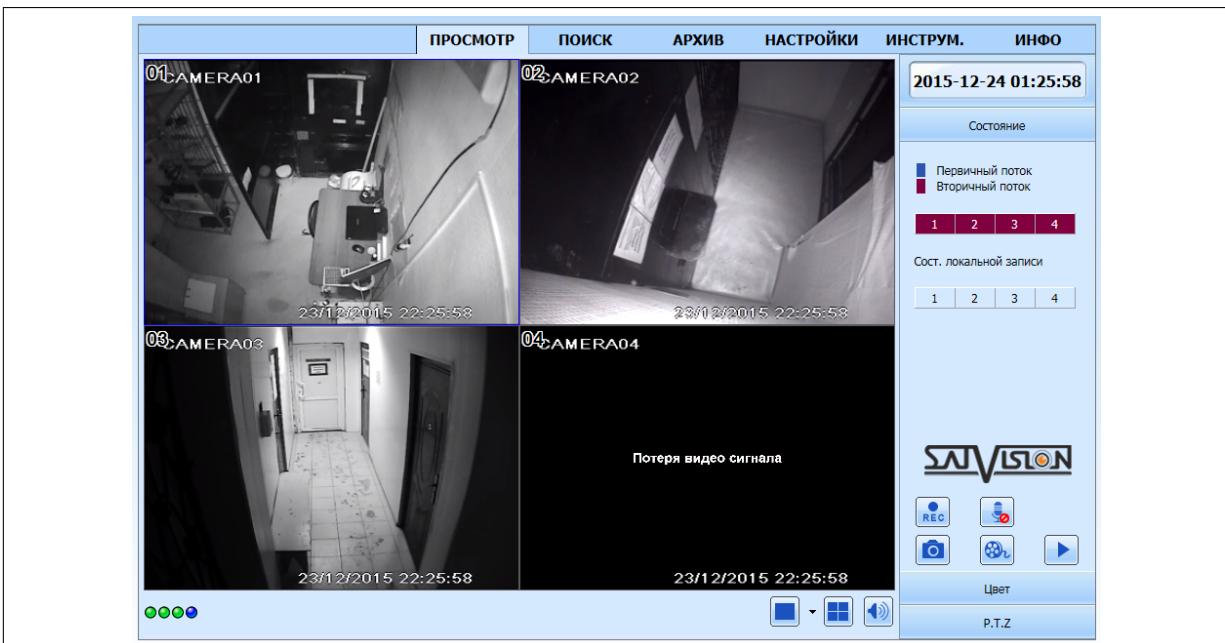
Изображение 35 — Chipspoint Electronics, окно авторизации



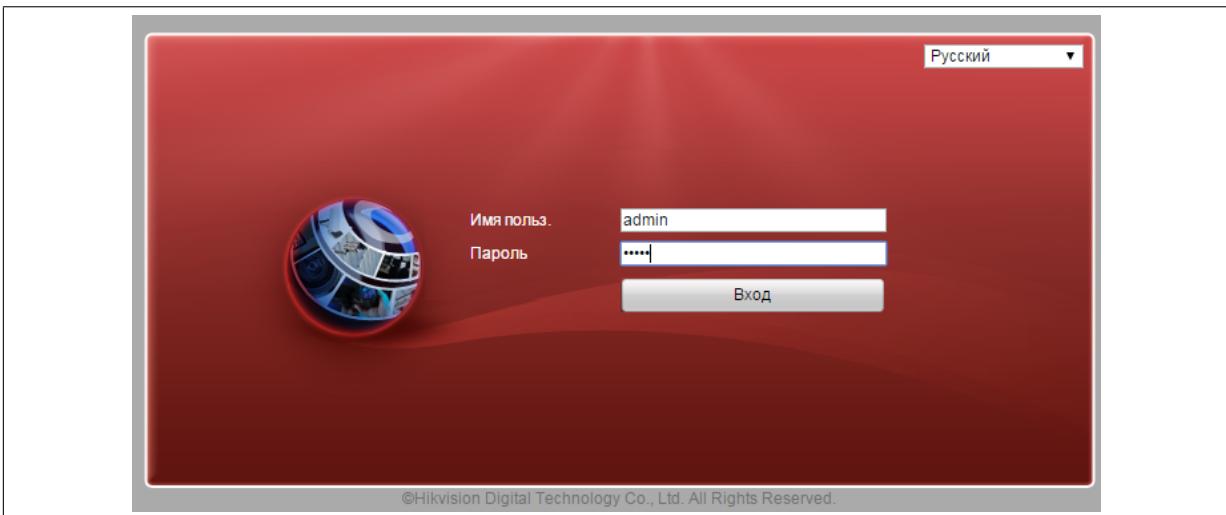
Изображение 36 — Chipspoint Electronics, уведомление о плагине



Изображение 37 — Chipspoint Electronics, основной интерфейс



Изображение 38 — Chipspoint Electronics, основной интерфейс



Изображение 39 – Hikvision, окно авторизации



Изображение 40 – Hikvision, основной интерфейс

5.3. Софт для камер

Ниже в таблице приведены ссылки на страницы скачивания софта для просмотра и управления камерами конкретных производителей.

Таблица 5 — Софт для камер

| Название | Описание |
|-------------------------------|--|
| Hikvision⁴⁶ | Различный софт, драйвера, утилиты для камер от производителя, русскоязычный портал. Для просмотра и управления используется программа iVMS . Актуальная версия – 4200. |
| Canon⁴⁷ | Для просмотра и управления используется программа WebView Livescope Viewer . Последняя доступная версия софта от 2004 года ⁴⁸ . Существуют кастомные замены для устаревших интерфейсов камер Canon (vb-c10-network-camera-js-client) ⁴⁹ . |
| Smart PSS⁵⁰ | Программа для просмотра NVR и DVR, в частности, камер Dahua. Существуют детальные инструкции ⁵¹ по использованию при поиске камер. |
| CMS⁵² | Линейка программ корейского производства для просмотра видеорегистраторов, доступна как на Windows, так и на Linux (xCMS) и Mac OS (iCMS). Аббревиатура "CMS" общеиспользуема, и почти у каждого вендора существует своя версия CMS. |

⁴⁶<http://www.hikvision.msk.ru/index/download/0-14>

⁴⁷<http://cweb.canon.jp/drv-upd/webview/viewer-w.html>

⁴⁸<http://pdfstream.manualsonline.com/8/8f1abc81-3686-49dd-928a-eeec74b679ee.pdf>

⁴⁹<https://github.com/davidbrenner/vb-c10-network-camera-js-client>

⁵⁰<http://www.safemag.ru/smart-pss/>

⁵¹<https://mega.nz/#!kI8UCJSA!P3KtS7gXQ2kXDvviYyNhC6UYYPNaAV-YT2Ov4FUNG3Q>

⁵²<http://www.cctvnpos.com/Support/Download.html>

6. Послесловие

Данный документ является попыткой систематизировать доступные в Сети сведения об онлайн-камерах и доступу к ним и будет активно дорабатываться. В дальнейшем планируется:

- Продолжить систематизацию шаблонов для поиска и описать его особенности для сервисов *ZoomEye* и *Censys*
- Сделать обзор устройства сетей видеонаблюдения и описать возможности для получения доступа к ним
- Изложить краткую историю стандартизации в области видеонаблюдения и описать особенности стандартов *ONVIF* и *PSIA*
- Подробнее раскрыть тему получения доступа к устройствам с помощью таких инструментов как *Hydra* и *Burp Suite*
- Произвести обзор в области кибербезопасности IoT, касающийся видеорегистраторов и их роли для киберпреступности (в частности, тема DDoS: *Mirai* и подобное)

Прислать авторам материалы, комментарии, пожелания и исправления можно на коллективный ящик электронной почты.