



КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

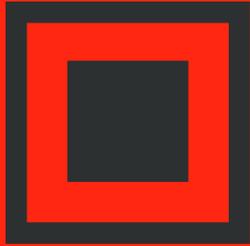
КАК НЕЗАЩИТИТЬ ДАННЫЕ. РЕАЛЬНЫЙ СЛУЧАЙ АНАЛИЗА ИНЦИДЕНТА

ВЯЧЕСЛАВ МЕДВЕДЕВ
*Ведущий аналитик отдела
развития
Доктор Веб*

МЕСТО ВСТРЕЧИ
ИБ-ПРОФЕССИОНАЛОВ

13 ФЕВРАЛЯ '20

 РОСТОВ-НА-ДОНУ



КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

Как изменится ваша ИБ в 2020 году



Вячеслав Медведев
ООО «Доктор Веб»

ТЕЛЕФОН: +7 495 789-45-87

EMAIL: v.medvedev@drweb.com

13 февраля 2020
Ростов-на-Дону

Мы постоянно рассказываем о росте количества угроз, новом функционале, возможностях, которые могут использовать наши клиенты

Давайте в этот раз сделаем по иному. Посмотрим, что получается, когда советы не используются

Компания Dr. Web занимается анализом компьютерных инцидентов (тем что в просторечии называется расследованием преступлений), выступает в роли эксперта по таким делам.

И что удивительно – ситуации бывают самые разные. А вот причины, которые послужили основой возникших проблем – почти всегда одинаковы

Пример реального инцидента

#CODEIB

Вводная:

Весной 2019 года в службу технической поддержки «Доктор Веб» обратился корпоративный клиент с жалобой на проблемы в работе сервера. Нагрузка на вычислительные мощности была очень высокой и возникала словно из ниоткуда.

Перед экспертами было поставлено несколько задач.

- Обнаружить причину необычно высокого потребления ресурсов.
- Отследить источник и способ атаки, чтобы пресечь дальнейшее распространение вредоносной программы. Сделать подробное описание атаки.
- На основании проведенного исследования разработать рекомендации по усилению мер безопасности в сети клиента.
- Помочь правоохранительным органам найти виновного в атаке.

Заражение начиналось с RCE-уязвимости в легальном продукте.

- Уязвимости есть всегда. Только не все они еще известны
- Мер защиты много. В частности антивирус – это защита от использования уязвимостей:
 - Превентивная защита
 - Контроль целостности
 - Защита от эксплойтов
 - ...

Anti-virus Network > Everyone > Windows > Application Control ☆

Selected objects

- General
- Statistics
- Configuration
 - Permissions
 - Task Scheduler
 - Update restrictions
 - Installing components
 - Connection settings
 - Windows
 - Scanner
 - SpIDer Mail and SpIDer Gate
 - Dr.Web Agent
 - Office Control
 - SpIDer Guard for workstations
 - SpIDer Guard for servers
 - Dr.Web for Microsoft Outlook
 - Dr.Web Firewall
 - Preventive protection
 - Network port monitor
 - Application Control

Everyone. Custom settings are specified.

Profile name	Operation mode
new	Active, Test

1

Anti-virus Network > WIN10_RUS > Windows > Preventive protection ☆

Selected objects

- General
 - Charts
 - Security identifiers
 - Protection components
 - Quarantine
 - Hardware and software
 - Detected hardware
 - Users sessions
 - Properties
- Statistics
- Configuration
 - Permissions
 - Task Scheduler
 - Update restrictions
 - Installing components
 - Connection settings
 - Scanner
 - SpIDer Mail and SpIDer Gate
 - Dr.Web Agent
 - Preventive protection
 - Dr.Web Firewall
 - Dr.Web for Microsoft Exchange Server
 - Network port monitor
 - Application Control
 - SpIDer Guard for workstations
 - Office Control

WIN10_RUS. Settings are inherited from the Default policy policy.

General

Exploit prevention
Prevent unauthorized code from running

Level of suspicious activity blocking
Optimal

Protected object	Allow	Ask	Block
Integrity of running applications	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Integrity of users files	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
HOSTS file	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Low-level disk access	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Drivers loading	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Image File Execution Options	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Windows Multimedia Drivers	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Winlogon parameters	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Winlogon notifiers	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Windows shell autorun	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Executable files associations	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Software Restriction Policies	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Отключение защиты целостности процессов в используемом антивирусе – путь к заражению!

Через эксплойт на стороне пострадавшего клиента создавалась административная учетная запись для доступа по RDP.

Возможные проблемы:

- Работа программ с административными правами
- Отсутствие запрета на запуск нового ПО
- Слабые пароли
- Отсутствие контроля целостности



...до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев. 273 УК РФ

Злоумышленник вручную заходил на сервер по RDP и, используя легитимное ПО ProcessHacker, «убивал» установленный антивирус или просто отключал его напрямую через GUI

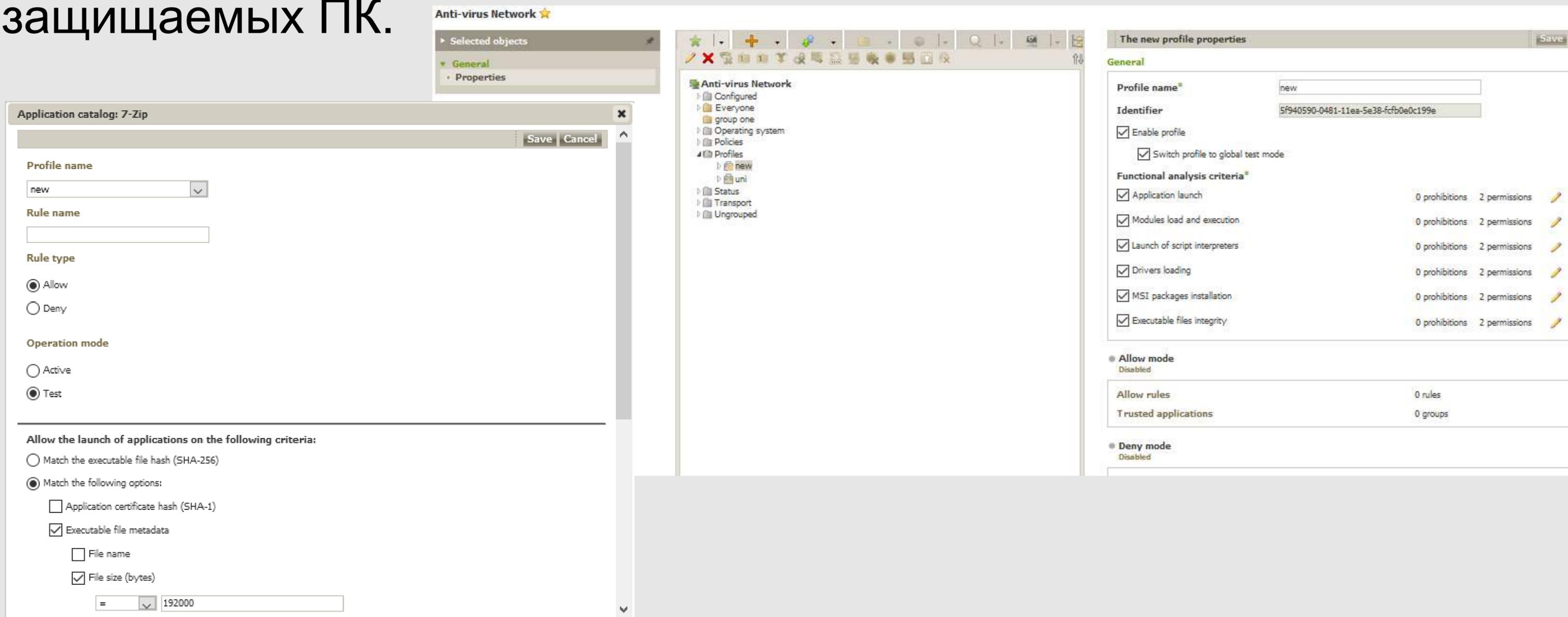
Возможные проблемы

- Наличие удаленного доступа
- Запущенные ненужные сервисы
- Установка неразрешенного ПО
- Разрешение на загрузку драйверов
- Наличие прав пользователя на отключение антивируса
- Отсутствие централизованной защиты
- Отсутствие контроля за изменением состава ПО
- Отсутствие белого списка ПО
- Отсутствие пароля на доступ к настройкам антивируса
- Отсутствие пароля на удаление ПО или пароль, совпадающий с паролем доступа в систему

Управление работой модуля **Контроль приложений** производится на основе:

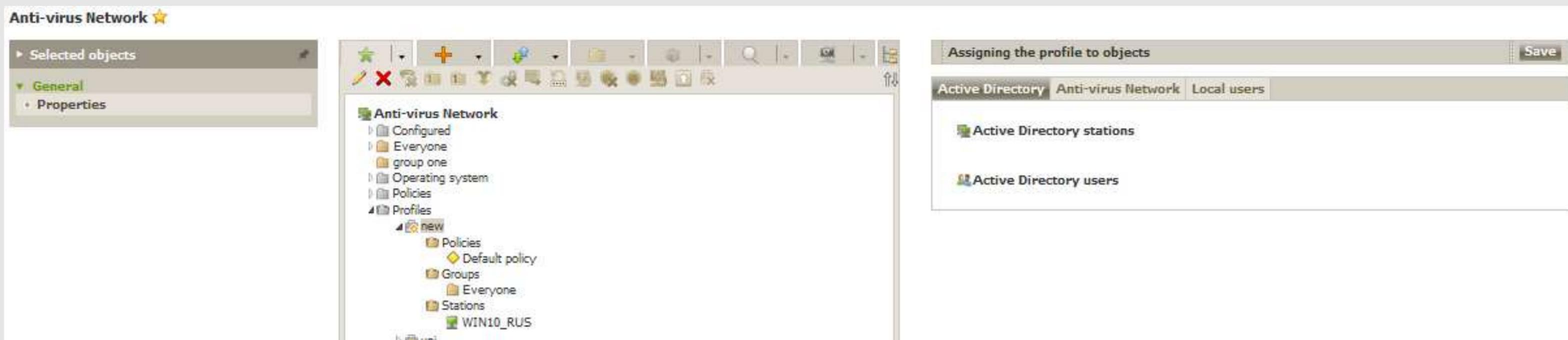
- ✓ запрещающих правил,
- ✓ разрешающих правил,
- ✓ специальных правил, созданных для противодействия наиболее часто используемым злоумышленниками методик обхода антивирусной защиты.

Администратор может определять, что контролировать на защищаемых ПК.



The screenshot displays the Dr. Web application control interface. The main window is titled "Application catalog: 7-Zip". It shows the configuration for a new profile named "new". The "Rule name" field is empty. The "Rule type" is set to "Allow". The "Operation mode" is set to "Test". Under "Allow the launch of applications on the following criteria:", the "Match the following options:" radio button is selected. The "Executable file metadata" checkbox is checked, and the "File size (bytes)" checkbox is also checked. A value of "192000" is entered in the field below. The "Functional analysis criteria" section is visible, showing various criteria like "Application launch", "Modules load and execution", etc., each with 0 prohibitions and 2 permissions. The "Allow mode" and "Deny mode" are both disabled. The background shows the "Anti-virus Network" tree view with the "new" profile selected under "Profiles".

Ограничения по запуску программ могут быть назначены на отдельных пользователей, станции или группы.



Получив доступ в систему, злоумышленник загружал на сервер троянца-майнера и запускал его. В дальнейшем расследование показало, что в планах злоумышленника был запуск шифровальщика

Заметили проблему – займитесь анализом или обращайтесь к нам!



Возможности технологий Dr.Web

Эвристический анализатор

Технология Origins Tracing

Модуль эмуляции исполнения

Технология Fly-Code

Комплексный анализатор упакованных угроз

Технология Script Heuristic

Технология анализа структурной энтропии
и много других технологий

Типичная проблема – отключение компонента вместо
настройки антивируса

————— #CODEIB —————

В результате исследования этого носителя и используемых «Доктор Веб» [ханипотов](#) было обнаружено еще несколько эксплойтов. Было выявлено несколько видов ранее неизвестных антивирусу Dr.Web вредоносных программ и список жертв, атакованных аналогичным образом. Среди пострадавших оказались пользователи самых разных антивирусных продуктов. После анализа полученных исходных кодов нового вредоносного ПО вирусная база Dr.Web пополнилась новыми записями.

Выяснив какое ПО связано с активностью троянца, мы обратились к его разработчику, который передал нам для анализа НЖМД **руководителя (!)** своей разработки.

Именно там мы нашли исходники эксплойтов

Вывод. Доверяй, но проверяй. Увы, но если вы разработчик ПО, то всегда есть вероятность, что в вашем коллективе есть крыса. Анализируйте свое ПО на наличие недокументированного функционала. Репутация – ваше все



...до пяти лет с ограничением свободы на срок до двух лет или без такового либо лишением свободы на срок от двух до пяти лет со штрафом в размере от пятисот тысяч до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет.

274.1 УК РФ

Виновный наказан?

Совместно с правоохранительными органами и разработчиком данного ПО, удалось установить злоумышленника и возбудить уголовное дело.

#CODEIB

Самое главное:

Благодаря экспертизе, разработчику удалось закрыть уязвимость, переосмыслить подходы к разработке ПО с учетом текущих требований к информационной безопасности, установить соответствующий контроль за выпускаемой продукцией/услугой и предпринять соответствующие меры для недопущения подобных инцидентов в будущем.

Но стоит особо отметить, что в данном случае жертва еще «легко отделалась». Злоумышленник, получив доступ в систему, устанавливал туда троянца-майнера, который «всего лишь» сильно загружал ресурсы системы, не нанося прямого урона. Поскольку речь идёт о весьма специфическом ПО, которое обычно находится на том же сервере, что и, например, приложения типа 1С, ситуация могла развиваться иначе.

Если произошла нештатная ситуация (пропали деньги или данные, утекли пароли к корпоративным ресурсам, компьютеры работают с перебоями и т. д.) и вы предполагаете, что причина в действиях вредоносного ПО, закажите экспертизу ВКИ в компании «Доктор Веб».

Итого

...до пяти лет с ограничением свободы на срок до двух лет или без такового либо лишением свободы на срок от двух до пяти лет со штрафом в размере от пятисот тысяч до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет.

274.1 УК РФ

...до пяти лет с ограничением свободы на срок до двух лет или без такового либо лишением свободы на срок от двух до пяти лет со штрафом в размере от пятисот тысяч до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет.

274.1 УК РФ

Для предотвращения инцидентов:

- ✓ Устанавливайте обновления
- ✓ Используйте белый список ПО
- ✓ Контролируйте изменения состава ПО
- ✓ Никаких админских прав у пользователей
- ✓ Надежные пароли, отличающиеся для пользователей и программ
- ✓ Централизованное управление защитой и/или паролем на доступ к антивирусу
- ✓ Минимум прав у пользователей
- ✓ Отключайте ненужные сервисы

Anti-virus Network > Everyone > Windows > Office Control ☆

Selected objects

- General
- Statistics
- Configuration
 - Permissions
 - Task Scheduler
 - Update restrictions
 - Installing components
 - Connection settings
 - Windows
 - Scanner
 - SpIDer Mail and SpIDer Gate
 - Dr.Web Agent
 - Office Control
 - SpIDer Guard for workstations
 - SpIDer Guard for servers
 - Dr.Web for Microsoft Outlook
 - Dr.Web Firewall
 - Preventive protection
 - Network port monitor
 - Application Control
 - Android
 - macOS
 - UNIX
 - Scanner for workstations
 - Dr.Web Agent
 - Dr.Web MailD
 - Dr.Web ICAPD
 - SpIDer Guard

General User-defined

Everyone. Custom settings are specified.

Users

- Administrators
- Guests
- Users

General Allowed devices

Block all except websites from the white list

Enable safe search

Black and white lists
You can use white and black lists to allow or block access to specified web sites.

White list

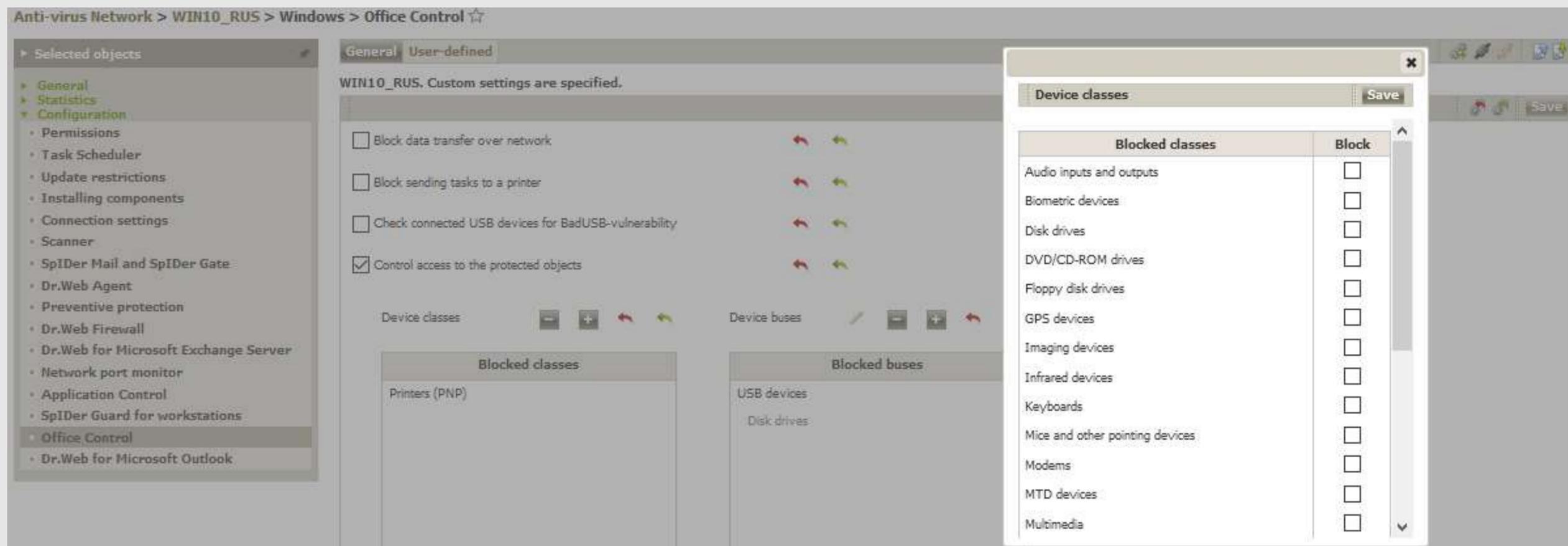
Black list

Folders and files

Protect folders and files

List of protect folders and files: Read-only Blocked

Предотвращение заражений через сменные носители



Anti-virus Network > Everyone > Windows > Office Control ☆

Selected objects

- General
- Statistics
- Configuration
 - Permissions
 - Task Scheduler
 - Update restrictions
 - Installing components
 - Connection settings
 - Windows
 - Scanner
 - SpIDer Mail and SpIDer Gate
 - Dr.Web Agent
 - Office Control**
 - SpIDer Guard for workstations
 - SpIDer Guard for servers
 - Dr.Web for Microsoft Outlook
 - Dr.Web Firewall
 - Preventive protection
 - Network port monitor
 - Application Control
 - Android
 - macOS
 - UNIX
 - Scanner for workstations
 - Dr.Web Agent
 - Dr.Web MailD
 - Dr.Web ICAPD

General User-defined

Everyone. Custom settings are specified.

Users

- Administrators
- Guests
- Users

General Allowed devices

- Social networks
- Anonymizers
- Block all except websites from the white list
- Enable safe search

Black and white lists

You can use white and black lists to allow or block access to specified web sites.

White list

Black list

Folders and files

- Protect folders and files

Anti-virus Network > Everyone > Windows > Application Control ☆

Selected objects

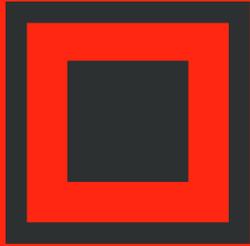
- General
- Statistics
- Configuration
 - Permissions
 - Task Scheduler
 - Update restrictions
 - Installing components
 - Connection settings
 - Windows
 - Scanner
 - SpIDer Mail and SpIDer Gate
 - Dr.Web Agent
 - Office Control
 - SpIDer Guard for workstations
 - SpIDer Guard for servers
 - Dr.Web for Microsoft Outlook
 - Dr.Web Firewall
 - Preventive protection
 - Network port monitor
 - Application Control**

Everyone. Custom settings are specified.

Profile name v ^	Operation mode v ^	Functional analysis criteria v ^	Deny rules v ^	Allow rules v ^	Trusted applications v ^	T ⚙
new	Active, Test	12 conditions	0 rules	0 rules	0 groups	

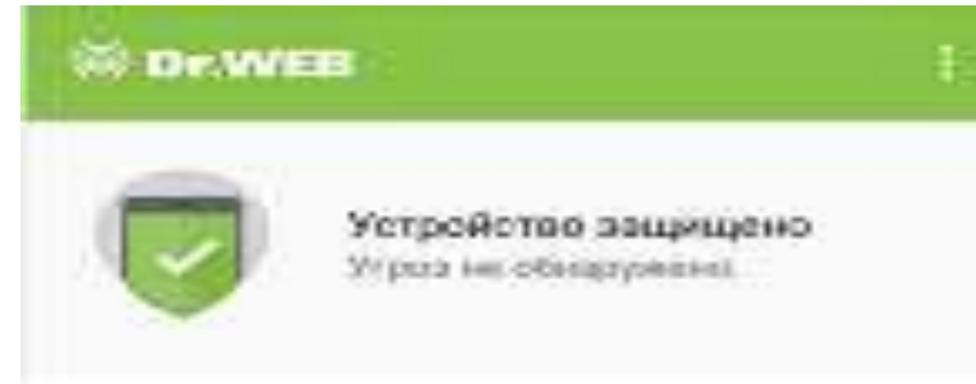
1

Page: 1 Showing 1 – 1 of 1 10 v



КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

Благодарим за внимание!



Номер службы технической поддержки

8-800-333-7932

Запомнить просто! –
возникла проблема – набери DRWEB!

8-800-33-DRWEB

Убедитесь, что на ваших компьютерах нет вирусов

#CODEIB

