

**Защита критической инфраструктуры
в государственных
и бизнес-структурах
на свежем примере**



Необходимость защиты
критической инфраструктуры
не вызывает сомнений:

существуют требования государства, прописана ответственность за их нарушение...



И, в принципе, от чего защищаться – известно.

Например (но не только) – от внедрения вредоносных программ.
Но несмотря на то, что защита от вредоносных программ в той или иной мере есть почти у всех, результаты противостояния вирусописателям разнятся.

Почему? Разберем на примере.



В марте 2019 года в компанию «Доктор Веб»
обратился клиент из государственного учреждения Республики
Казахстан
по вопросу наличия вредоносного ПО
на одном из компьютеров корпоративной сети.



В ходе расследования было установлено,
что сетевая инфраструктура учреждения
была скомпрометирована
как минимум с декабря 2017 года.

Несанкционированное присутствие продолжалось как
минимум три года



**И это –
не самое поразительное**



Были выявлены совершенно разные семейства троянских программ,
а это позволяет предположить,
что за заражениями могут стоять сразу несколько хакерских групп.



И да – часть заражений имела зарубежное происхождение:
некоторые найденные трояны используются различными АРТ-группами Китая.



Как происходило заражение?



С использованием уязвимости злоумышленники загружали на компьютер одну из модификаций трояна семейства **BackDoor.PlugX**. Модули полезной нагрузки трояна позволяли удаленно управлять инфицированным компьютером и использовать его для дальнейшего продвижения по сети... После установления присутствия в сети хакерская группа использовала специализированное вредоносное ПО для решения поставленных задач.



Из интересного



Семейство обладает руткитом для сокрытия сетевой активности и следов присутствия в скомпрометированной системе, обнаружить который удалось при помощи антируткита Dr.Web, установленного на атакованном сервере.
...В основе программ лежат проекты с открытым исходным кодом...



Подведем итог



- Незакрытые уязвимости
- Возможность установки ПО на компьютеры, интересующие злоумышленников
- Использование вредоносного ПО, частично уже известного
- Использование для создания вредоносного ПО открытого кода
- Методы маскировки, не способные скрыть присутствие трояна от Антируткита Dr.Web



В августе 2019 года представитель Совбеза сообщил, что в 2018 г. было зафиксировано порядка 17 тыс. кибератак на КИИ в России.

Еще на 7 тыс. объектов злоумышленники пытались установить вредоносное ПО.

<https://www.tadviser.ru/index.php/>

Статья:Закон_О_безопасности_критической_информационной_инфраструктуры_Российской_Федерации

**Просто установить антивирус (любой)
для защиты от вредоносного ПО –
недостаточно**



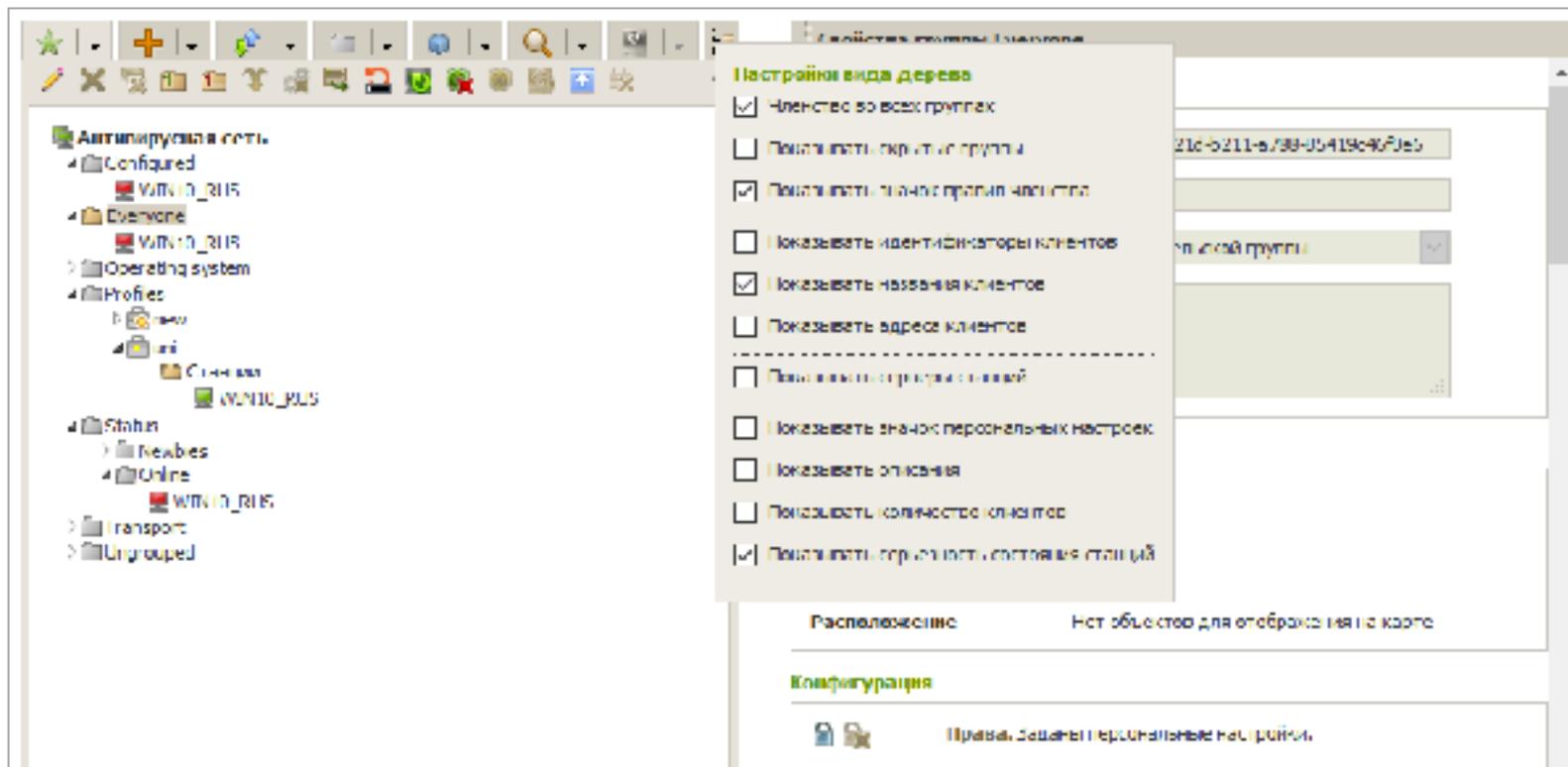
Необходимо:

- Своевременно закрывать уязвимости
- Ограничить возможность несанкционированной установки ПО
- Запретить работу под административными учетными записями
- Использовать надежные пароли и периодически их менять



Центр управления Dr.Web:

система комплексной настройки станций на основе политик и правил



Оборудование, программы и сменные носители, обнаруженные в сети

Антивирусная сеть > Evergroup > Оборудование и программы ☆

Выбранные объекты

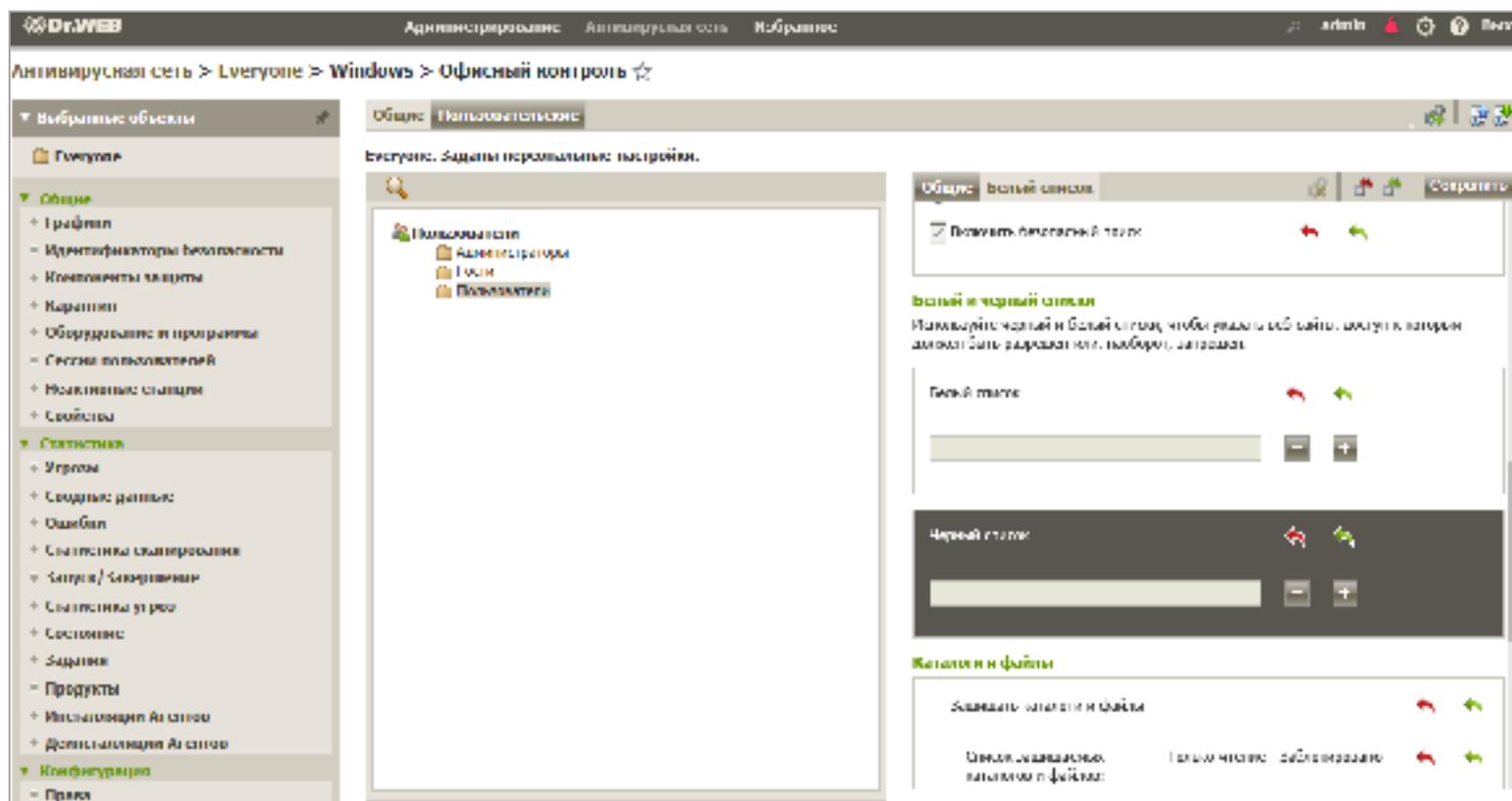
- Evergroup
 - Общие
 - Графики
 - Идентификаторы безопасности
 - Компоненты защиты
 - Карантин
 - Оборудование и программы**
 - Обнаруженные устройства
 - Сессии пользователей
 - Неактивные станции
 - Свойства
 - Статистика
 - Угрозы
 - Ошибки
 - Сводные данные
 - Связь с локальными сетями

Оборудование | Программы | Обновления Windows

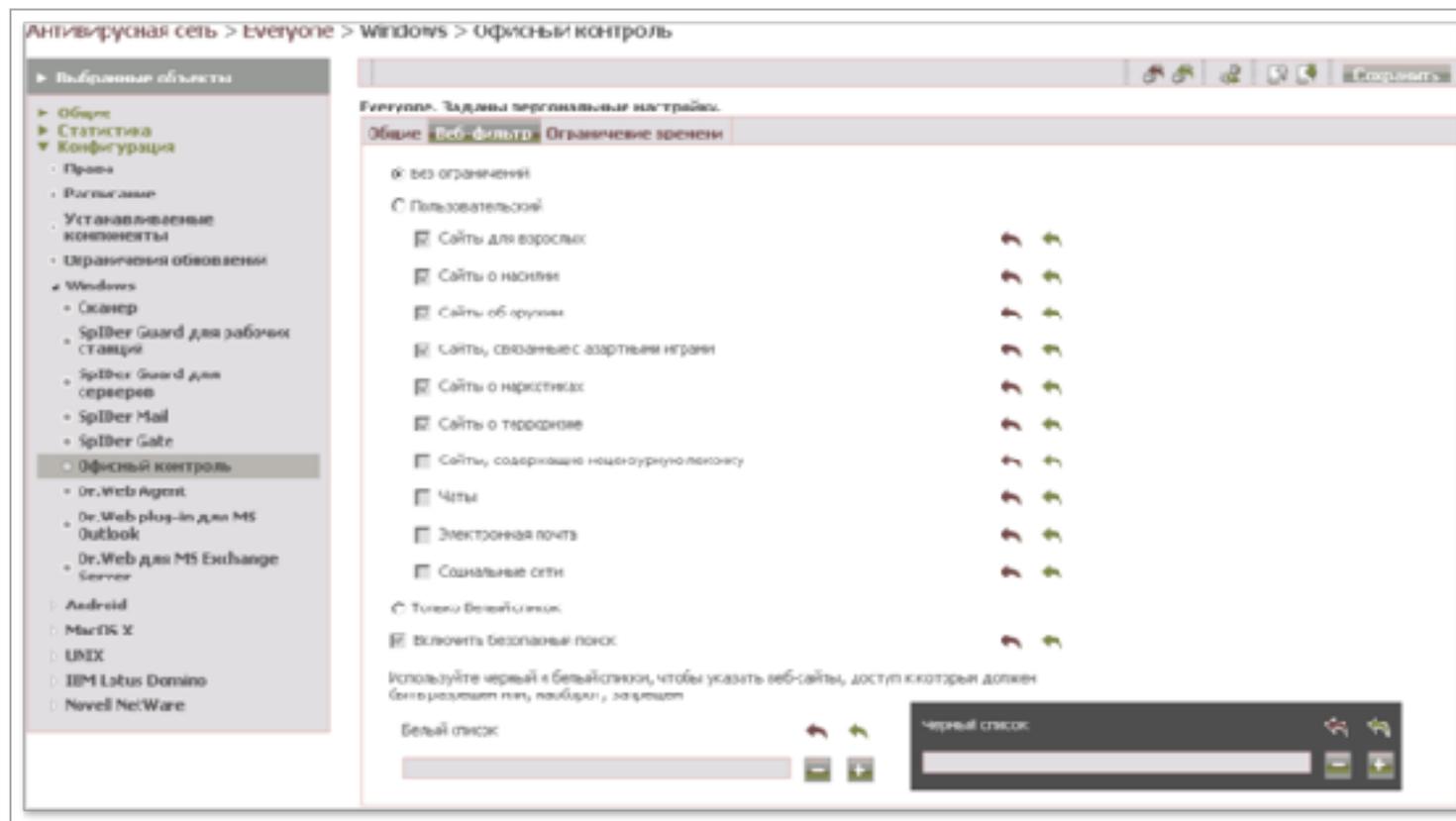
Станция	IP-адрес	Тип устройства	Название	Изготовитель	Дополнительно
WIN10_RUS (e3ef05b0-021a-11ea-4236-5cb189f...)	sd:/127.0.0.1:52254	Монитор	Generic Non-PnP Monitor	(Standard monitor type)	Разрешение экрана: 0 x 0
WIN10_RUS (e3ef05b0-021a-11ea-4236-5cb189f...)	sd:/127.0.0.1:52254	Сетевой адаптер	Intel(R) U25/4L Gigabit Network Connection	Intel Corporation	Пропускная способность: 10000 МБ/с
WIN10_RUS (e3ef05b0-021a-11ea-4236-5cb189f...)	sd:/127.0.0.1:52254	Процессор	Intel(R) Core(TM) i5-4570 CPU @ 3.20GHz	GenuineIntel	Количество ядер: 2 Тактовая частота: 3.193 ГГц
WIN10_RUS (e3ef05b0-021a-11ea-4236-5cb189f...)	sd:/127.0.0.1:52254	DVD-дисководы и дисководы компакт-дисков	NI (VMware VMWare IDE CDR10 ATA Device	(Standard CD ROM drives)	



Офисный контроль



Ограничение доступа сотрудников к сайтам



Контроль запуска программ пользователем

Антивирусная сеть > Everyone > Windows > Контроль приложений ☆

Выбранные объекты

- Everyone
- Общие
- Статистика
- Конфигурация
 - Прива
 - Планировщик заданий
 - Открытие объектов
 - Устанавливаемые компоненты
 - Параметры подключения
 - Windows
 - Скавер
 - Spider Mail и Spider Gate
 - Агент Dr.Web
 - Офисный контроль
 - Spider Guard для различных клиентов
 - Spider Guard для серверов
 - Dr.Web для Microsoft Outlook
 - браузер Dr.Web
 - Преактивная защита
 - Монитор сетевых версов
 - Контроль приложений

Everyone. Заданы персональные настройки.

Название профиля	Режим работы	Критерии функционального анализа	Запрещающие правила	Разрешающие правила
new	Активный, Тестовый	12 условий	0 правил	0 правил

1



Лечение активных заражений

Антивирусная сеть > Everyone > Windows > SpIDer Guard для рабочих станций ☆

Выбранные объекты

- Everyone
- Общие
- Статистика
- Конфигурация
 - Права
 - Планировщик заданий
 - Устанавливаемые компоненты
 - Ограничения обновлений
 - Параметры подключения
 - Agent Dr.Web для UNIX
 - Windows
 - Сканер
 - SpIDer Guard для рабочих станций
 - Офисный контроль

Everyone. Заданы персональные настройки.

Общие Действия Исключения Журнал

Режим проверки

- Оптимальный
- Параллельный

Использовать эвристический анализ

Проверять на наличие руткита

Дополнительные возможности

Проверять за рушаемые программы и модули

Превентивная защита

Антивирусная сеть > Everyone > Windows > Превентивная защита ☆

Выбранные объекты

- Everyone
- Общие
- Свойства
- Конфигурация
 - Права
 - Планировщик заданий
 - Устанавливаемые компоненты
 - Ограничения обновлений
 - Пользовательские процедуры
 - Агент Dr.Web для NPTX
- Windows
 - Сканер
 - SpIDer Guard для рабочих станций
 - Офисный контроль
 - Агент Dr.Web
 - Dr.Web для Microsoft Outlook
 - Превентивная защита**
 - Браузер Dr.Web
 - Монитор сетевых портов

Everyone. Заданы персональные настройки.

Общие

Блокировать WSL ↶ ↷

Защита от ожогов

Блокировать исполнение неавторизован ↶ ↷

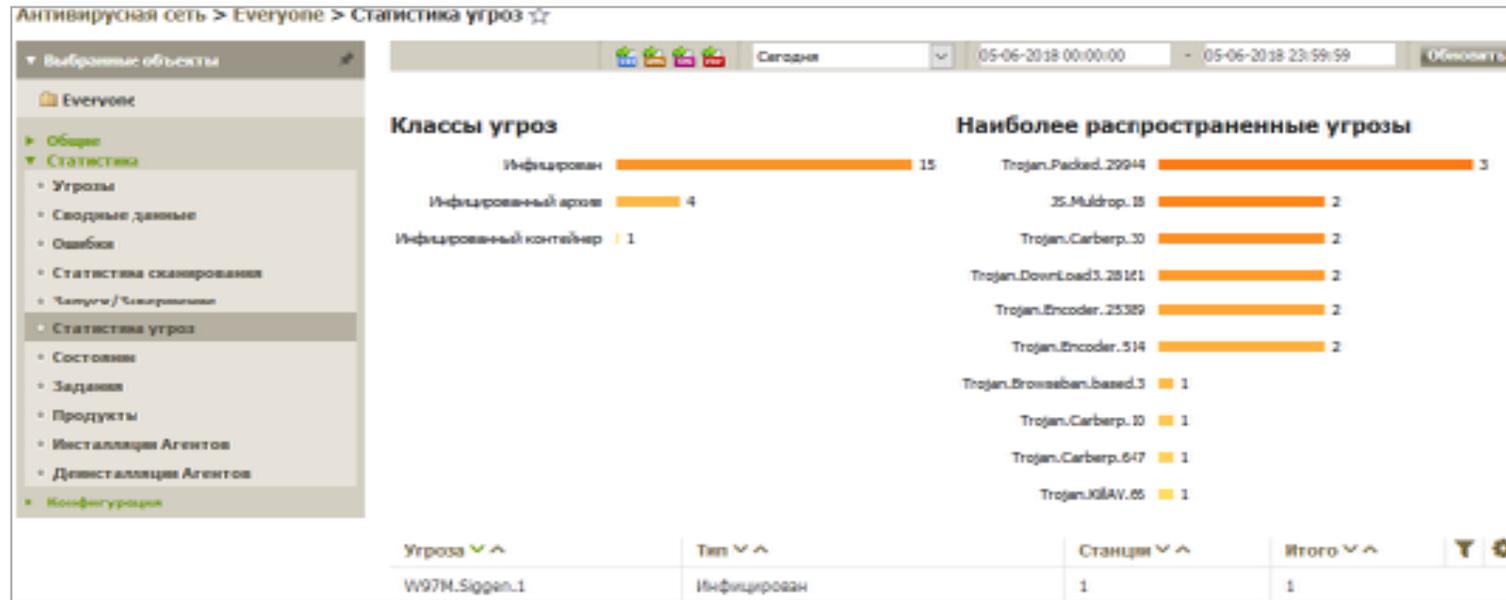
Уровень безопасности пользовательских действий

Оптимальный - + ↶ ↷

Защищаемый объект	Разрешить	Сравнивать	Запрещать
Исполнение приложений	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Целостность файлов пользователей	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
HOSTS файл	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Низкоуровневый доступ к диску	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Загрузка драйверов	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



Удобная статистика



- Интуитивно понятное отображение нужных сведений.
- Возможность экспорта статистических отчетов сразу для нескольких объектов антивирусной сети.

**С радостью ответим
на ваши вопросы!**

И благодарим за внимание.

