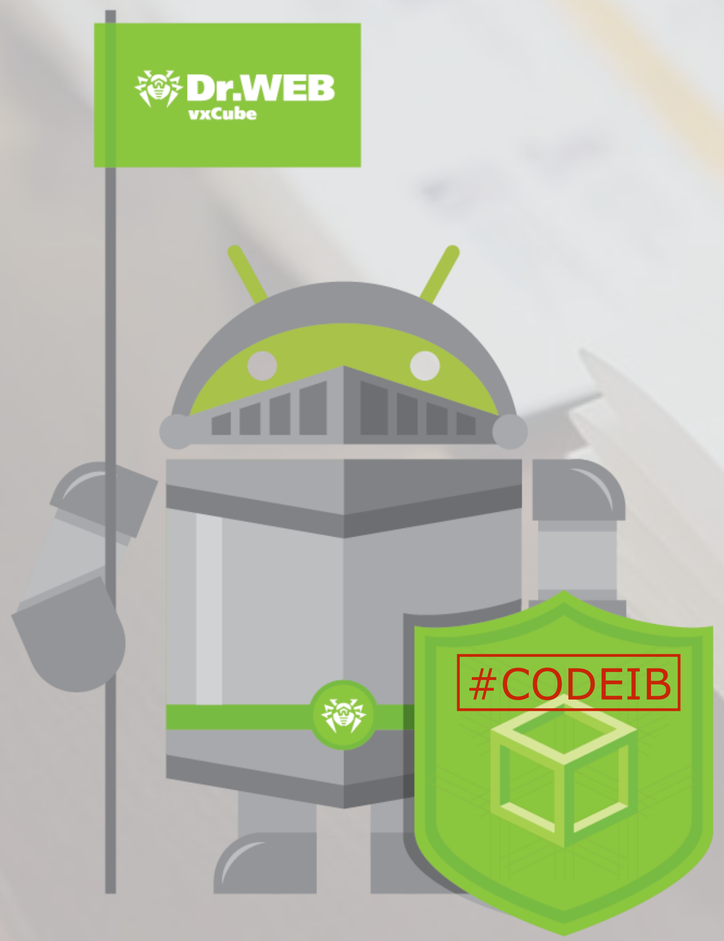
КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

29 НОЯБРЯ 2018 КАЛИНИНГРАД



Инструменты для специалиста по ИБ от Доктор Веб

Dr.WEB®
с 1992 года

Вячеслав Медведев
ООО «Доктор Веб»

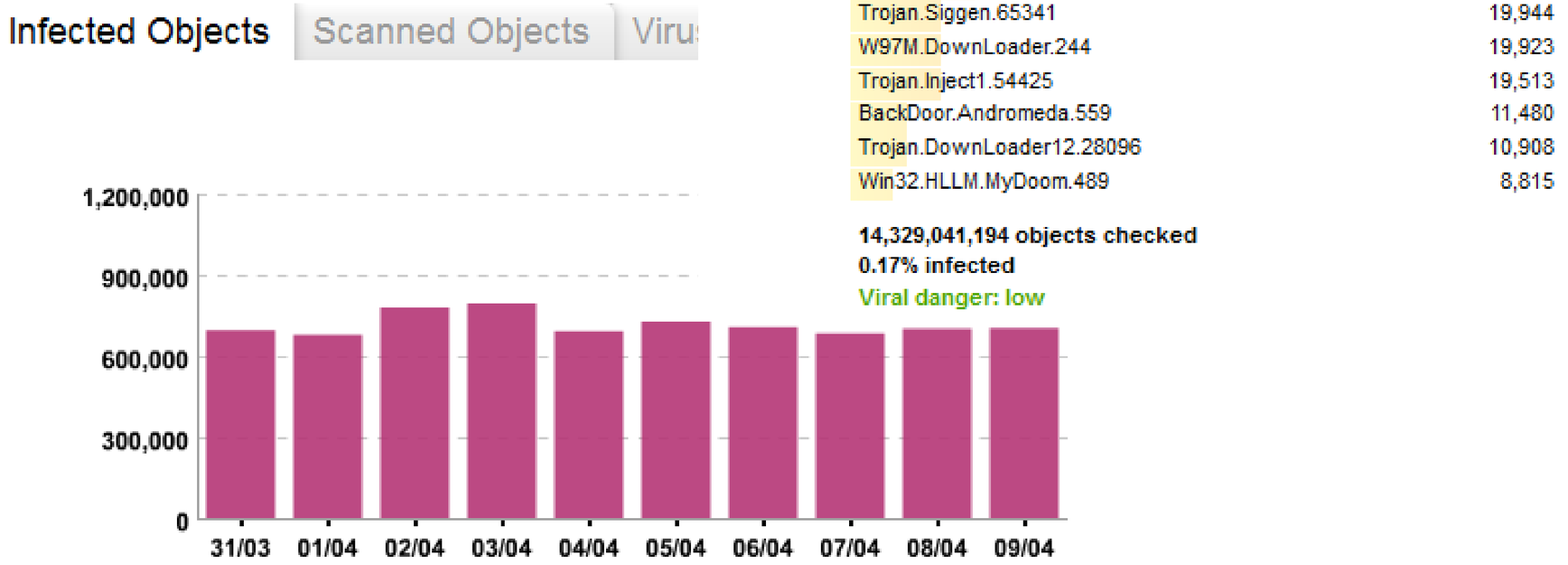
ТЕЛЕФОН: +7 495 789-45-87

EMAIL: v.medvedev@drweb.com

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

В один день
И это далеко не все, что создано…

Live.drweb.com



Dr.WEB®
с 1992 года

Объекты инфраструктуры, подвергавшиеся атакам

Verizon RISK: в 2016 г. 30% получателей писем в компании открыли письма и 12% запустили вложенные к письму файлы

http://www.cnews.ru/articles/2017-05-11_kiberbezopasnost_kak_strategiya_zashchity_biznesaanaliz_ugroz

Плюс очень часто сами сотрудники устанавливают майнеры

Современные майнеры умеют прятаться от пользователей, руками их уже не воз

- защита от перезаписи (не дает ставить другим обладателям нашего продукта майнер на ПК, на котором у
- после запуска загрузчик автоматически удаляется, а майнер остается вшитым в систему;
- возможность самостоятельно криптовать майнер (и даже использовать свой FTP для загрузки майнера с
- все файлы и папки майнера скрыты для пользователя и расположены в системных папках;
- фейковое сообщение об ошибке запуска программы с любым текстом при запуске майнера;
- майнер временно перестает работать, когда запущен диспетчер задач или его аналоги;
- невозможность остановки процессов майнера (3-х уровневая защита от закрытия)
- авто-восстановление удаленного майнера;
- возможность отключить работу диспетчера задачи или его аналогов;
- маскировка автозагрузки под пользовательские процессы;
- файлы майнера на видно и при показе скрытых файлов

Предложение майнеров в сети Интернет

Современные майнеры не только прячутся

Предложение майнеров в сети Интернет

Как правило майнеры относятся к семействам Trojan.BtcMine, Tool.BtcMine, JS.BtcMine, Tool.Mac.BtcMine, Tool.Linux.BtcMine

Несмотря на схожее назначение майнеры могут относиться к самым разным типам и семействам вредоносных- программ. В том числе распознаваться средствами защиты как Java-скрипты или потенциально-опасные утилиты.

В отличии от действий по умолчанию для троянов и червей, которые требуют от антивируса обезвредить найденную инфекцию – действия по умолчанию для типа Tool – этого могут и не требовать

Что делать, если компьютер в сети заражен и нужно вычистить заражение *полностью?*

Что делать?

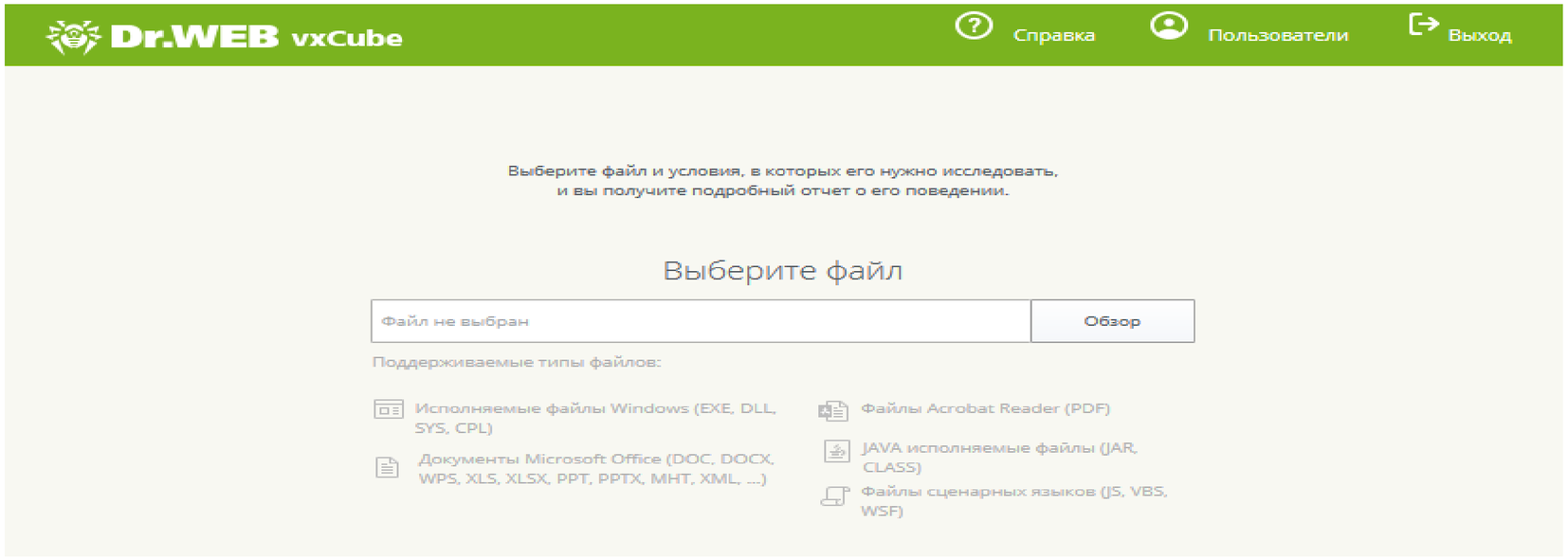
Ждать обновления штатного антивируса?

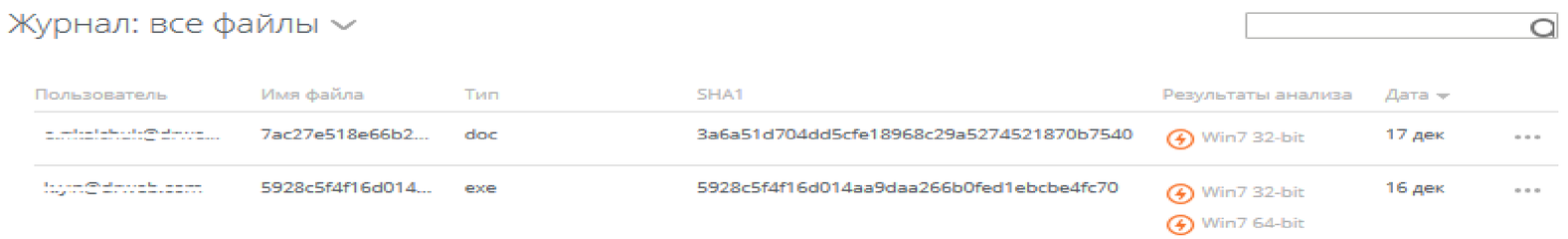
От момента совершения мошеннической операции и до вывода средств проходит 1–3 минуты!

Использовать сервис анализа потенциально вредоносных файлов!

#CODEIB

Отправляем файл на анализ, задав тестовое окружение

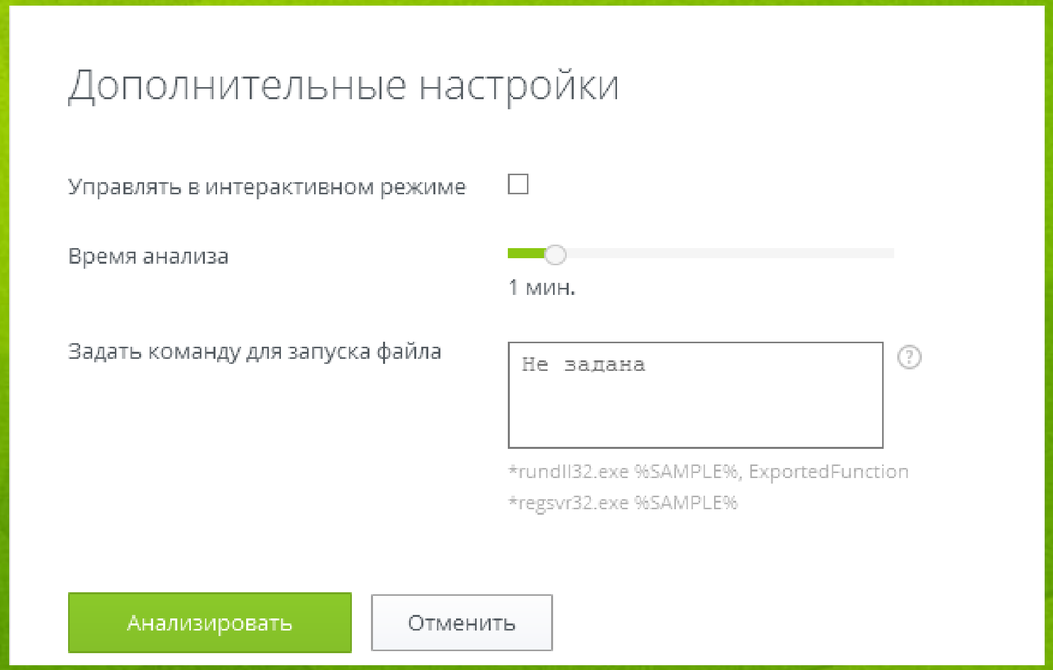




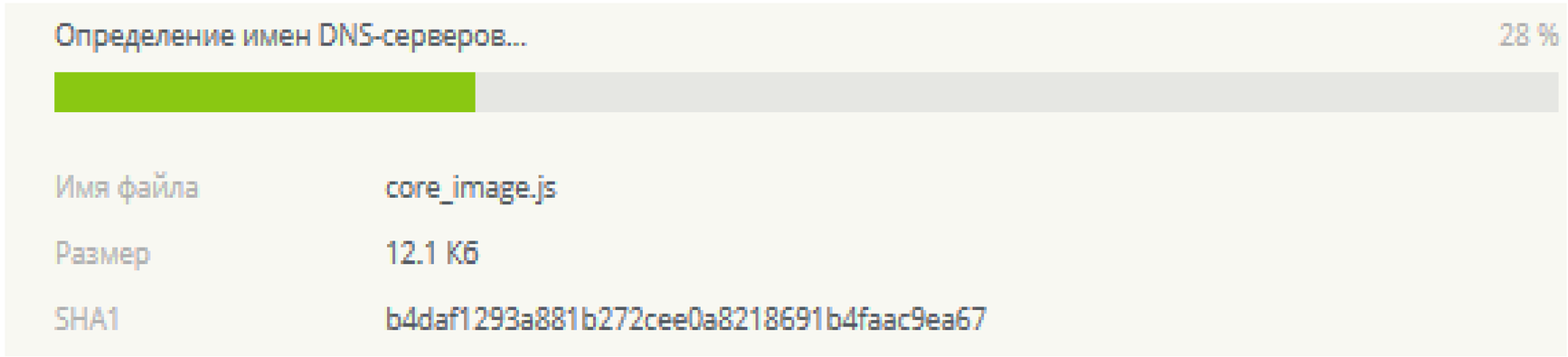
Dr.WEB®
с 1992 года

Сервис анализирует самые опасные типы файлов:

- ✓ Исполняемые файлы Windows и Андроид
- ✓ Документыи служебные файлы Microsoft Office
- ✓ Файлы Acrobat Reader
- ✓ Исполняемые файлы JAVA
- ✓ Скрипт-файлы



Dr.Web vxCube: анализ файла



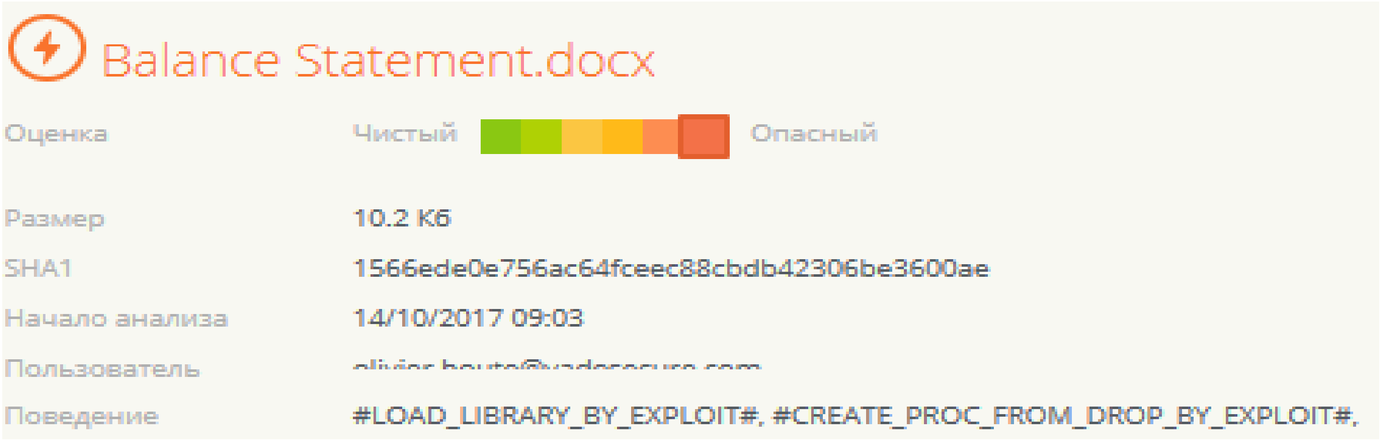
Как правило, проверка занимает не более одной минуты, но если исследователь считает, что этого недостаточно для полного анализа поведения подозрительного файла, желаемое время проверки можно задать в настройках.

Исследователь имеет возможность подключения к анализатору черезVNC для участия в процессе исследования.

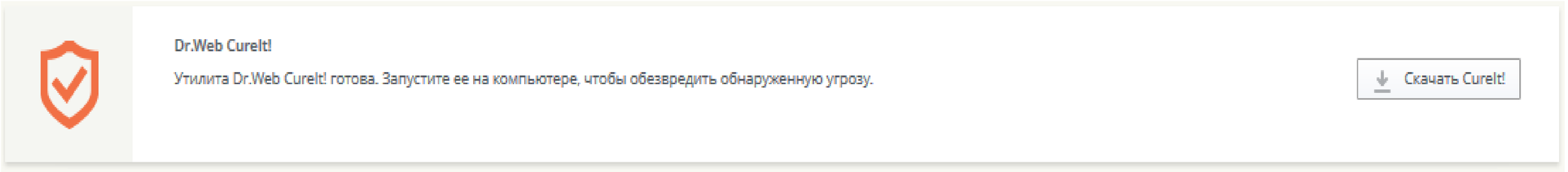
#CODEIB

Результатом анализа является оценка вредоносности файла - «вес» вредоносности по шкале от 0 до 100, а также отчет с техническими подробностями

Отчет содержит список действий исследуемого объекта и их видеосъемку.

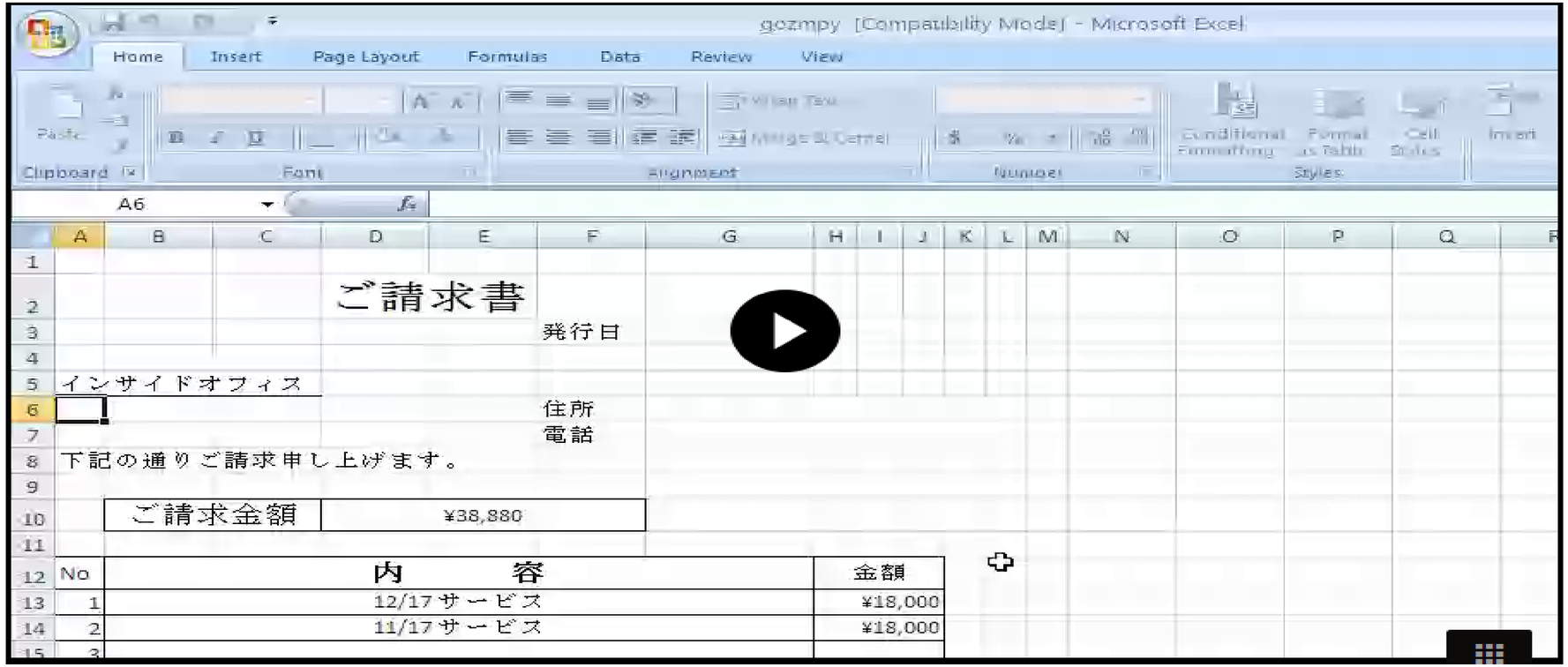


Если файл признан вредоносным, автоматически собирается специальная сборка утилита Dr.Web CureIt! – для лечения именно этой угрозы



#CODEIB

Все действия анализируемой программы записываются, запись действий доступна для последующего анализа - вы можете наблюдать за ходом воспроизведения действий подозрительного объекта.



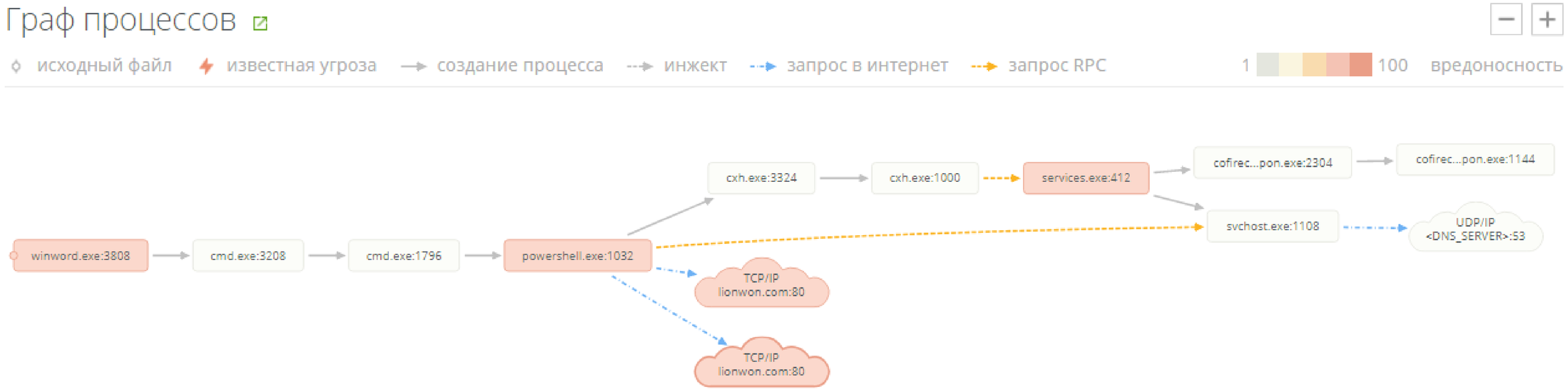
Обзор Техническая информация Файлы и дампы памяти Журнал API Карта сетевой активности

Для анализа также доступна техническая информация, ресурсы, к которым обращается анализируемый файл, список создаваемых им файлов, изменяемых ключей реестра и многое другое

Отчет можно просмотреть в личном кабинете или скачать в виде архива.

Так же в личном кабинете можно ознакомиться с результатами предыдущих проверок

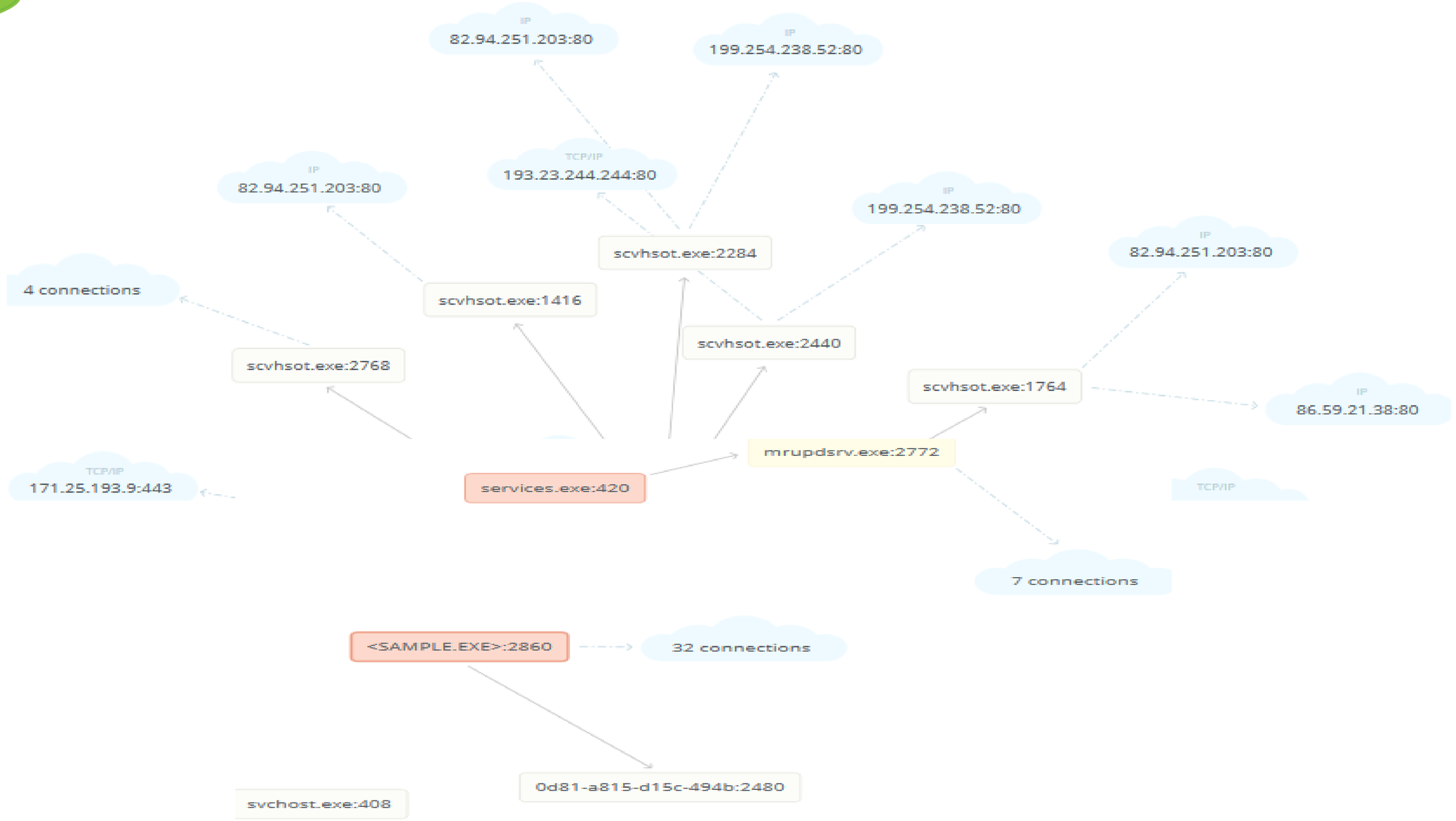
Примеры выявленных связей



Адрес	lionwon.com (47.254.77.6)
Порт	80
Уровень протокола	Транспортный: TCP, Прикладной: HTTP
URL	GET http://www.lionwon.com/8vkOTIP/

! Производится проверка на вредоносность удаленных ресурсов: на графе процессов они помечаются красным, оранжевым или серым в зависимости от степени опасности

Примеры выявленных связей



Ресурсы, используемые вредоносными файлами

Win7 64-bit

Поведение | Обзор | Описание | Файлы и дампы памяти | Журнал API | Карта сетевой активности

Описание

Для обеспечения автозапуска и распространения:

Модифицирует следующие ключи реестра:

> [<HKCU>\Software\Microsoft\Windows\CurrentVersion\RunOnce] 'uSjBVNE' = '%APPDATA%\Roaming\sevnz.exe'

Вредоносные функции:

Создает и запускает на исполнение:

> '%WINDIR%\syswow64\mshta.exe' "javascript:o=new ActiveXObject('Scripting.FileSystemObject');setInterval(function(){try{o.DeleteFile('<Имя файла>.exe');close()}catc
> {}},10);"' (со скрытым окном)

> '%WINDIR%\syswow64\mshta.exe' "javascript:o=new ActiveXObject('WScript.Shell');x=new ActiveXObject('Scripting.FileSystemObject');setInterval(function()
> {try{i=x.GetFile('sevnz.exe').Path;o.RegWrite('HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\RunOnce\\uSjBVNE',i);}catch(e){}},10);"' (со скрытым окном)

> '%WINDIR%\syswow64\mshta.exe' "javascript:eval(new ActiveXObject('WScript.Shell').RegRead('HKCU\\Software\\OXSYN\\SFBFD'));close();"' (со скрытым окном)

> '%APPDATA%\roaming\sevnz.exe' ' (со скрытым окном)

> '<Полный путь к файлу>' ' (со скрытым окном)

> '%WINDIR%\syswow64\cmd.exe' /c copy /y "<Полный путь к файлу>" "%APPDATA%\Roaming\sevnz.exe"' (со скрытым окном)

> '<Полный путь к файлу>' runas' (со скрытым окном)

Запускает на исполнение:

> '%WINDIR%\syswow64\mshta.exe' "javascript:o=new ActiveXObject('WScript.Shell');x=new ActiveXObject('Scripting.FileSystemObject');setInterval(function()
> {try{i=x.GetFile('sevnz.exe').Path;o.RegWrite('HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\RunOnce\\uSjBVNE',i);}catch(e){}},10);"

> '%WINDIR%\syswow64\mshta.exe' "javascript:eval(new ActiveXObject('WScript.Shell').RegRead('HKCU\\Software\\OXSYN\\SFBFD'));close();"

> '%WINDIR%\syswow64\cmd.exe' /c copy /y "<Полный путь к файлу>" "%APPDATA%\Roaming\sevnz.exe"

> '%WINDIR%\syswow64\mshta.exe' "javascript:o=new ActiveXObject('Scripting.FileSystemObject');setInterval(function(){try{o.DeleteFile('<Имя файла>.exe');close()}catc

Ресурсы, используемые вредоносными файлами

Win7 64-bit

Behavior | Overview | Description | Files and dumps | API log | Network activity map

Description

To ensure autorun and distribution:

Creates the following services:

> [<HKLM>\System\CurrentControlSet\Services\mrupdsrv] 'ImagePath' = '"%ProgramFiles(x86)%\Mail.Ru\Update Service\mrupdsrv.exe" --s'

> [<HKLM>\System\CurrentControlSet\Services\mrupdsrv] 'Start' = '00000002'

Malicious functions:

Creates and executes the following:

> '%ProgramFiles(x86)%\mail.ru\update service\mrupdsrv.exe' --s

> '%TEMP%\0d81-a815-d15c-494b' --install

> '%TEMP%\0d81-a815-d15c-494b' --install' (with hidden window)

Modifies file system:

Creates the following files:

> %TEMP%\0d81-a815-d15c-494b

> %ProgramFiles(x86)%\mail.ru\update service\mrupdsrv.exe

> %WINDIR%\syswow64\config\systemprofile\appdata\local\mail.ru\update service\us\d9bf774acb

> %PROGRAMDATA%\mail.ru\id

> <LS_APPDATA>\mail.ru\mailruupdater\us\2d0cd78004

> %WINDIR%\syswow64\grouppolicy\gpt.ini

Deletes the following files:

> %TEMP%\0d81-a815-d15c-494b

Network activity:

Connects to:

> 'xml.binupdate.mail.ru':443

Создаваемые файлы

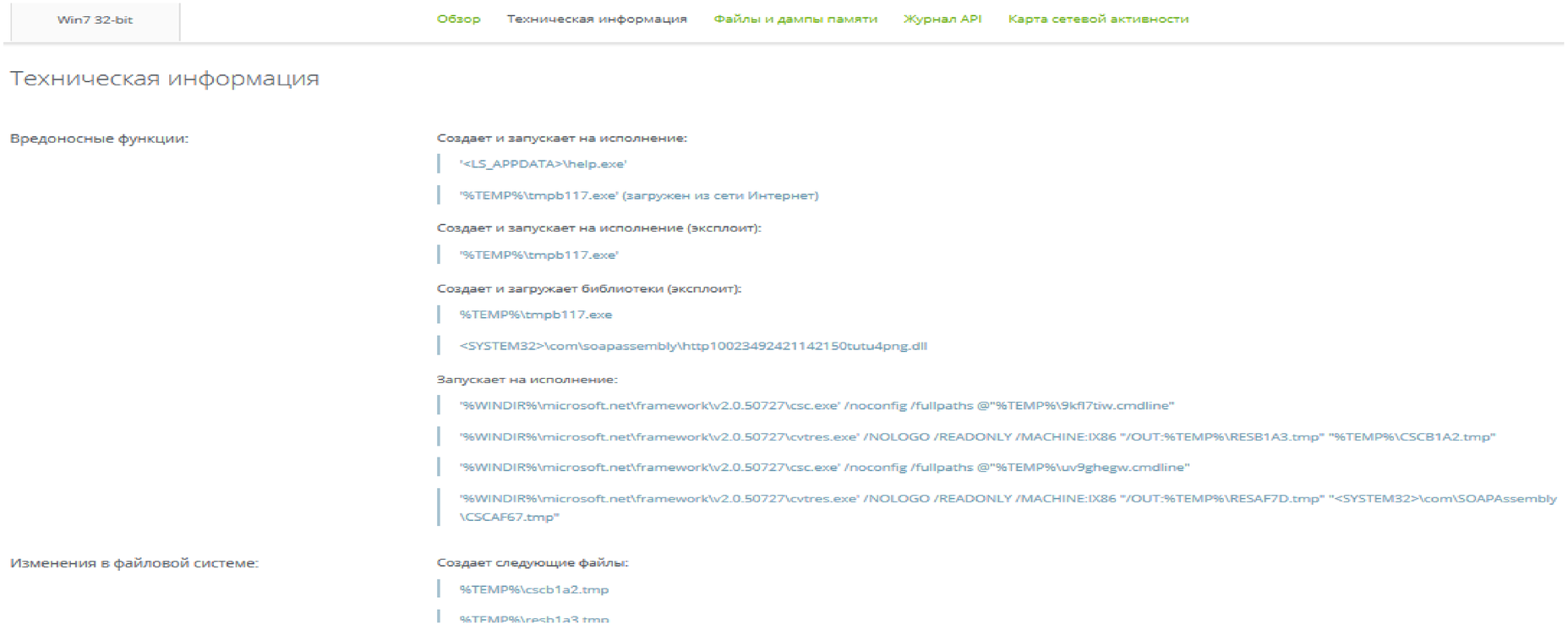
Созданные файлы [50] Файлы и дампы памяти [29]

Путь	SHA1	Обнаружено
%HOMEPATH%\start menu\programs\startup\yddmnlqliny.exe	c1c6d7fa967d4e95d8b61ae8c21a66c3f87cae28	Trojan.Carberp.647
%TEMP%\1.tmp	c1c6d7fa967d4e95d8b61ae8c21a66c3f87cae28	Trojan.Carberp.647
%TEMP%\10.tmp	cc33461f7147042c14d739ba7dc1916e6ccc8139	—
%TEMP%\11.tmp	e4eb14f7a950a30bc632446a9c9b418837378aac	—
%TEMP%\12.tmp	7cf3366c68e402eb3678046fe97651a586044560	—
%TEMP%\13.tmp	f683eb85535e34c41e5bf5da535d9dcc4aefe8b2	—
%TEMP%\14.tmp	08fe9ff1fe9b8fd237adedb10d65fb0447b91fe5	—
%TEMP%\15.tmp	a98e4be7f72f32b0ce5da60e59d2f6256d78bf04	—
%TEMP%\16.tmp	3127dbe44b75c673c24f9ad63675ff91cd9c6321	—
%TEMP%\19.tmp	3cf1eb1003a5342fd0f3495b67ff9bb90c855413	—

1 2 3 4 5 Следующая страница → 1–10 из 50 10

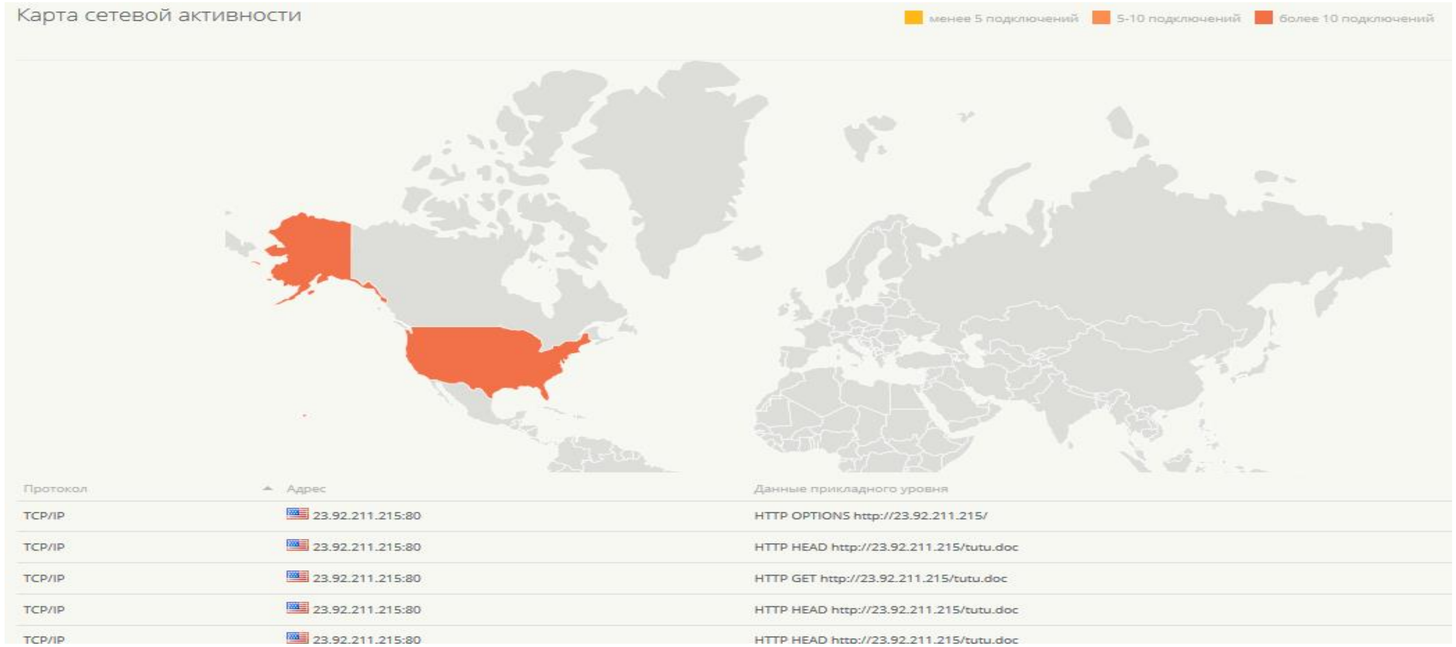
Техническая информация

Воспроизведение действий вредоносной программы
Список локальных и сетевых ресурсов к которым обращается анализируемая программа
Список файлов, внедряемых анализируемой программой в атакуемую систему
Дампы памяти

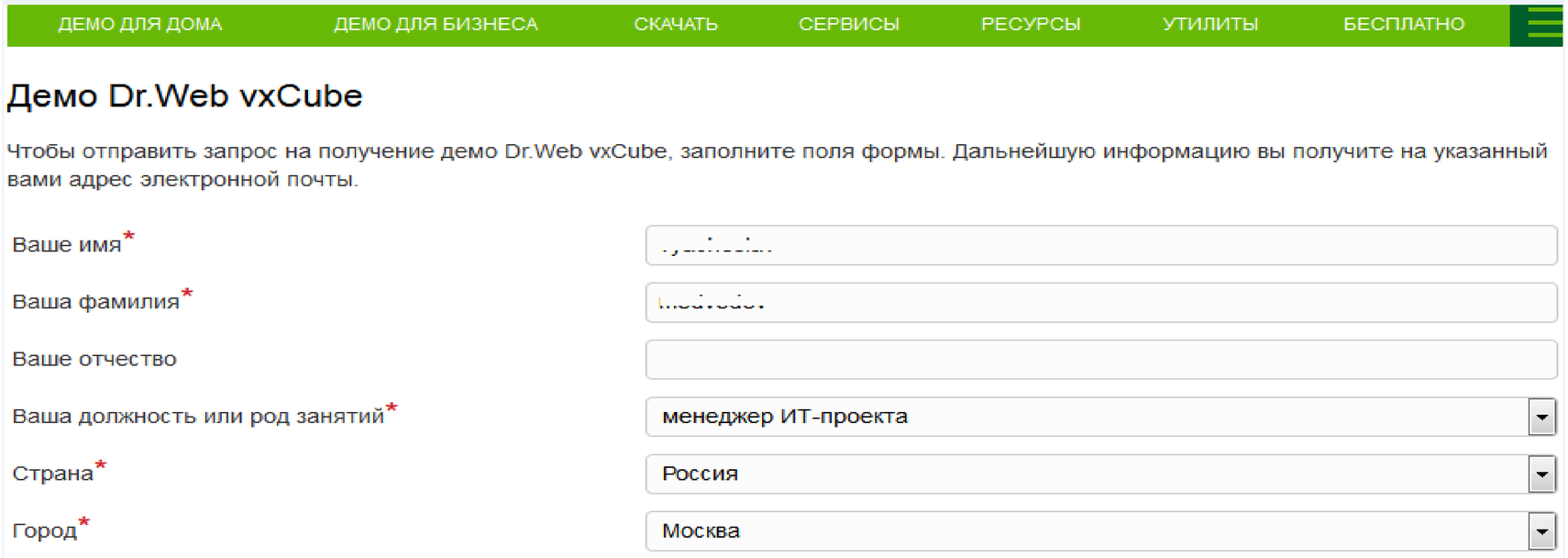


Карта сетевой активности

Будучи запущенной в виртуальной среде вредоносная программа с головой выдает свою вредоносность, в том числе, обращаясь к локальным и сетевым ресурсам. На странице отчета в разделе сетевой активности вы увидите где находятся хосты, к которым обращается анализируемая программа.



Демоверсия



#CODEIB

Сервис имеет возможность интеграции с внутренними системами компании

Администратор компании может получать автоматический ответ о вредоносности файла

#CODEIB

Лицензирование Dr.Web vxCube

	Демо	Коммерческая
Срок действия	10 дней	Согласно купленной лицензии
Количество файлов для проверки	10	
Изготовление специальной сборки Dr.Web CureIt!	Для каждого вредоносного или потенциально опасного файла	
Другие ограничения	1 демодоступ в течение 1 года	—
Стоимость	БЕСПЛАТНО	Зависит от параметров лицензии

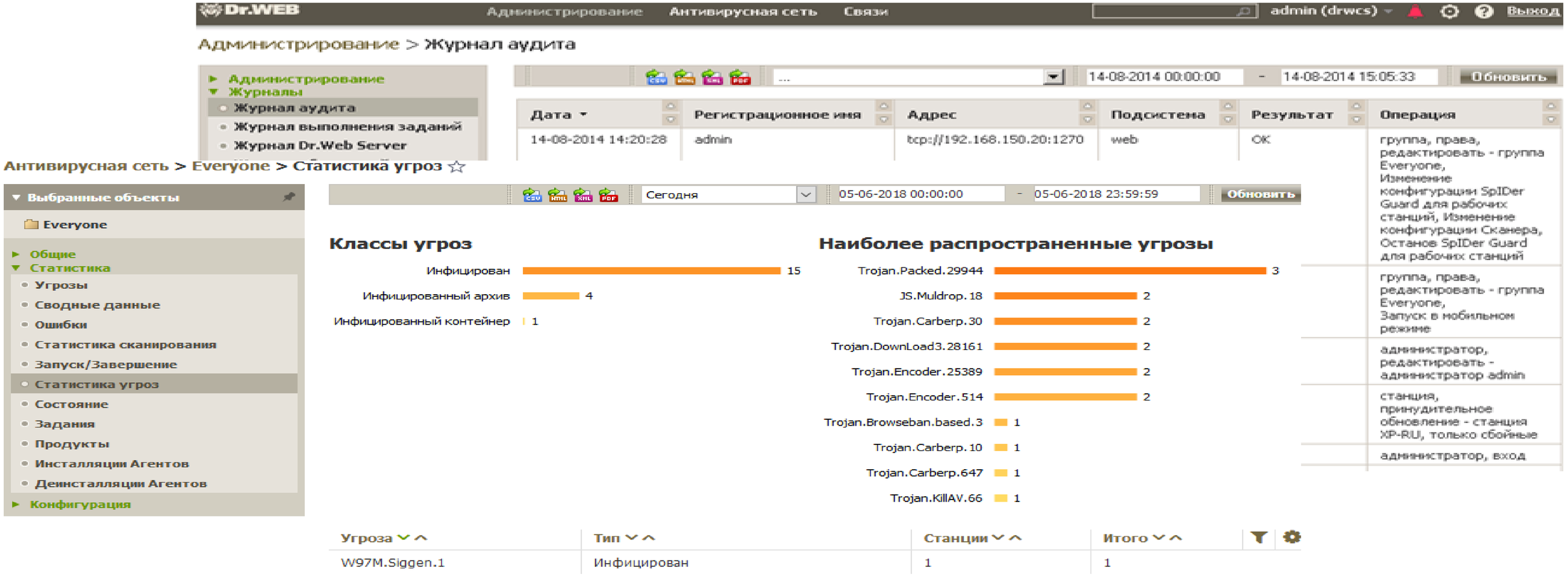
И немного о том, чтобы вам не пришлось пользоваться сервисом

#CODEIB

Dr.WEB®
с 1992 года

Продукты Dr.Web Security Space и Dr.Web Enterprise Security Suite Комплексная защита позволяют защититься даже от угроз, еще не известных вирусным базам

Dr.Web Enterprise Security Suite 11



Dr.Web Enterprise Security Suite 11

1. Обнаружение вредоносных программ с помощью машинного обучения
2. Новые функции безопасности
3. Защита от сканирования
4. Новый интерфейс
5. Новые возможности по работе на плохих линиях связи
6. Возможность настройки для каждого пользователя защищаемой станции
7. Новые возможности Брандмауэра Dr.Web
8. Настройка на основе политик

Машинное обучение (англ. machine learning, ML) — класс методов искусственного интеллекта, характерной чертой которых является не прямое решение задачи, а **обучение** в процессе применения решений множества сходных задач.

Начиная с версии 11.5 модуль SpIDer Guard использует результаты машинного обучения

В новой версии сделан упор на развитие несигнатурных методов детектирования угроз. Это дало:

- Возможность обнаружения угроз без постоянного обращения к вирусным базам – что положительно сказывается как на быстродействии, так и качестве обнаружения новейших угроз
- Обнаружение угроз до фактического исполнения их кода
- Обнаружение популярных в данных момент действий злоумышленников - использование вредоносных майнеров, загрузчиков вредоносного ПО - как активных, так и предназначенных к запуску во всех областях системы

В новой версии сделан упор на развитие несигнатурных методов детектирования угроз – в частности детектирования бестелесных угроз, в которых вредоносный код не сохраняется на диск, а исполняется сразу в памяти, вредоносных майнеров, скриптовых вирусов

Несигнатурное детектирование угроз позволяет отслеживать действия – в частности детектирование подмены ярлыков популярных программ с целью запуска вредоносной ссылки или кода, подмены поиска, стартовой страницы и других настроек в браузерах, подмены прокси-сервера, DNS в системе и популярных браузерах на вредоносные и их лечение

Несанкционированное использование настроек прокси-сервера Windows или настроек непосредственно в используемом браузере может привести к перехвату данных и их воровству

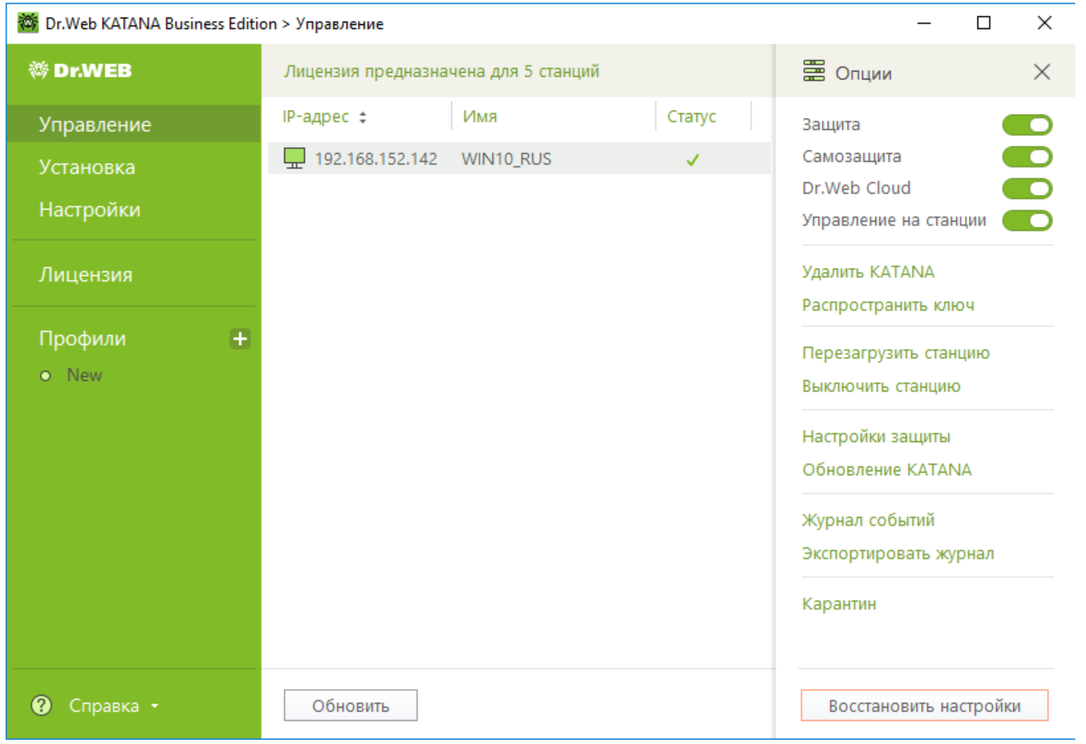
Облако Dr.Web

Использование облачного сервиса Dr.Web позволяет реализовать многие из новых эвристических подходов при детектировании угроз, и является ключевой составляющей эффективной защиты новой версии.

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

А если у вас не Dr.Web?

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ



Dr.Web Katana защищает от использования эксплойтами как уже известных, так и еще неизвестных уязвимостей.

В отличие от традиционного сигнатурного анализа **Dr.Web Katana** анализирует угрозы «на лету» – непосредственно в процессе попыток использования уязвимостей в защищаемой системе.

Новая стоимость надежного продукта

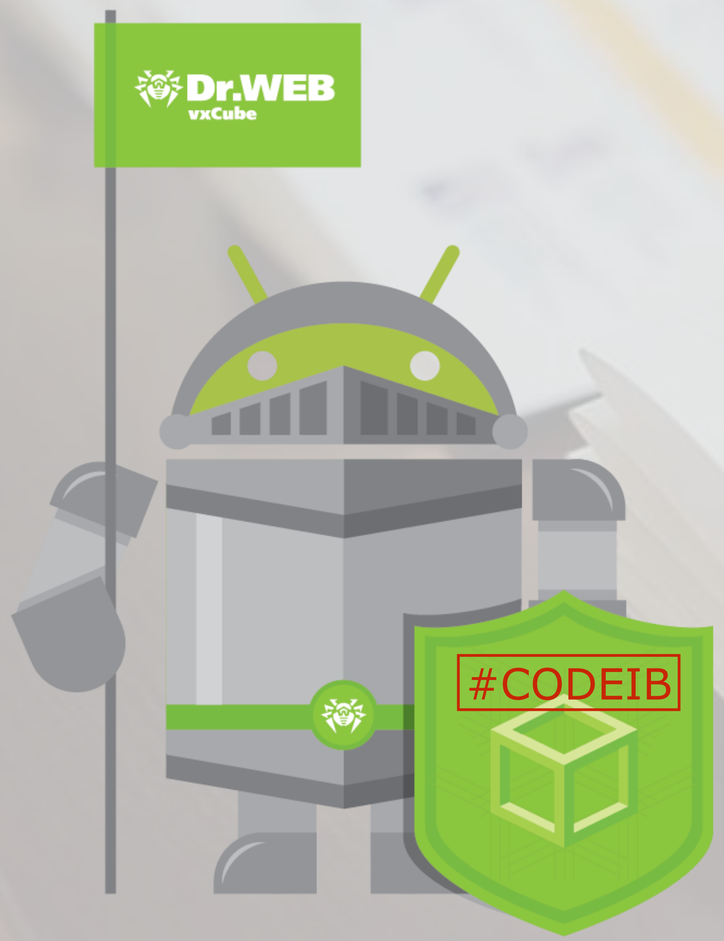
При продаже Dr.Web для 9 и более серверов … стоимость защиты сервера приравнена к стоимости защиты рабочей станции

https://pa.drweb.com/info/?i=12745

«Доктор Веб» – это выгодно!

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

29 НОЯБРЯ 2018 КАЛИНИНГРАД



Благодарим за внимание!

Номер службы технической поддержки

8-800-333-7932

Запомнить просто! –
возникла проблема – набери DRWEB!

8-800-33-DRWEB

Dr.WEB®
с 1992 года