

Незримая угроза: как ее обнаружить и обезвредить

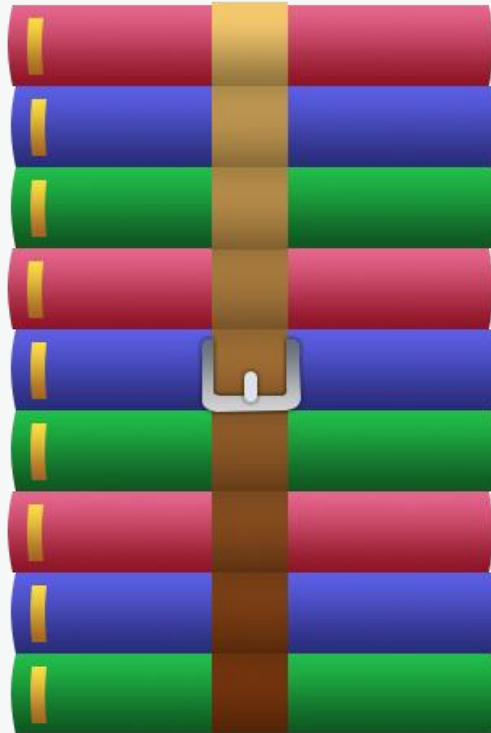
Насколько хорошо защищает антивирус?



Оставаться в тени как можно дольше



Разнообразие упаковок



- Мультисканер проверяет только известен ли файл **вирусным базам** — никакой гарантии «чистоты».
- Легальные мультисканеры передают новые файлы вендорам, для добавления в базы, если они вредоносные.

Мульти-пульти прошлый век («Антивирусная Правда!»)

<https://www.drweb.ru/pravda/issue/?number=1073&lng=ru>



Изучение работы антивируса



Ожидание часа X или действия



Сочетание разных приемов



Трояны в легальном ПО



Идеальной защиты не бывает



**НОВАЯ
ВЕРСИЯ 12**

Dr.Web Enterprise Security Suite
Всё под контролем

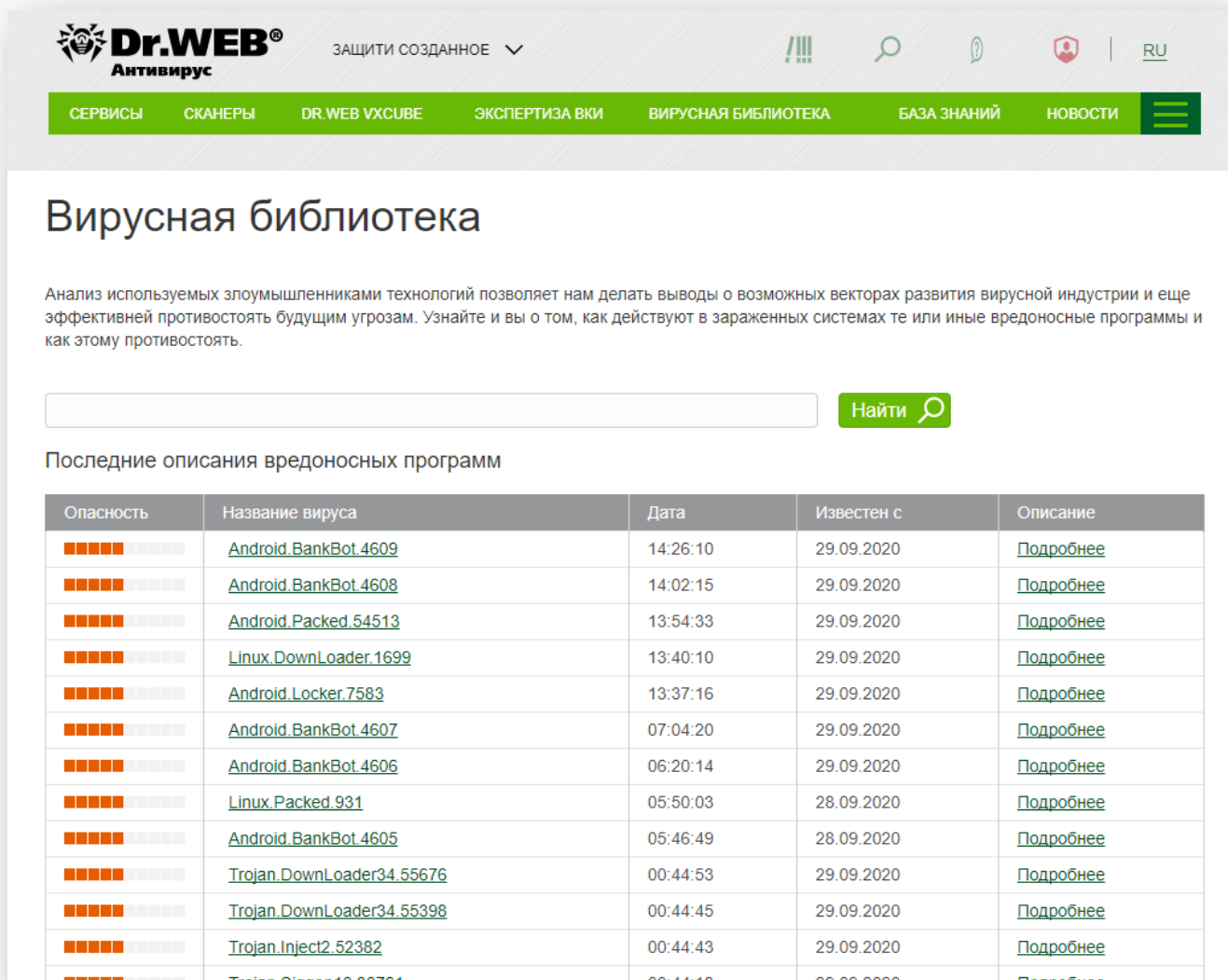
Что нового?



The image shows a 3D rendering of the Dr.Web Enterprise Security Suite software box. The box is black with green and white text and graphics. It features the Dr.Web logo and the text 'Dr.Web Enterprise Security Suite' and 'Централизованная защита всех узлов корпоративной сети'. The box is set against a background of glowing green hexagonal patterns.



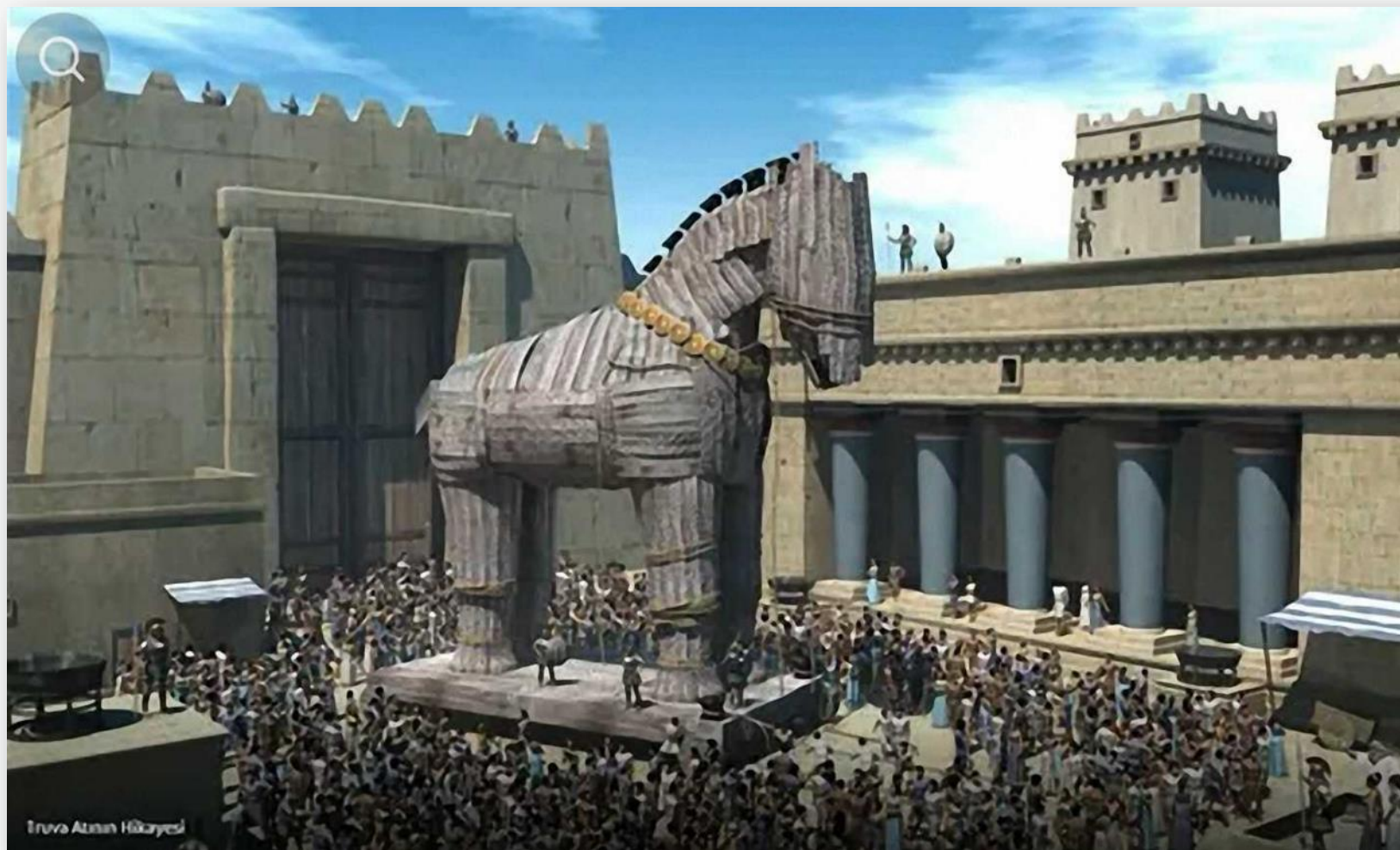
vms.drweb.ru/search



The screenshot shows the Dr.Web Virus Library website. At the top, there is a navigation bar with the Dr.Web logo and the text "ЗАЩИТИ СОЗДАННОЕ". Below the navigation bar, there is a green header with menu items: "СЕРВИСЫ", "СКАНЕРЫ", "DR.WEB VXСUBE", "ЭКСПЕРТИЗА ВКИ", "ВИРУСНАЯ БИБЛИОТЕКА", "БАЗА ЗНАНИЙ", and "НОВОСТИ". The main content area is titled "Вирусная библиотека" and contains a paragraph of text about the analysis of technologies used by attackers. Below the text is a search bar with a "Найти" button. Underneath the search bar, there is a section titled "Последние описания вредоносных программ" followed by a table of virus descriptions.

Опасность	Название вируса	Дата	Известен с	Описание
■■■■■	Android.BankBot.4609	14:26:10	29.09.2020	Подробнее
■■■■■	Android.BankBot.4608	14:02:15	29.09.2020	Подробнее
■■■■■	Android.Packed.54513	13:54:33	29.09.2020	Подробнее
■■■■■	Linux.DownLoader.1699	13:40:10	29.09.2020	Подробнее
■■■■■	Android.Locker.7583	13:37:16	29.09.2020	Подробнее
■■■■■	Android.BankBot.4607	07:04:20	29.09.2020	Подробнее
■■■■■	Android.BankBot.4606	06:20:14	29.09.2020	Подробнее
■■■■■	Linux.Packed.931	05:50:03	28.09.2020	Подробнее
■■■■■	Android.BankBot.4605	05:46:49	28.09.2020	Подробнее
■■■■■	Trojan.DownLoader34.55676	00:44:53	29.09.2020	Подробнее
■■■■■	Trojan.DownLoader34.55398	00:44:45	29.09.2020	Подробнее
■■■■■	Trojan.Inject2.52382	00:44:43	29.09.2020	Подробнее
■■■■■	Trojan.Siggen10.30761	00:44:40	29.09.2020	Подробнее





The screenshot shows a web browser window with the address bar displaying `https://la.drweb.com/login`. The page features the Dr.Web FixIt! logo at the top center. Below the logo is a white login form with the following elements:

- Вход** (Login) header
- Input field for "Электронная Почта" (Email)
- Input field for "Пароль" (Password)
- "Войти" (Login) button
- Checkbox for "Запомнить меня" (Remember me)

The browser's taskbar at the bottom shows the Windows logo, search icon, and several application icons. The system tray on the right indicates the time as 12:56 and the date as 17.09.2020, along with language and volume settings.



Dr.Web FixIt! https://la.drweb.com/tasks

Dr.WEB FixIt!

Список задач (12)

Задача	Описание	Статус	Отчеты	Результаты анализа	Изменено
000333	Проверка на вредоносное ПО нулевого дня.	Открыта	1	Инфицированные	15.09.20 18:35
000282	Диагностика ПК бухгалтера.	Открыта	2	Руткиты	13.08.20 19:13
000192	Проверить компьютер еще раз	Открыта	1	Инфицированные	01.06.20 13:48
000188	Проверка компьютера	Открыта	3	Инфицированные	22.05.20 22:30
000185	Проверка компьютера в гостиной.	Закрыта	3	Инфицированные	22.05.20 21:55
000184	Проверка компьютера в гостиной.	Закрыта	1	Инфицированные	20.05.20 17:30
000182	Тест 2	Закрыта	1	Инфицированные	20.05.20 00:33
000181	Тест 1	Закрыта	1	Инфицированные	20.05.20 00:05
000178	тест на вирусах	Открыта	0	Неизвестные	16.05.20 17:16

12:56 17.09.2020



Dr.Web FixIt! x +

← → ↻ 🏠 🔒 <https://la.drweb.com/tasks/new> ☆ ☆ 🗑️ 👤 ⋮

← Новая задача

1 Создать задачу ————— 2 Загрузить отчет

Описание задачи

Поиск новой угрозы.

19 / 250

Настройка FixIt!

- Автоматически загружать отчеты:
 - В эту задачу
 - На URL
- Отправлять статистику об обнаруженных угрозах и применяемых действиях
- Использовать Dr.Web Cloud
- Сбирать подозрительные файлы

Отмена **Создать задачу**

Windows taskbar: 🏠 🔍 🕒 📁 🌐 🇷🇺 🗑️ 📄 🗑️ 🔊 🇷🇺 12:57 17.09.2020 🗨️




Dr.Web FixIt!

← Задача 000335

> Поиск новой угрозы.

1 Создать задачу — 2 Загрузить отчет



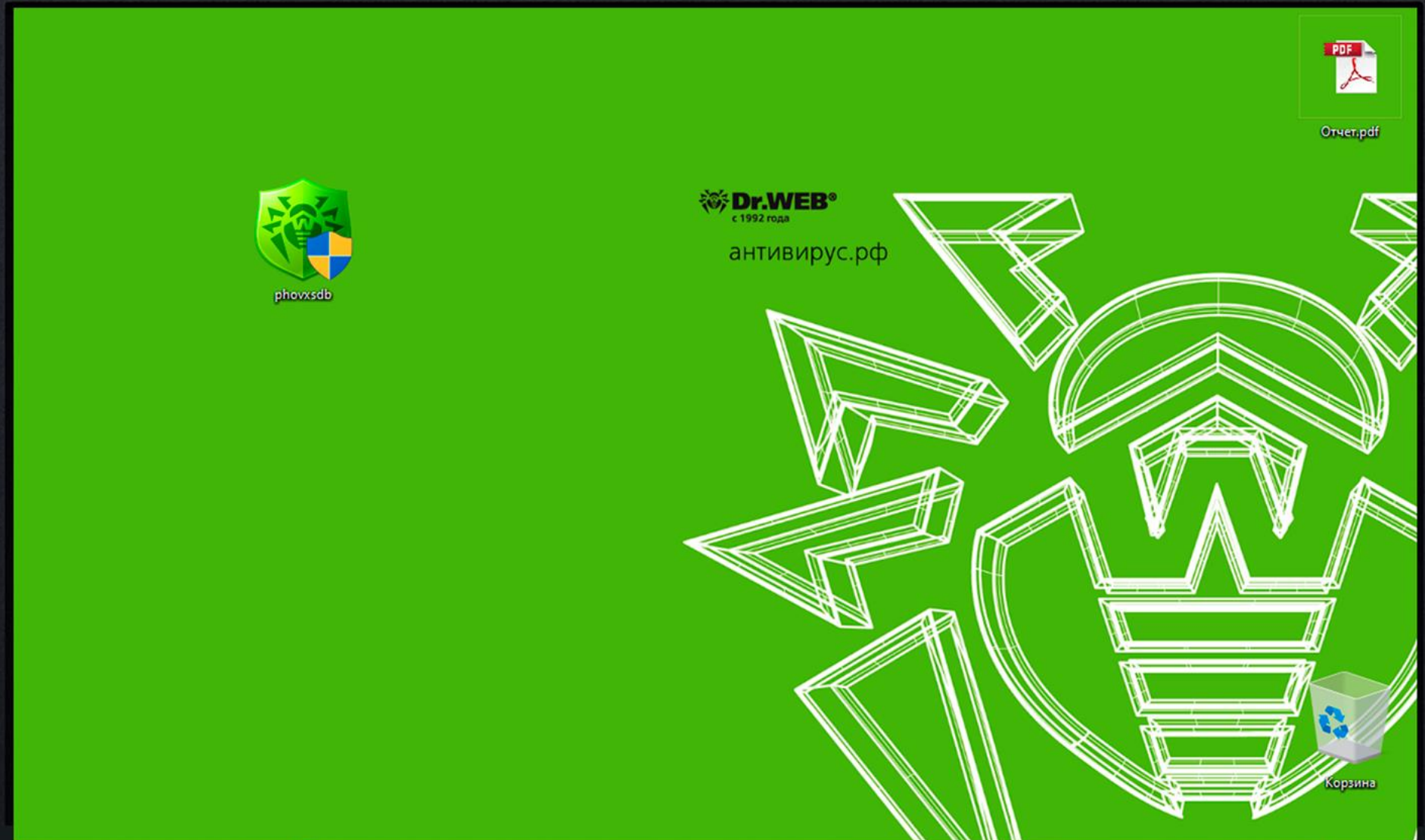
Как загрузить отчет

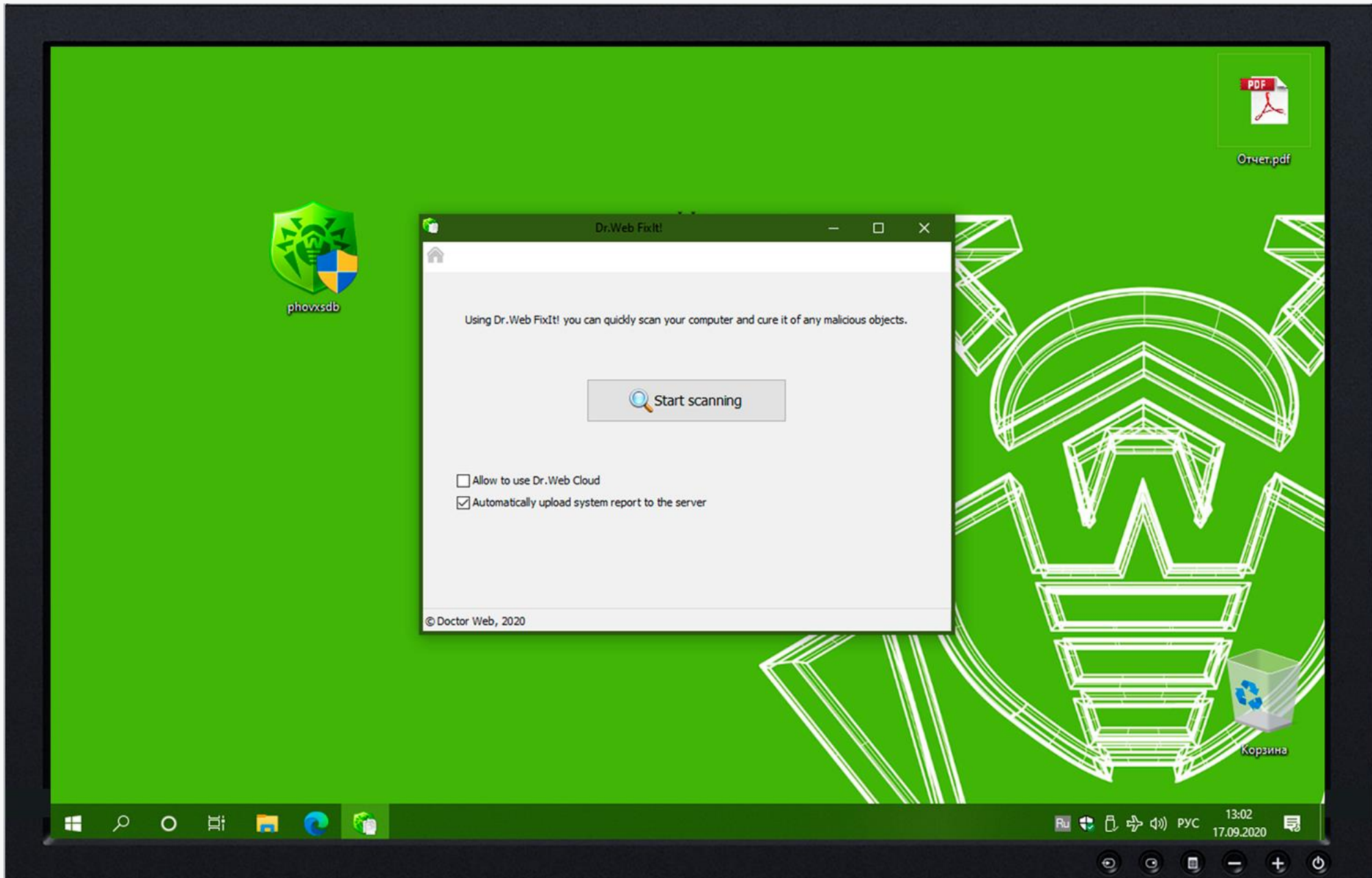
Чтобы получить отчет, скачайте утилиту FixIt! и отправьте клиенту. FixIt! проверит компьютер клиента и сформирует отчет.
Если FixIt! не загрузит отчет автоматически, загрузите его вручную.

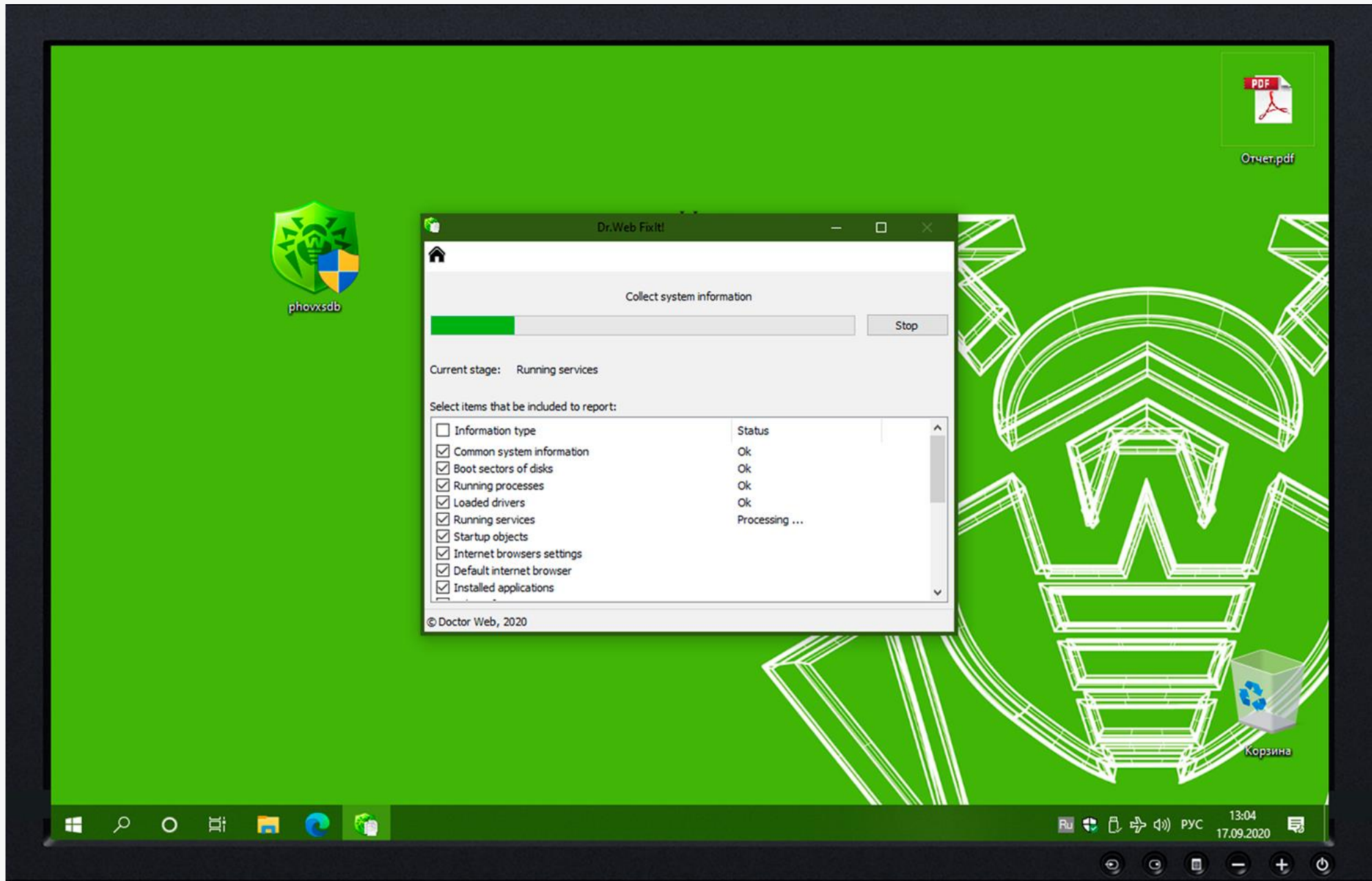
Загрузить отчет Скачать FixIt!

12:57
17.09.2020









Dr.Web Fixit!

Collect system information

Stop

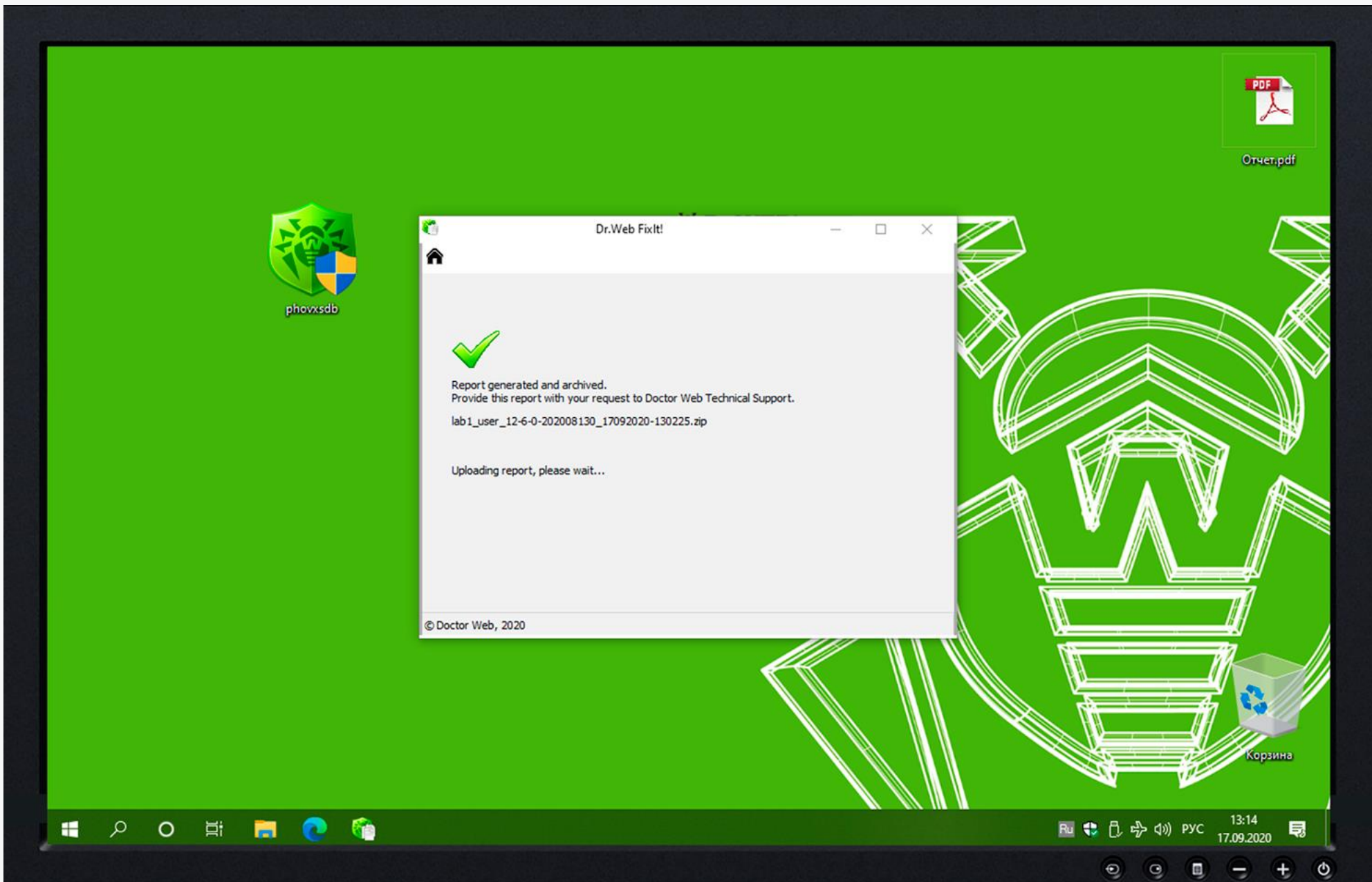
Current stage: Running services

Select items that be included to report:

<input type="checkbox"/>	Information type	Status
<input checked="" type="checkbox"/>	Common system information	Ok
<input checked="" type="checkbox"/>	Boot sectors of disks	Ok
<input checked="" type="checkbox"/>	Running processes	Ok
<input checked="" type="checkbox"/>	Loaded drivers	Ok
<input checked="" type="checkbox"/>	Running services	Processing ...
<input checked="" type="checkbox"/>	Startup objects	
<input checked="" type="checkbox"/>	Internet browsers settings	
<input checked="" type="checkbox"/>	Default internet browser	
<input checked="" type="checkbox"/>	Installed applications	

© Doctor Web, 2020





Dr.Web FixIt!

✓

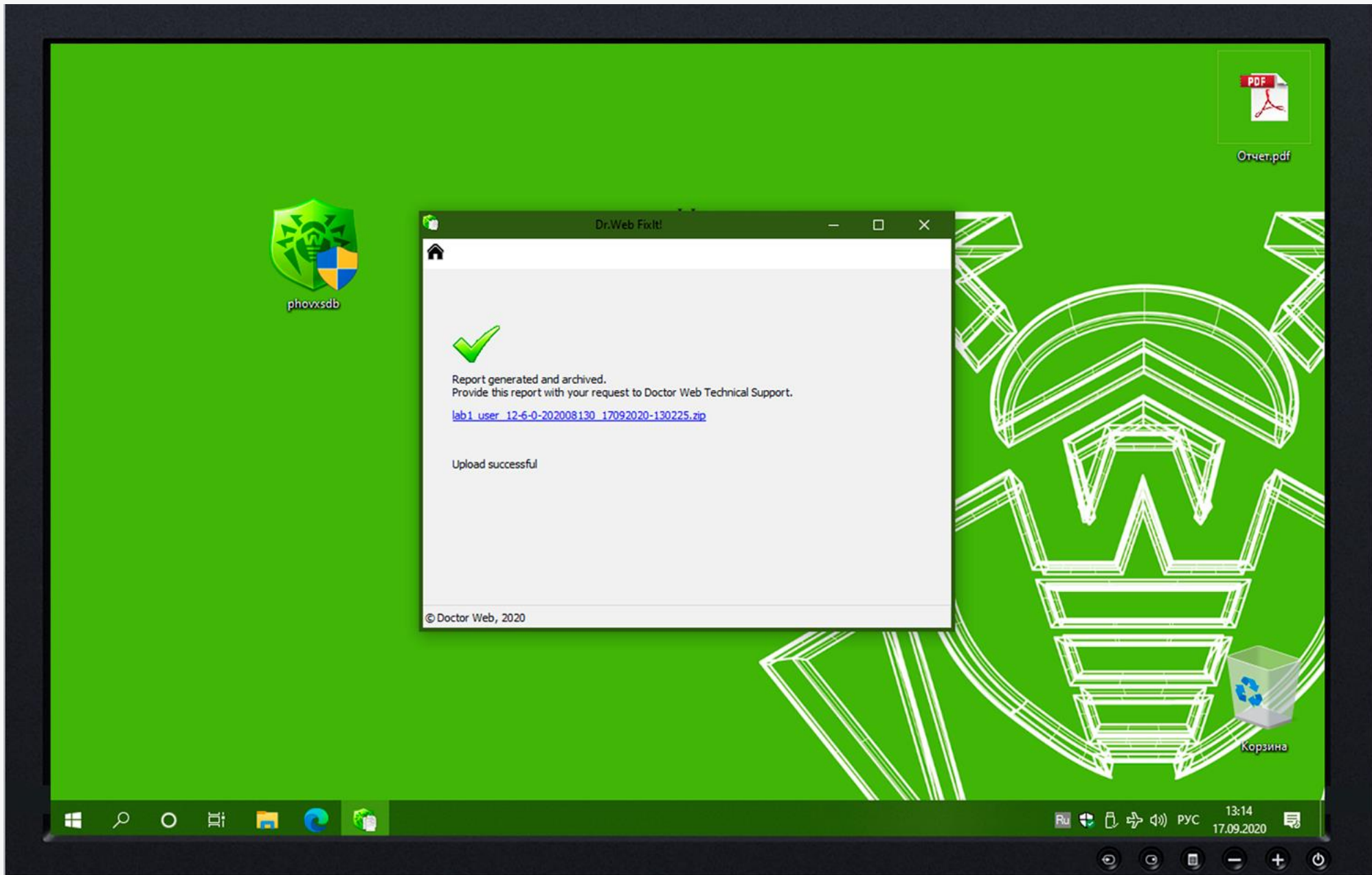
Report generated and archived.
Provide this report with your request to Doctor Web Technical Support.

lab1_user_12-6-0-202008130_17092020-130225.zip


Uploading report, please wait...

© Doctor Web, 2020





Dr.Web FixIt!



Report generated and archived.
Provide this report with your request to Doctor Web Technical Support.

[lab1_user_12-6-0-202008130_17092020-130225.zip](#)

Upload successful

© Doctor Web, 2020



Dr.Web FixIt! x +

← → ↻ 🏠 🔒 <https://la.drweb.com/tasks/item/335> 🔍 ☆ ⭐ 🗑️ 👤 ⋮

Dr.WEB FixIt! 👤

← Задача 000335

> Поиск новой угрозы.

Дата создания: 17.09.20 12:57 Клиент: LAB1 Загружено отчетов: 1
Кем создано: Kirill Tezikov ОС: Microsoft Windows 10 Ente... Ключ: BC6297DB2D89702BF... 📄

Фильтр Легенда

🔍 Поиск

statuses: Инфицированные ✕

Статус объекта | Инфицированные | Руткиты | Подозрительные | Неизвестные | Ненайденные | Доверенные

+ Отчет 1

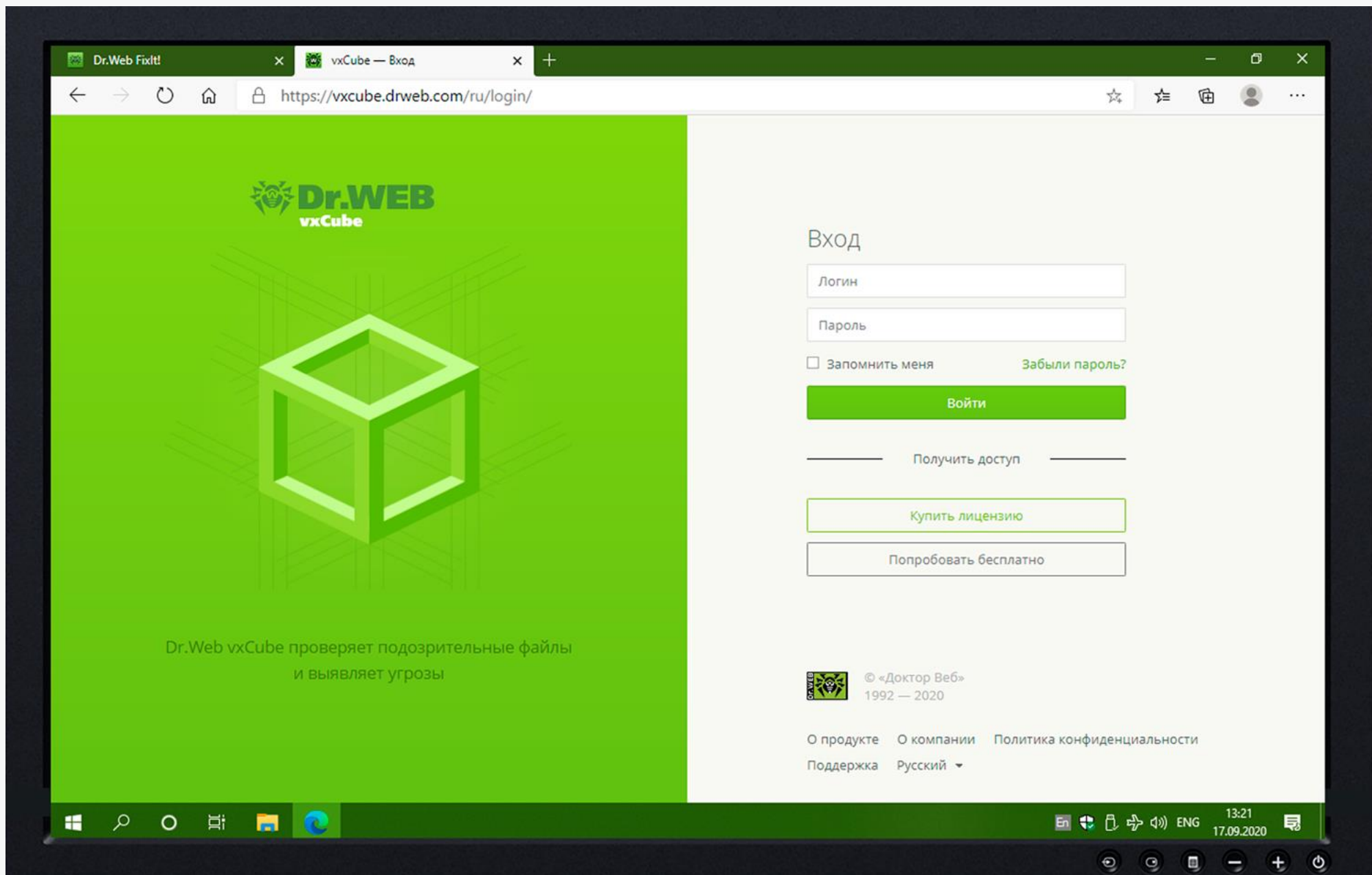
Дата создания: 17.09.20 13:14 Отфильтровано объектов: 2 из 19609 📄 Скачать отчет

▼ Несигнатурные детекты 1 / 1

- ▼ Инфицированные | 1
 - Отчет.pdf.exe C:\users\user\desktop\Отчет.pdf.exe

Windows taskbar: 🏠 🔍 🕒 📁 🌐 🇷🇺 🗑️ 📄 🗑️ 🔊 🇷🇺 13:17 17.09.2020 🗨️





Dr.Web FixIt

vxCube — Главная страница

https://vxcube.drweb.com/ru/main/

Лицензия Справка Профиль

Загрузите файл и выберите условия для анализа.
Вы получите подробный отчет о результатах проверки.

Выберите файл [9/100]

Файл не выбран Обзор

Поддерживаемые форматы файлов

- Исполняемые файлы Windows:
EXE, DLL, CPL, SYS, NATIVE APP
- Исполняемые файлы Java:
JAR, CLASS
- Пакеты Android:
APK
- Файлы сценарных языков:
JS, VBS, WSF, JSE, VBE, PS1 и т. д.
- Документы Microsoft Office:
DOC, DOCX, WPS, XLS и т. д.
- Другие:
MOF, LNK, HTA, CHM
- Файлы Acrobat Reader:
PDF

13:21
17.09.2020



Dr.Web FixIt! vxCube — Главная страница

https://vxcube.drweb.com/ru/main/ Лицензия Справка Профиль

Dr.WEB
vxCube

Загрузите файл и выберите условия для анализа.
Вы получите подробный отчет о результатах проверки.

Выберите файл [9/100]

Отчет.pdf.exe EXE Обзор

Выберите ОС: Windows XP 32-bit Windows 7 32-bit Windows 7 64-bit
 Windows 10 64-bit

Анализировать

Дополнительные настройки

Журнал: все файлы

13:21 17.09.2020 ENG



Dr.Web FixIt | vxCube — Главная страница | <https://vxcube.drweb.com/ru/main/>

Dr.WEB vxCube

Лицензия | Справка | Профиль

Дополнительные настройки

- Использовать VNC
- Отслеживать все процессы при использовании VNC
- Время выполнения файла 1 мин.
- Ограничение на общий размер созданных файлов МБ
- Задать команду для запуска файла
 - *rundll32.exe %SAMPLE%, ExportedFunction
 - *regsvr32.exe %SAMPLE%
- Тип подключения

Анализировать | Отменить

Журнал: все файлы

13:21 17.09.2020



Dr.Web FixIt vxCube — Отчет

https://vxcube.drweb.com/ru/report/106222

← Назад WinXP 32-bit Win7 32-bit Win7 64-bit Win10 64-bit

Проверка модулей браузеров... 60%

Имя файла	Отчет.pdf.exe
Размер	36.0 KB
Формат	EXE
SHA1	a1a73cefb5ed8f15d1bec517d20f8a9cf9b03525
Начало анализа	17/09/2020 13:22

Использовать VNC


17.09.2020 13:24 ENG




Dr.Web FixIt! vxCube — Отчет

https://vxcube.drweb.com/ru/report/106222

← Назад WinXP 32-bit Win7 32-bit Win7 64-bit Win10 64-bit

 **Dr.Web CureIt!**
Dr.Web vxCube определил, что файл является вредоносным. Идет создание утилиты Dr.Web CureIt! для обезвреживания угрозы. [Скачать CureIt!](#)

Отчет.pdf.exe

Оценка	Чистый  Опасный
Обнаружено	Опасное поведение
	Угрозы в файлах и дампах памяти
Размер	36.0 KB
Формат	EXE
SHA1	a1a73cefb5ed8f15d1bec517d20f8a9cf9b03525

Дополнительно ▾

[Скачать исходный файл](#) [Скачать архив](#) [Скачать отчет](#) [Скачать PCAP](#)

[Поведение](#) [Граф процессов](#) [Описание](#) [Файлы и дампы памяти](#) [Журнал API](#) [Карта сетевой активности](#)

13:25 17.09.2020



Dr.Web FixIt! vxCube — Отчет

https://vxcube.drweb.com/ru/report/106222

Win10 64-bit Поведение Граф процессов Описание Файлы и дампы памяти Журнал API Карта сетевой активности

Поведение

Вредоносное | Несанкционированное внедрение в системный процесс

Подозрительное | Нет данных

Нейтральное | Отправка UDP-запроса • Запуск процесса • Запуск стандартного отладчика Windows (dwwin.exe)

Граф процессов

φ исходный файл ⚡ известная угроза → создание процесса ⇨ инъект ⇨ запрос в интернет ⇨ запрос RPC ⚙ вредоносный модуль

вредоносность 1 100

```
graph TD; Sample["<SAMPLE.EXE>:1972"]; Werfault["werfault.exe:3968"]; Svchost3804["svchost.exe:3804"]; Svchost280["svchost.exe:280"]; Internet["::ffff:...52:5355<br/>4 подключения"]; Sample -- "инъект" --> Werfault; Sample -- "инъект" --> Svchost3804; Svchost280 -.-> Internet;
```

https://vxcube.drweb.com/ru/report/106222#tab-227849

13:25 17.09.2020



Dr.Web FixIt! vxCube — Отчет

https://vxcube.drweb.com/ru/report/106222

Win10 64-bit Поведение **Граф процессов** Описание Файлы и дампы памяти Журнал API Карта сетевой активности

Граф процессов

⚙ исходный файл ⚡ известная угроза → создание процесса ↔ инъект → запрос в интернет → запрос RPC ⚙ вредоносный модуль

вредоносность
1 100

```

    graph TD
      Sample["⚡ <SAMPLE.EXE>:1972"]
      Werfault["werfault.exe:3968"]
      Svchost3804["svchost.exe:3804"]
      Svchost280["svchost.exe:280"]
      Svchost3712["svchost.exe:3712"]
      Internet["::ffff:...52:5355  
4 подключения"]

      Sample --> Werfault
      Sample -.-> Svchost3804
      Sample -.-> Svchost280
      Svchost280 -.-> Internet
      Svchost3712 -.-> Svchost280
  
```

PID 1972
 https://vxcube.drweb.com/ru/report/106222#tab-227849 <SAMPLE.EXE>

13:25 17.09.2020



Dr.Web FixIt! vxCube — Отчет

https://vxcube.drweb.com/ru/report/106222

Win10 64-bit

Поведение Граф процессов **Описание** Файлы и дампы памяти Журнал API Карта сетевой активности

Описание

Вредоносные функции	Внедряет код в следующие системные процессы: %WINDIR%\syswow64\svchost.exe
Сетевая активность	UDP ::ffff:224.0.0.252:5355
Другое	Запускает на исполнение '%WINDIR%\syswow64\svchost.exe'

Созданные файлы [15] Дампы памяти [136]


13:26 17.09.2020 ENG





Dr.Web FixIt! vxCube — Отчет

https://vxcube.drweb.com/ru/report/106222

← Назад WinXP 32-bit Win7 32-bit Win7 64-bit Win10 64-bit

 **Dr.Web CureIt!**
Утилита Dr.Web CureIt! готова. Запустите ее на компьютере, чтобы обезвредить обнаруженную угрозу. [Скачать CureIt!](#)

 **Отчет.pdf.exe**

Оценка	Чистый  Опасный
Обнаружено	Опасное поведение Угрозы в файлах и дампах памяти
Размер	36.0 KB
Формат	EXE
SHA1	a1a73cefb5ed8f15d1bec517d20f8a9cf9b03525

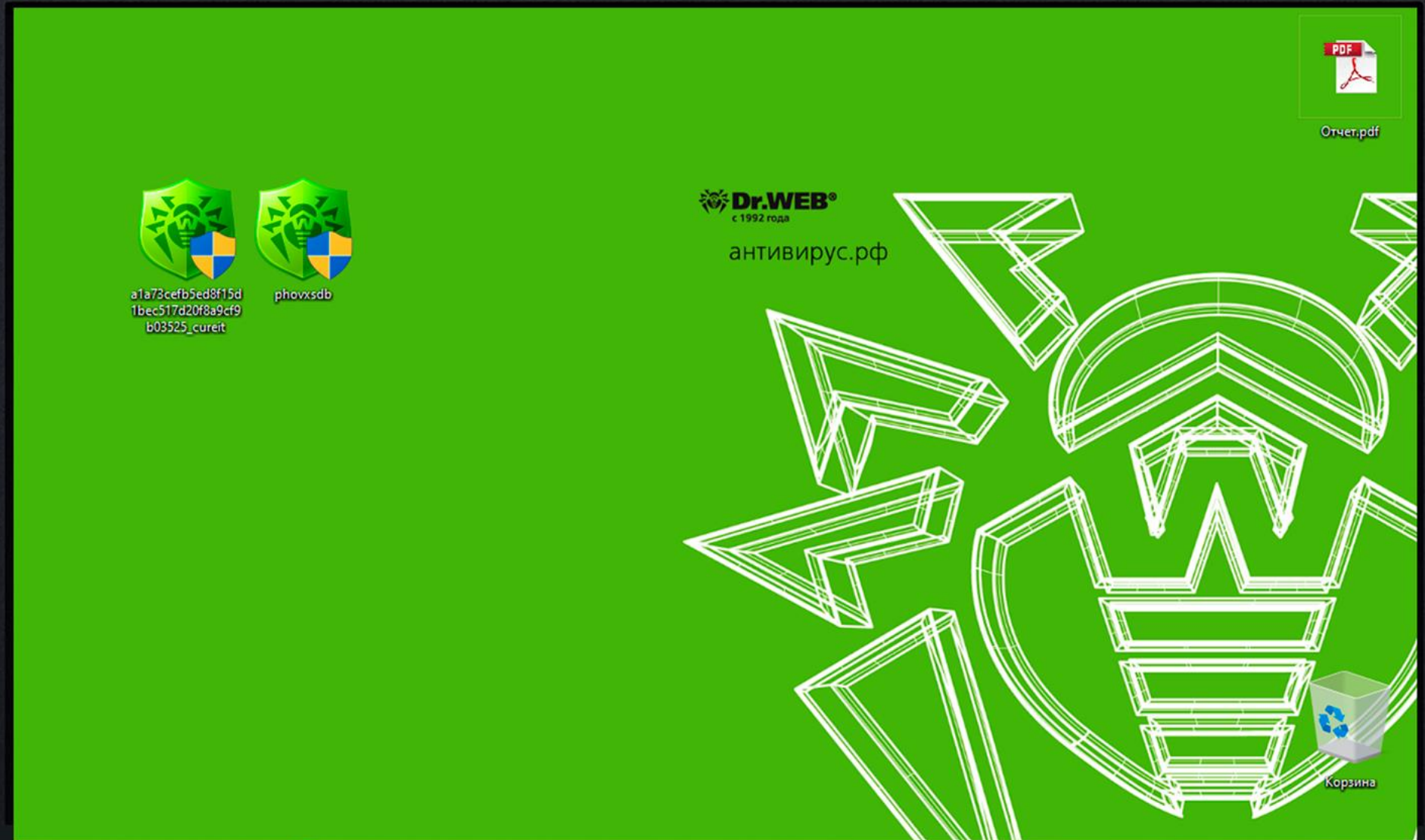
Дополнительно ▾

[Скачать исходный файл](#) [Скачать архив](#) [Скачать отчет](#) [Скачать PCAP](#)

[Поведение](#) [Граф процессов](#) [Описание](#) [Файлы и дампы памяти](#) [Журнал API](#) [Карта сетевой активности](#)

13:26 17.09.2020 ENG





Dr.WEB®
с 1992 года

антивирус.рф

a1a73cefb5ed8f15d
1bec517d20f8a9cf9
b03525_cureit

phovxsdb

Отчет.pdf

Корзина



ENG 13:27 17.09.2020



© ООО «Доктор Веб», 2020

www.антивирус.рф

www.drweb.ru



Dr.Web CureIt!

Выбор проверки

Dr.Web CureIt!

С помощью утилиты Dr.Web CureIt! вы можете быстро проверить ваш компьютер и, в случае обнаружения вредоносных объектов, выпечить его.

Начать проверку

[Выбрать объекты для проверки](#)

АКЦИЯ! Дарим год защиты

Отчет.pdf

Корзина

13:28
17.09.2020



Dr.Web CureIt!

Выборочная проверка

Dr.Web CureIt! выполняет проверку компьютера...

Пауза Стоп

Время запуска: 13:35:43 Проверенные объекты: 511546
 Осталось времени: 00:17:21 Обнаружено угроз: 1

Объект: C:\Windows\Micros...\Microsoft.VisualBasic.Compatibility.Data.resources.dll

Объект	Угроза	Действие	Путь
Отчет.pdf.exe	vxcube.detect	Вылечить	C:\U...\Отчет.pdf.exe

АКЦИЯ! Дарим год защиты

Корзина


14:10
17.09.2020






Dr.Web CureIt!

Лечение завершено

 Все угрозы безопасности успешно обезврежены.
Dr.Web CureIt! обезвредил все обнаруженные угрозы.

Угроз обнаружено: 1
Угроз обезврежено: 1
[Открыть отчет](#)

<input checked="" type="checkbox"/>	Объект	Угроза	Действие	Путь
<input checked="" type="checkbox"/>	Отчет.pdf.exe	vxcube.detect	Перемещен	C:\U...\Отчет.pdf.exe

АКЦИЯ! Дарим год защиты 



ENG 14:32 17.09.2020



А если угроза перехитрит Dr.Web vxCube?

Dr.Web vxCube - это >370 техник
ухода от обнаружения



Как устроена песочница

- Виртуальная машина (VirtualBox, VMware, QEMU, XEN/KVM, etc)
- Регистратор событий операционной системы
 - Агент
 - Гипервизор
 - Вариант от Dr.Web



Как устроена песочница: Агент

- **Драйвер операционной системы**
 - Легко обнаружить
 - Снять перехваты или выгрузить драйвер
 - Агент может “утечь”

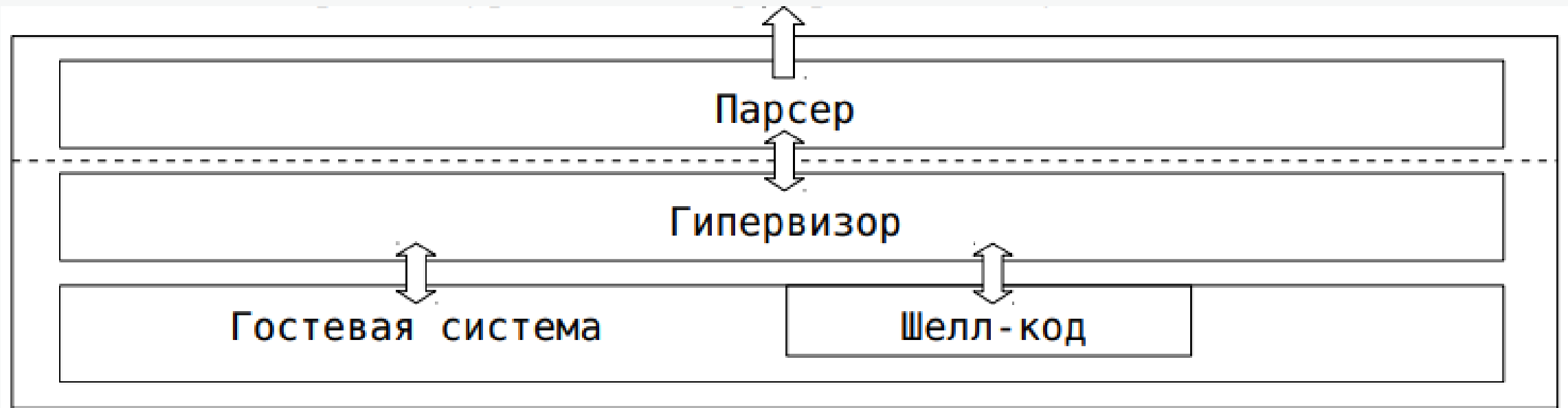


Как устроена песочница: Гипервизор

- Гипервизор
 - Сложен в разработке
 - Ничего не знает о внутренностях операционной системы



Как устроена песочница: Агент, скрытый гипервизором (Dr.Web vxCube)



А теперь о подарке



<https://download.drweb.ru/vxcube/?podarok=y>



Вопросы?

