

Вы хотите защитить КИИ?

**Мы вас обрадуем –
начать нужно с другого**



Поскольку времени у нас мало,
разберем всего один случай



Пришел китайский станок лазерной резки. На борту ОС Windows 7

Вставили гарантированно чистую от вирусов флешку, для копирования файлов программ со станка, принесли на рабочий ПК, получили оповещение о вирусе...

Также со станком шло ПО, на usb носителе, при попытке скопировать с него файлы дистрибутивов получили множество детектов, см. вложение.

Поскольку времени у нас мало, разберем всего один случай

Обращение в службу технической поддержки



ИИ	Тип	Угроза	Действие	Компонент	Объект
к	Инфицирован	Worm.Siggen.12242	В карантине	SpiDer Guard для рабочих станций Windows	G:_WA.nil
к	Инфицирован	Trojan.BrowseBan.565	В карантине	SpiDer Guard для рабочих станций Windows	G:\EZCAD2-170\Ezcad2.14.11(20190531) - Lite\J8.exe
к	Инфицирован	Trojan.Inject1.10883	В карантине	SpiDer Guard для рабочих станций Windows	G:\EZCAD2-170\Ezcad2.14.11(20190531) - Lite\J8.exe
к	Инфицирован	Trojan.Inject1.10883	Вылечен	SpiDer Guard для рабочих станций Windows	G:\EZCAD2-170\Ezcad2.14.11(20190531) - Lite\CorFile2.exe
к	Инфицированный архив	Trojan.Inject1.10883	Вылечен	SpiDer Guard для рабочих станций Windows	G:\EZCAD2-170\dirver\MINI卡驱动\2014签名release\CH341SER.EXE
к	Инфицирован	Trojan.BrowseBan.565	В карантине	SpiDer Guard для рабочих станций Windows	G:\EZCAD2-100\Ezcad2.14.11(20190531) - Lite\J8.exe
к	Инфицирован	Trojan.Inject1.10883	В карантине	SpiDer Guard для рабочих станций Windows	G:\EZCAD2-100\Ezcad2.14.11(20190531) - Lite\J8.exe
к	Инфицированный архив	Trojan.Inject1.10883	Вылечен	SpiDer Guard для рабочих станций Windows	G:\EZCAD2-100\dirver\MINI卡驱动\2014签名release\CH341SER.EXE
к	Инфицирован	Trojan.Inject1.10883	Вылечен	SpiDer Guard для рабочих станций Windows	G:\EZCAD2-100\Ezcad2.14.11(20190531) - Lite\CorFile2.exe
к	Инфицирован	Worm.Siggen.12242	В карантине	SpiDer Guard для рабочих станций Windows	G:_WIFNDNIU.nil

Кстати Worm – это червь, так что возможно злоумышленник, надеялся заразить всю сеть клиента. А может и нет, просто китайский бардак



- ... несанкционированный вход, через подбор пароля одной из учетных записей
- ... после входа по RDP злоумышленник запустил шифрующий скрипт
- ... судя по последнему отчету, у вас в сети должен быть сервер с адресом _____, на котором видна подозрительная сетевая активность
- ... на сервер ... антивирус Dr.Web был установлен уже после шифрования

Из ответов специалистов техподдержки «Доктор Веб» по итогам разбора инцидентов



Клиент параллельно запросил поставщика в Китае - "это не вирус, просто отключите свой антивирус и работайте спокойно"



Исследование станка выявило,
что вредоносный софт не просто
там находился – была заражена
нужная для работы программа



Типичная атака “через поставщика”, методы защиты от которой известны давно и достаточно просты.
Но используются ли они?





Защита КИИ – это не только защита
промышленных протоколов и контроль
целостности на устройствах различного
назначения

Это еще и безопасное окружение –
которое именно и находится под атакой.



Лишь 11% пойманных
на USB-накопителях вредоносных
программ были нацелены на АСУ ТП.

Статистика неумолима – гораздо чаще
случаются атаки не на само
промышленное оборудование.



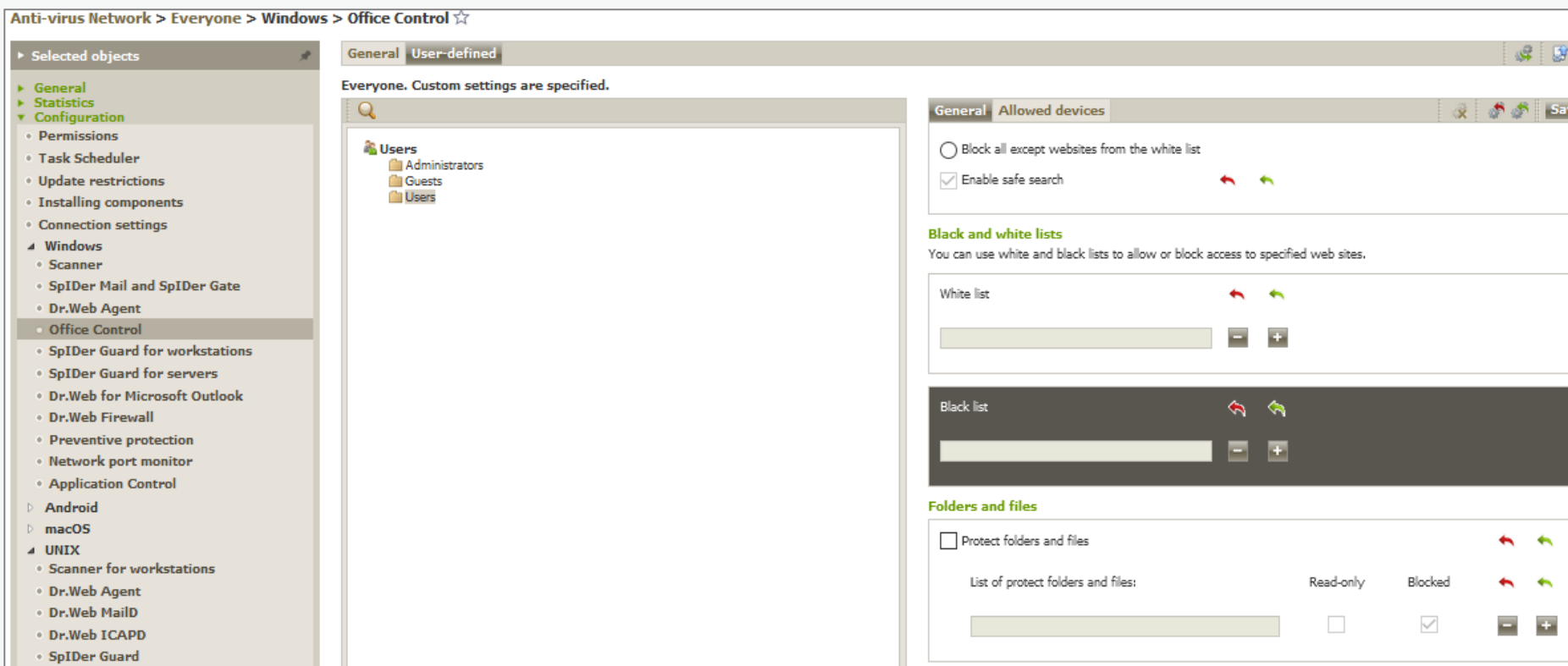
Dr.Web Enterprise Security Suite

Антивирус – это не только
антивирусные базы



Доступ только к “ЧИСТЫМ” ресурсам

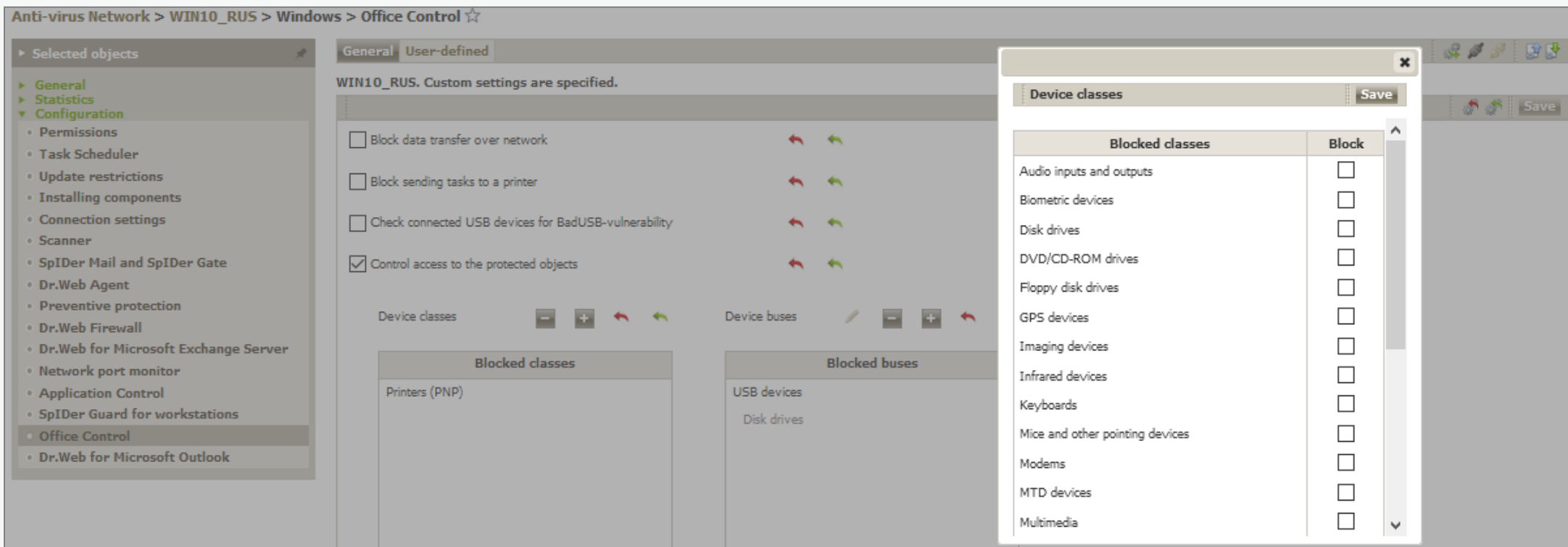
Доступ к ресурсам только в указанное время



The screenshot shows the Dr.Web Office Control configuration interface. The left sidebar contains a tree view with categories like General, Statistics, Configuration, Windows, Android, macOS, and UNIX. The main area is titled "Office Control" and shows a search bar and a list of users: Administrators, Guests, and Users. The right sidebar contains several configuration panels:

- General**: Includes "Block all except websites from the white list" (unchecked) and "Enable safe search" (checked).
- Black and white lists**: A section for managing lists of websites. It includes a "White list" and a "Black list", each with a search bar and add/remove buttons.
- Folders and files**: Includes a checkbox for "Protect folders and files" (unchecked) and a section for "List of protect folders and files" with columns for "Read-only" and "Blocked".

Контроль использования внешних носителей и оборудования компании



Anti-virus Network > WIN10_RUS > Windows > Office Control ☆

Selected objects

- General
- 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
 - Dr.Web for Microsoft Outlook

General User-defined

WIN10_RUS. Custom settings are specified.

- Block data transfer over network
- Block sending tasks to a printer
- Check connected USB devices for BadUSB-vulnerability
- Control access to the protected objects

Device classes

Blocked classes

- Printers (PNP)

Device buses

Blocked buses

- USB devices
- Disk drives

Device classes

Blocked classes	Block
Audio inputs and outputs	<input type="checkbox"/>
Biometric devices	<input type="checkbox"/>
Disk drives	<input type="checkbox"/>
DVD/CD-ROM drives	<input type="checkbox"/>
Floppy disk drives	<input type="checkbox"/>
GPS devices	<input type="checkbox"/>
Imaging devices	<input type="checkbox"/>
Infrared devices	<input type="checkbox"/>
Keyboards	<input type="checkbox"/>
Mice and other pointing devices	<input type="checkbox"/>
Modems	<input type="checkbox"/>
MTD devices	<input type="checkbox"/>
Multimedia	<input type="checkbox"/>



Контроль запуска программ пользователем (и под его именем)

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	Functional analysis criteria	Deny rules	Allow rules	Trusted applications
new	Active, Test	12 conditions	0 rules	0 rules	0 groups

1

Page: 1 Showing 1 – 1 of 1 10



Контроль установки обновлений безопасности

Антивирусная сеть > Everyone > Оборудование и программы ☆

Выбранные объекты

- Everyone
- Общие
 - Графики
 - Идентификаторы безопасности
 - Компоненты защиты
 - Карантин
 - Оборудование и программы
 - Обнаруженные устройства
 - Сессии пользователей
 - Неактивные станции
 - Свойства
- Статистика
- Конфигурация
 - Права
 - Планировщик заданий
 - Ограничения обновлений
 - Устанавливаемые компоненты
 - Параметры подключения
- Windows

Оборудование Программы Обновления Windows

Станция	IP-адрес	Название
WRK-BASILIO (d00b7e76-d21d-b211-8768-d4069...)	ssl://172.25.2.164:54023	KB2479943: Security Update for Wind...
DRWEB-PC (8022a863-d21d-b211-a69f-94118a27...)	ssl://172.25.2.252:49685	KB2479943
WRK-BASILIO (d00b7e76-d21d-b211-8768-d4069...)	ssl://172.25.2.164:54023	KB2491683: Security Update for Wind...
DRWEB-PC (8022a863-d21d-b211-a69f-94118a27...)	ssl://172.25.2.252:49685	KB2491683
WRK-BASILIO (d00b7e76-d21d-b211-8768-d4069...)	ssl://172.25.2.164:54023	KB2506014: Update for Windows 7 for...
DRWEB-PC (8022a863-d21d-b211-a69f-94118a27...)	ssl://172.25.2.252:49685	KB2506014
WRK-BASILIO (d00b7e76-d21d-b211-8768-d4069...)	ssl://172.25.2.164:54023	KB2506212: Security Update for Wind...
DRWEB-PC (8022a863-d21d-b211-a69f-94118a27...)	ssl://172.25.2.252:49685	KB2506212
WRK-BASILIO (d00b7e76-d21d-b211-8768-d4069...)	ssl://172.25.2.164:54023	KB2506928: Update for Windows 7 for...
DRWEB-PC (8022a863-d21d-b211-a69f-94118a27...)	ssl://172.25.2.252:49685	KB2506928

1 2 3 4 ... 39 Следующая →

Страница: 1 Результаты 1 – 10 из 389 10



Контроль установленных программ

Контроль установленных компонентов защиты

Антивирусная сеть > Everyone > Компоненты защиты

Идентификатор	Станция	Адрес станции	Компонент	Время установки	Тип запуска	Пользователь	Время з
<input type="checkbox"/> 9ee74281-b745-4f5a-b6ea-06ada4a16bdc	astradrw	ssl://194.85.20.253:30325	Dr.Web ConfigD для UNIX	14-06-2019 13:47:21	Служебный процесс		16-03-20:
<input type="checkbox"/> 9ee74281-b745-4f5a-b6ea-06ada4a16bdc	astradrw	ssl://194.85.20.253:30325	Scanning Engine для UNIX	25-07-2019 11:00:07	Служебный процесс		16-03-20:
<input type="checkbox"/> 9ee74281-b745-4f5a-b6ea-06ada4a16bdc	astradrw	ssl://194.85.20.253:30325	Dr.Web File Checker для UNIX	25-07-2019 11:00:07	Служебный процесс		16-03-20:
<input type="checkbox"/> 9ee74281-b745-4f5a-b6ea-06ada4a16bdc	astradrw	ssl://194.85.20.253:30325	SpIDer Gate для UNIX	25-07-2019 11:00:07	Служебный процесс		16-03-20:
<input type="checkbox"/> 9ee74281-b745-4f5a-b6ea-06ada4a16bdc	astradrw	ssl://194.85.20.253:30325	SpIDer Guard для UNIX	25-07-2019 11:00:07	Служебный процесс		16-03-20:
<input type="checkbox"/> 9ee74281-b745-4f5a-b6ea-06ada4a16bdc	astradrw	ssl://194.85.20.253:30325	Dr.Web Agent Сканер для UNIX	25-07-2019 11:00:07			
<input type="checkbox"/> 9ee74281-b745-4f5a-b6ea-06ada4a16bdc	astradrw	ssl://194.85.20.253:30325	Dr.Web MailD для	25-07-2019 11:00:07			

Важно!

Возможности Dr.Web позволяют защищать сотрудников компании, работающих не только внутри локальной сети, но и удаленно – как временно, так и постоянно



Dr.Web позволяет:

- Обнаруживать и удалять вредоносные программы любого типа и любой сложности
- Применять политики безопасности, принятые в компании, для защиты, в том числе, устройств удаленных сотрудников
- Контролировать состояние защиты, список установленного ПО, установку обновлений...



DR.WEB ENTERPRISE SECURITY SUITE

Защищает по закону



ИСПДн

до 1 уровня
защищенности
включительно



ГИС/МИС

до 1 класса
защищенности
включительно



Системы обработки
сведений, содержащих
гостайну



Объекты КИИ

вплоть до высшей
категории

- ✓ Государственные гарантии отсутствия в сертифицированных продуктах Dr.Web недеklarированного функционала.
- ✓ Лицензии и сертификаты ФСТЭК России, Минобороны России, ФСБ России.

Все лицензии и сертификаты: https://company.drweb.ru/licenses_and_certificates/



 **Dr.WEB®**
Сделано в России

ЗАЩИТИ СОЗДАННОЕ

Поддерживаем всех

Российские ОС и оборудование

Альт Линукс, Astra Linux, ОС ROSA, Ред ОС 7.1 Муром, Эльбрус-Д, Эльбрус-8.32

Неподдерживаемые Microsoft версии

ОС Windows 7/Vista/XP

Российское ПО

1С
Valo
Р-Платформа

Новейшие версии Microsoft

Windows 10



 © ООО «Доктор Веб», 2003–2020 www.drweb.ru | antivirus_p@drweb.ru



КИИ?

У вас есть Dr.Web!

