

Задача —→

**Идентификация
пользователя по фото/
видео изображению**

Команда —→

 **Чёрный лебедь**

Название сервиса → Око

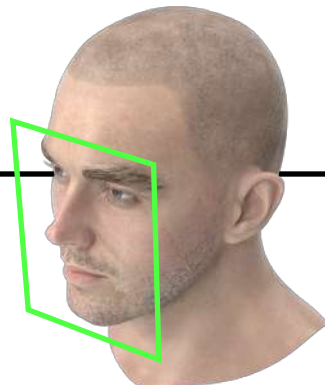
Докладчик —→ **Чернов Вадим**

Задача

Создать агентское приложение для windows



Должно периодически фотографировать человека, который сидит за компьютером



Проверять по базе лиц соответствует ли он тому пользователю который залогинился в системе

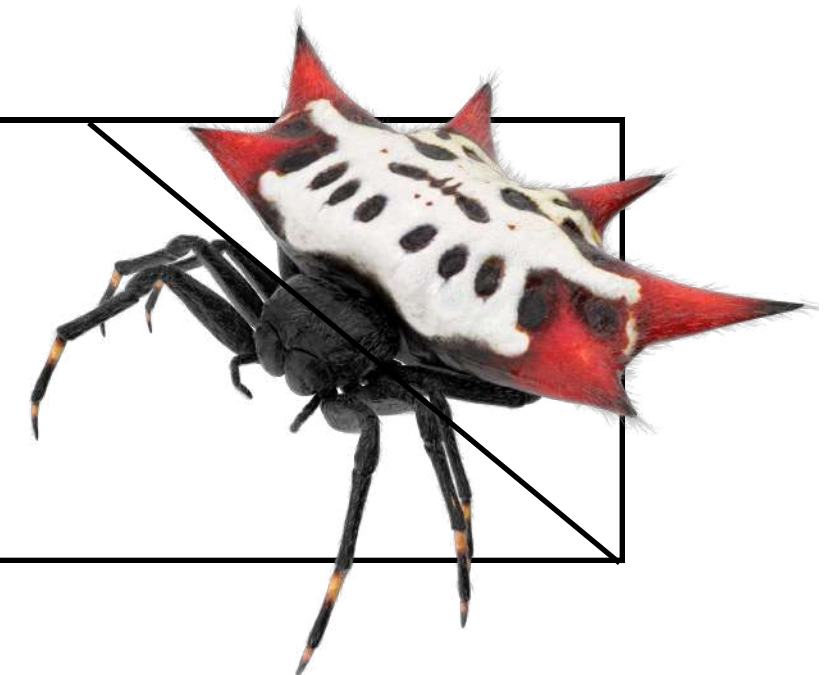


Если не соответствует, то блокировать компьютер и сообщать администратору

Должно быть защищено от остановки пользователем и локальным администратором



Не используем недокументированные возможности: мы не делаем вирус



Что удалось выяснить

1

Администратор Windows обладает
неограниченными правами
и возможностями



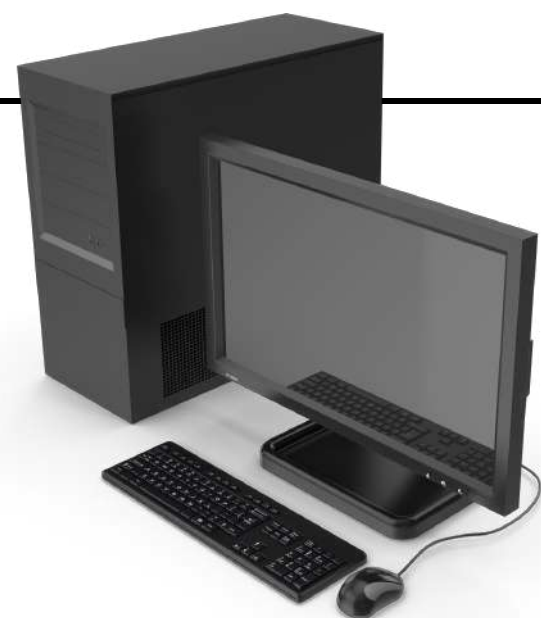
2

Любой запрет или ограничение есть
масса способов обойти

3

Что-то можно сделать средствами контроллера домена
и доменными политиками, но это не защитит нас от пункта 2

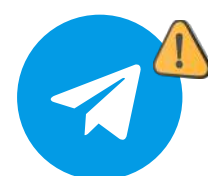
Поэтому Мы не доверяем клиентскому компьютеру



Держим на клиенте минимум информации, чтобы нас было сложнее изучить и вмешаться в работу системы



Выносим всю логику на сервер, который будет работать на доверенном хосте

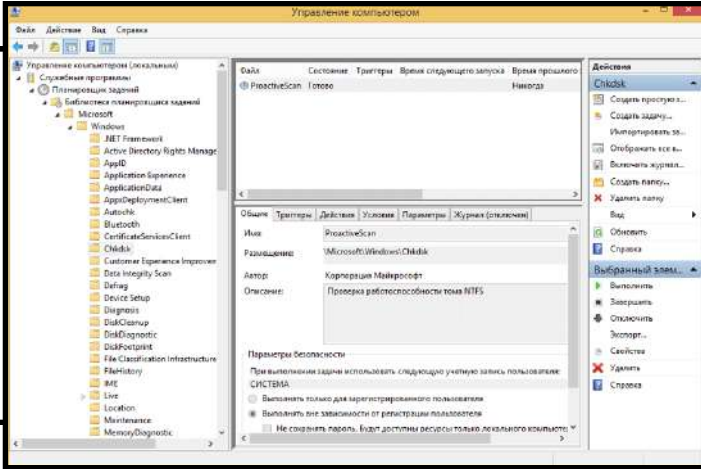


Упор на оповещения
о подозрительных активностях

Какие были идеи



N процессов, следящие друг за другом



Задействовать планировщик для автозапуска агента



Защиту типа «антивирусное ПО»

Решение



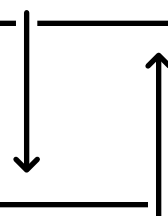
Быстрый центральный узел – Надзиратель

- 1) Хранит полную конфигурацию агентов
- 2) Периодически опрашивает агентов
- 3) Оповещает о подозрительных активностях



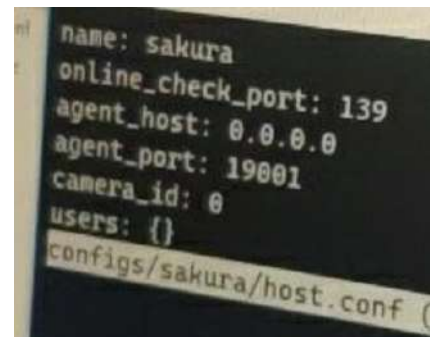
Легковесный агент

- 1) Хранит минимум информации, защищает её в процессе работы
- 2) Загружает необходимую конфигурацию из центрального узла
- 3) Содержит минимум логики

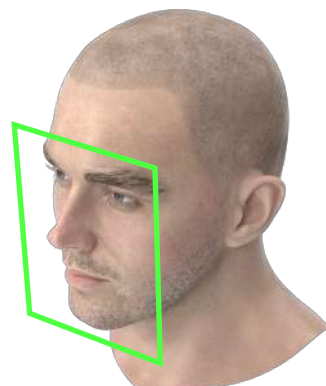




Преимущества Надзирателя



Автоматическое создание конфигурации по-умолчанию при старте нового агента



Интеграция с API распознавания лиц



Утилита для добавления пользователей и фотографий

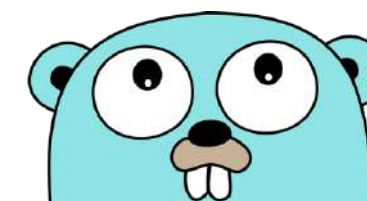


Оповещения в телеграм

- 1) Об остановке агента
- 2) О проблемах при попытке получить кадр
- 3) Об обнаружении неразрешённого лица



Устанавливается в виде службы Windows



Написан на Go

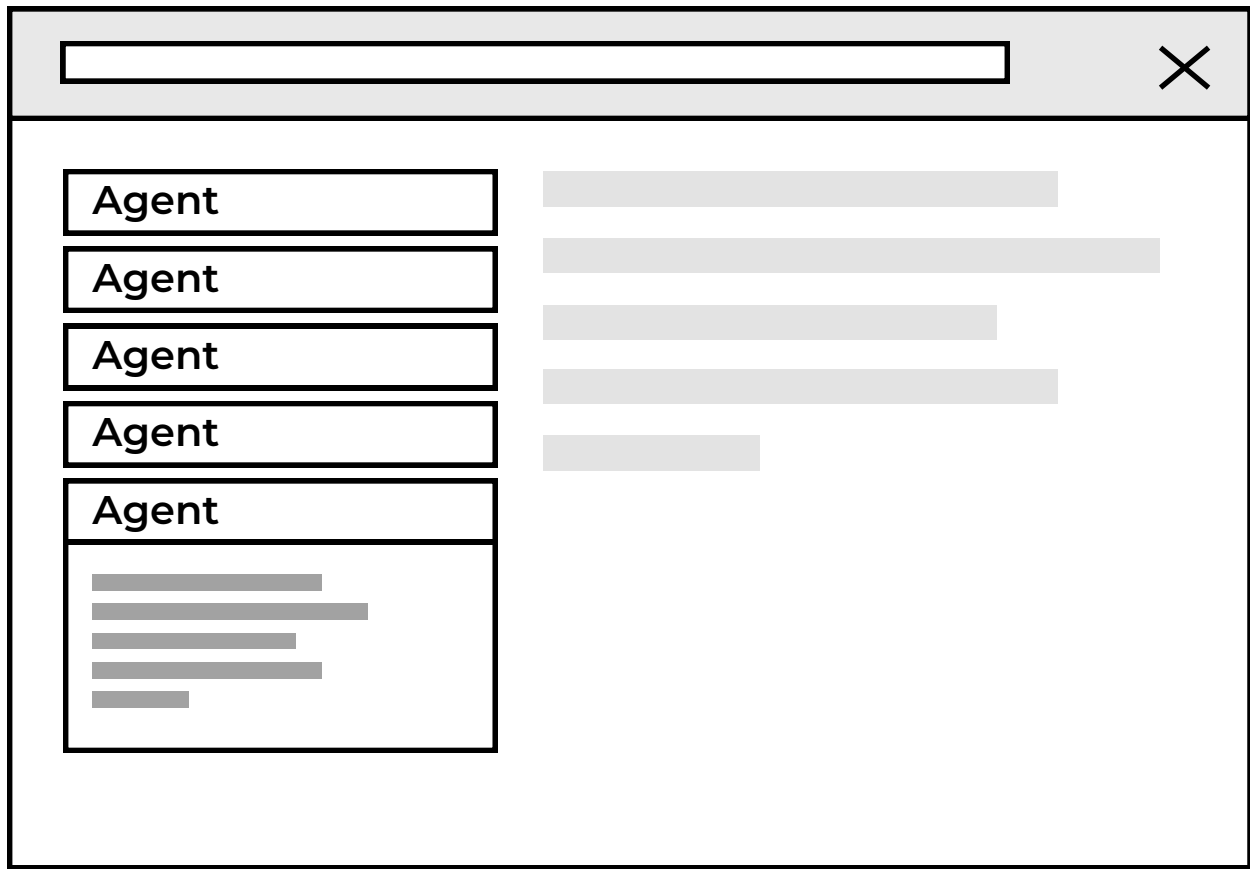


Преимущества агента

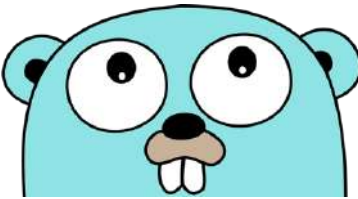
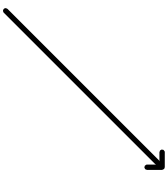
	<p>Лёгкий и простой агент, который можно реализовать на любом языке программирования</p>	<p>до 50 МВ</p> <p>Низкое потребление оперативной памяти</p>
	<p>Агент можно реализовать не только под Windows, но и под другую операционную систему</p>	 <p>Прост в разворачивании: нужно всего лишь доставить два файла</p>
	<p>Следит за сетью: разлогинивает при потере соединения</p>	 <p>Устанавливается в виде службы Windows</p>
		 <p>Службу можно скрыть доменными политиками <u>смотрите приложение к презентации</u></p>

Перспективы развития

Веб-интерфейс для Надзирателя с полным контролем конфигурации, просмотра истории уведомлений и состояния клиентов



Переписать агента на Go или C++



Команда —→

 **Чёрный лебедь**



Вадим

Програмная реализация



Динара

Экономист, бизнес-аналитик



Роза

Проджект-менеджер,
организационные вопросы (контроль
сроков, расписание), поиск данных



Ильнар

Дизайнер, визуализация
презентации и работы
системы