Dr.WEB®
с 1992 года

Незримая угроза: как ее обнаружить и обезвредить

www.антивирус.рф
www.drweb.ru

Dr.WEB®
с 1992 года

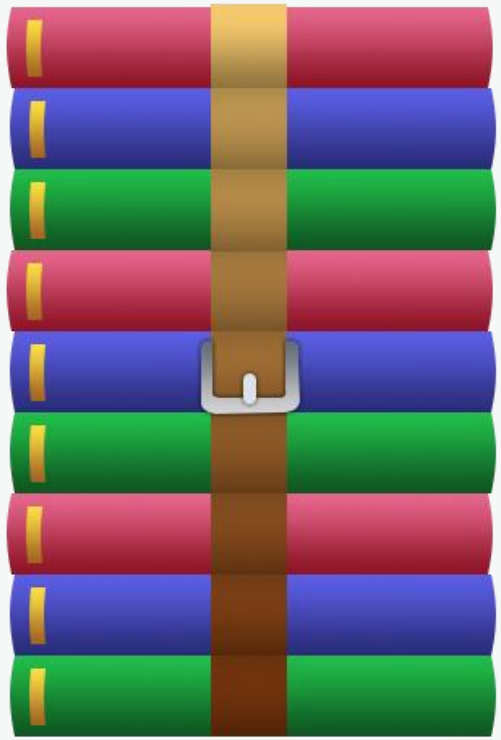
Насколько хорошо защищает антивирус?

Dr.WEB®
с 1992 года

Оставаться в тени как можно дольше

Dr.WEB®
с 1992 года

Разнообразие упаковщиков



Dr.WEB®
с 1992 года

VIRUSTOTAL

- 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

Dr.WEB®
с 1992 года

Изучение работы антивируса

Dr.WEB®
с 1992 года

Ожидание часа X или действия

Dr.WEB®
с 1992 года

Сочетание разных приемов

Dr.WEB®
с 1992 года

Трояны в легальном ПО

Dr.WEB®
с 1992 года

Идеальной защиты не бывает

Dr.WEB®
с 1992 года

НОВАЯ ВЕРСИЯ 12

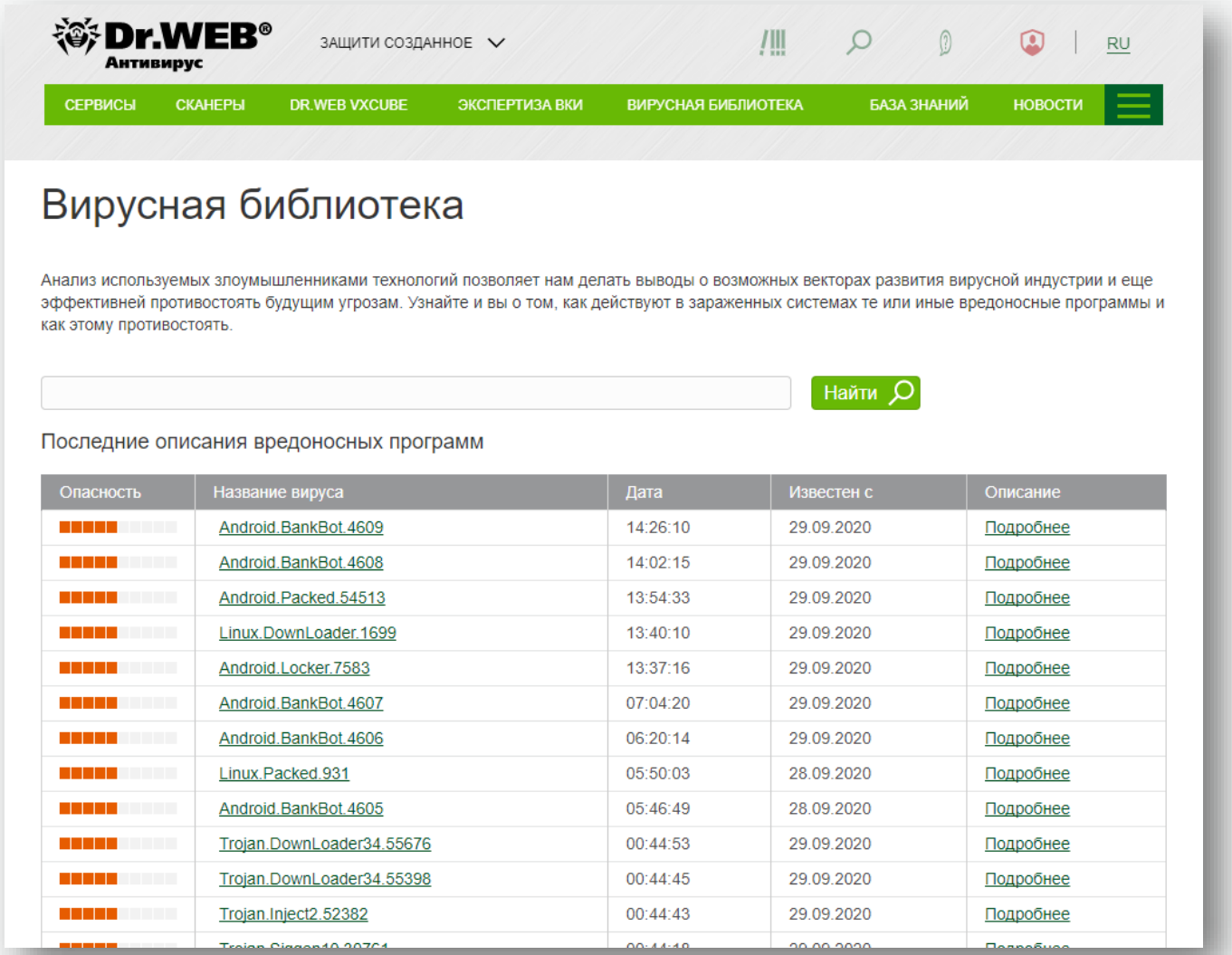
Dr.Web Enterprise Security Suite

Всё под контролем

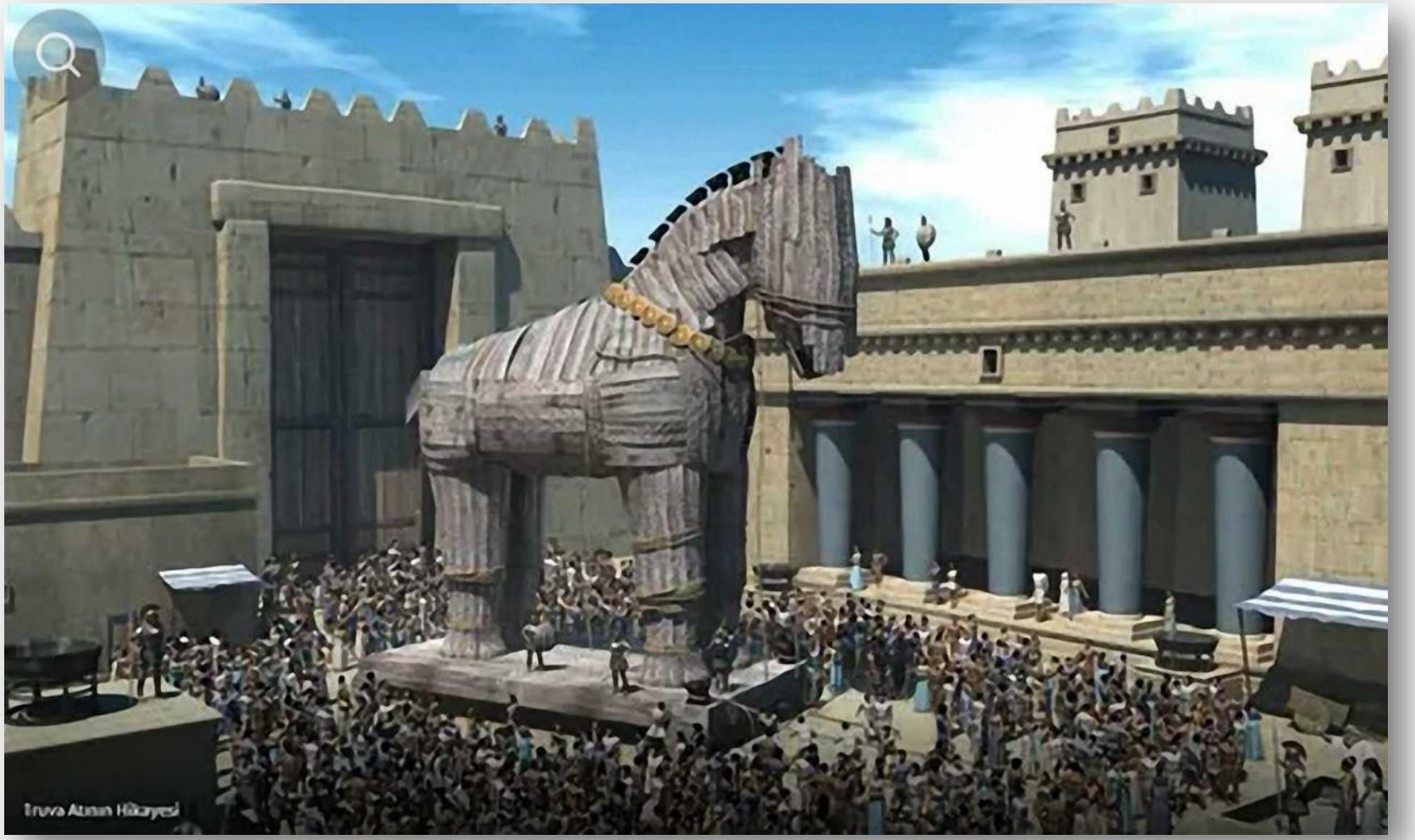
Что нового?

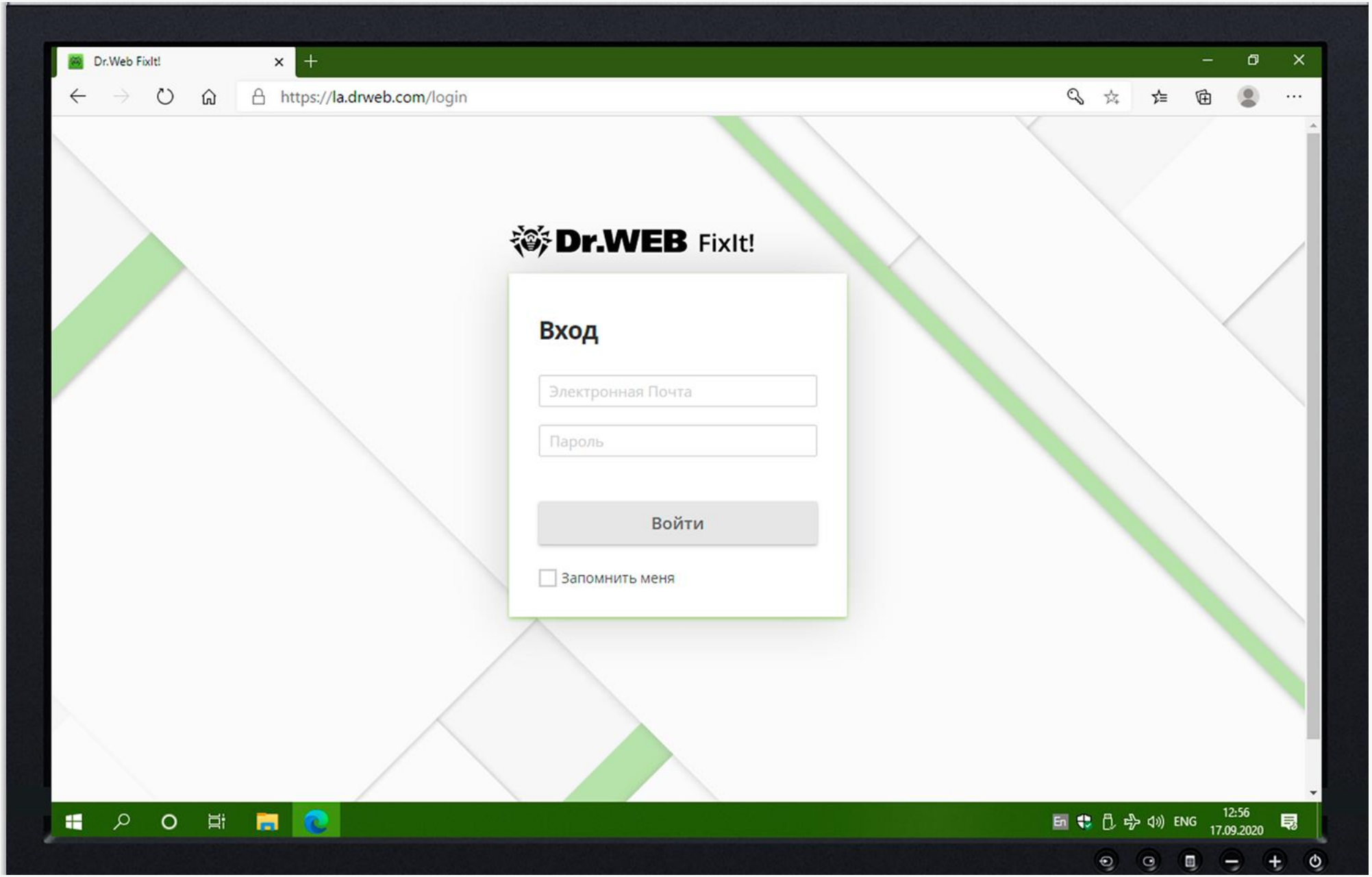
Dr.WEB®
с 1992 года

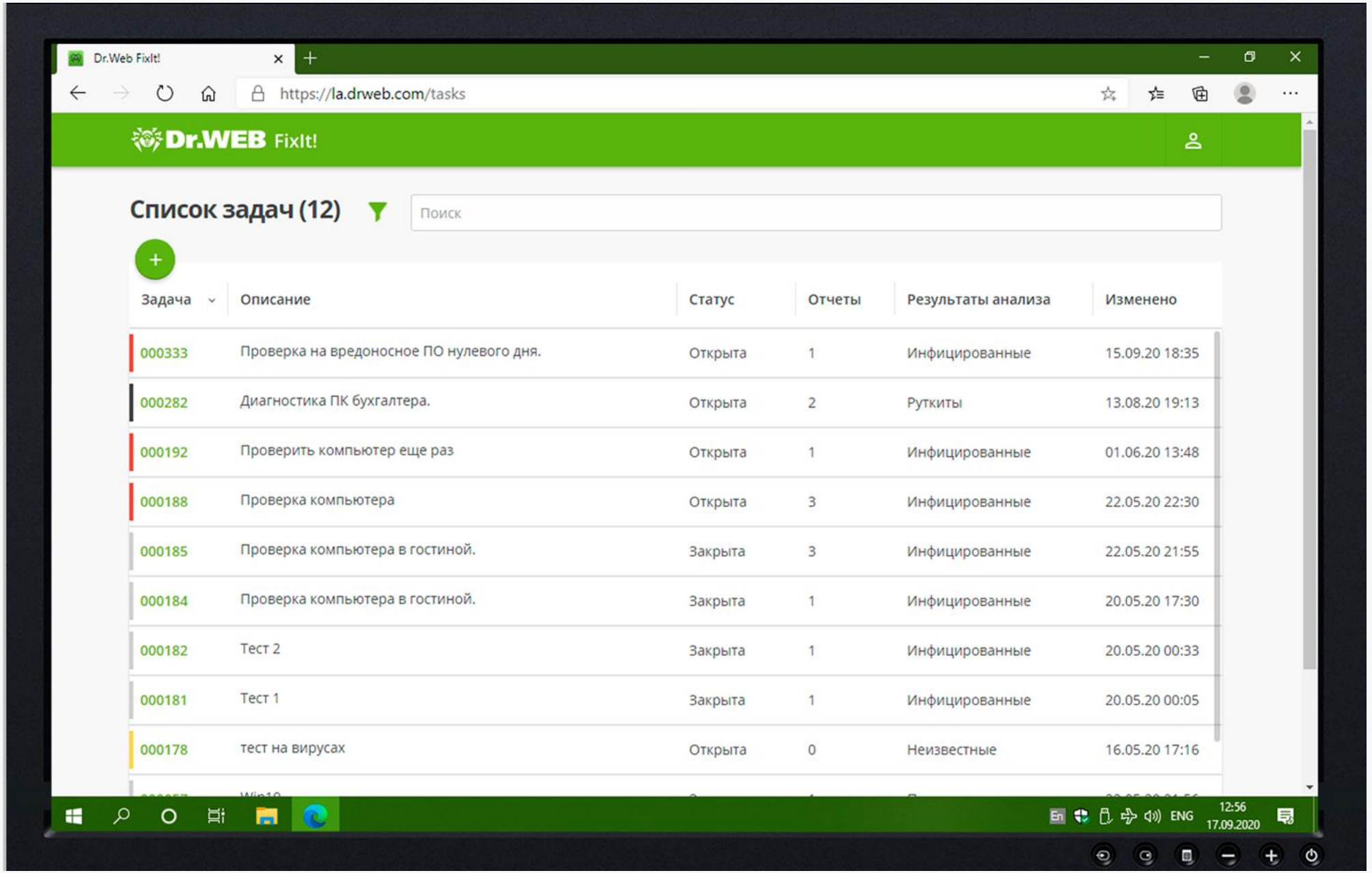
vms.drweb.ru/search

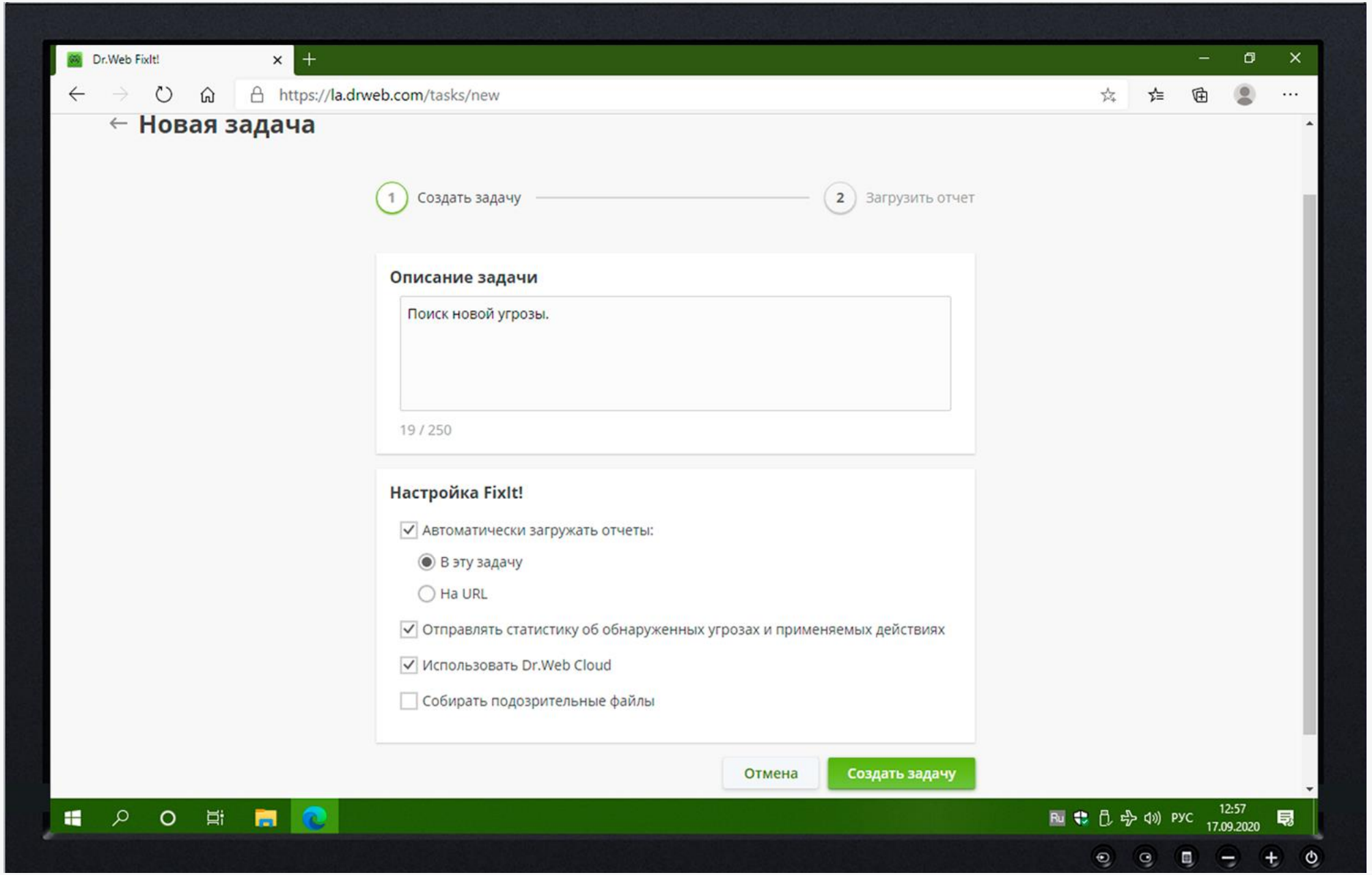


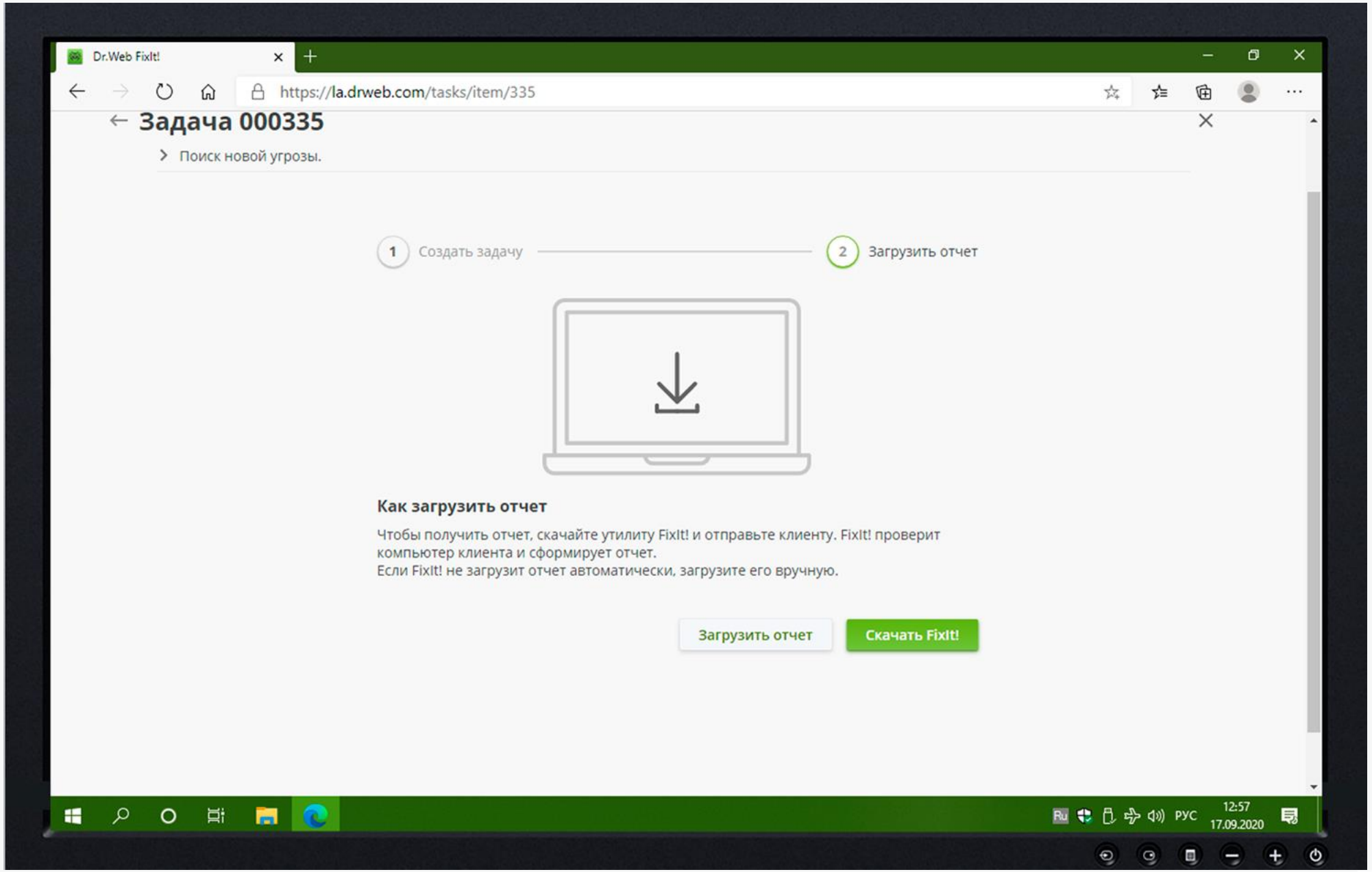
Опасность	Название вируса	Дата	Известен с	Описание
	Android.BankBot.4609	14:26:10	29.09.2020	Подробнее
	Android.BankBot.4608	14:02:15	29.09.2020	Подробнее
	Android.Packed.54513	13:54:33	29.09.2020	Подробнее
	Linux.DownLoader.1699	13:40:10	29.09.2020	Подробнее
	Android.Locker.7583	13:37:16	29.09.2020	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

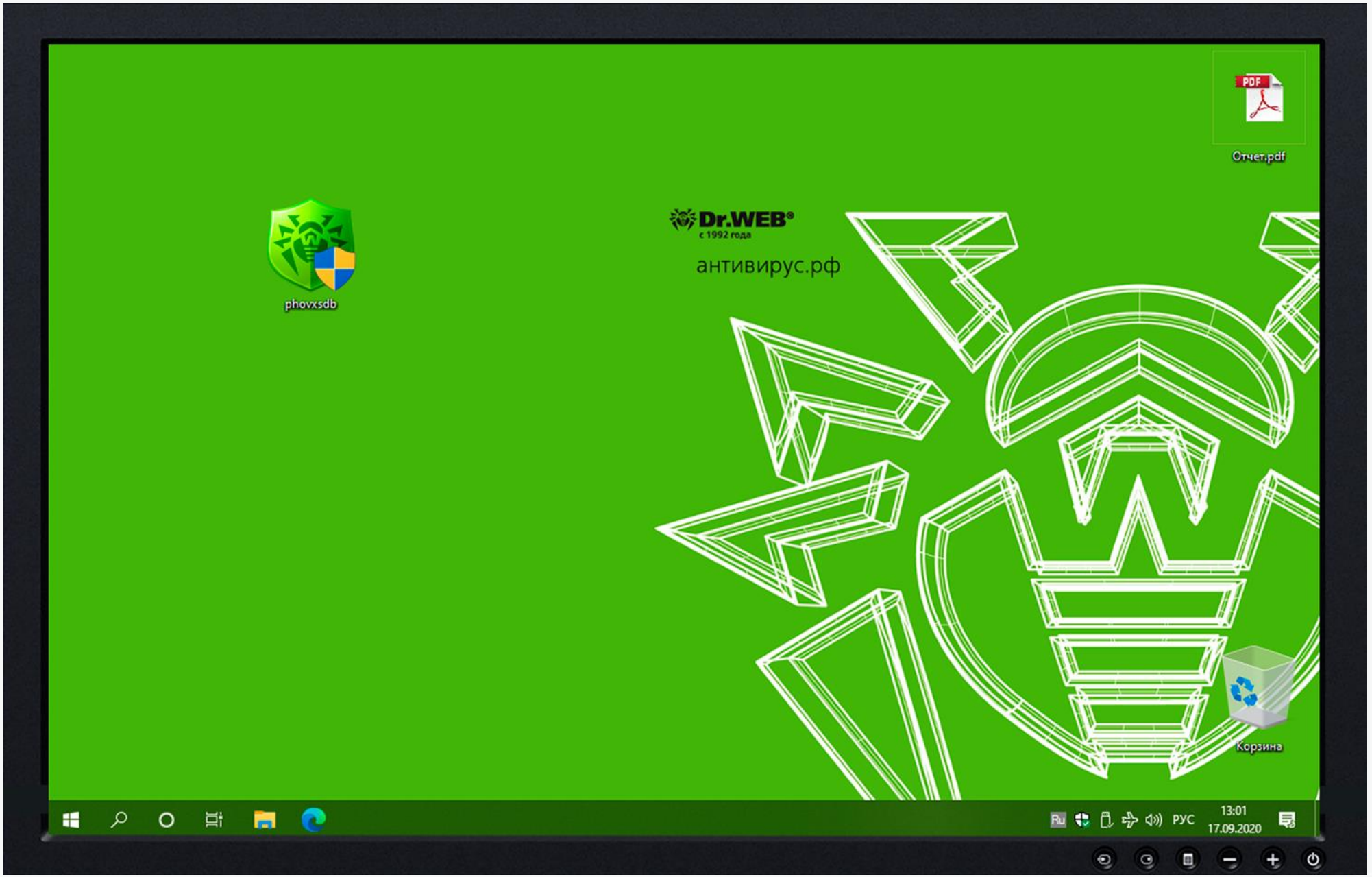


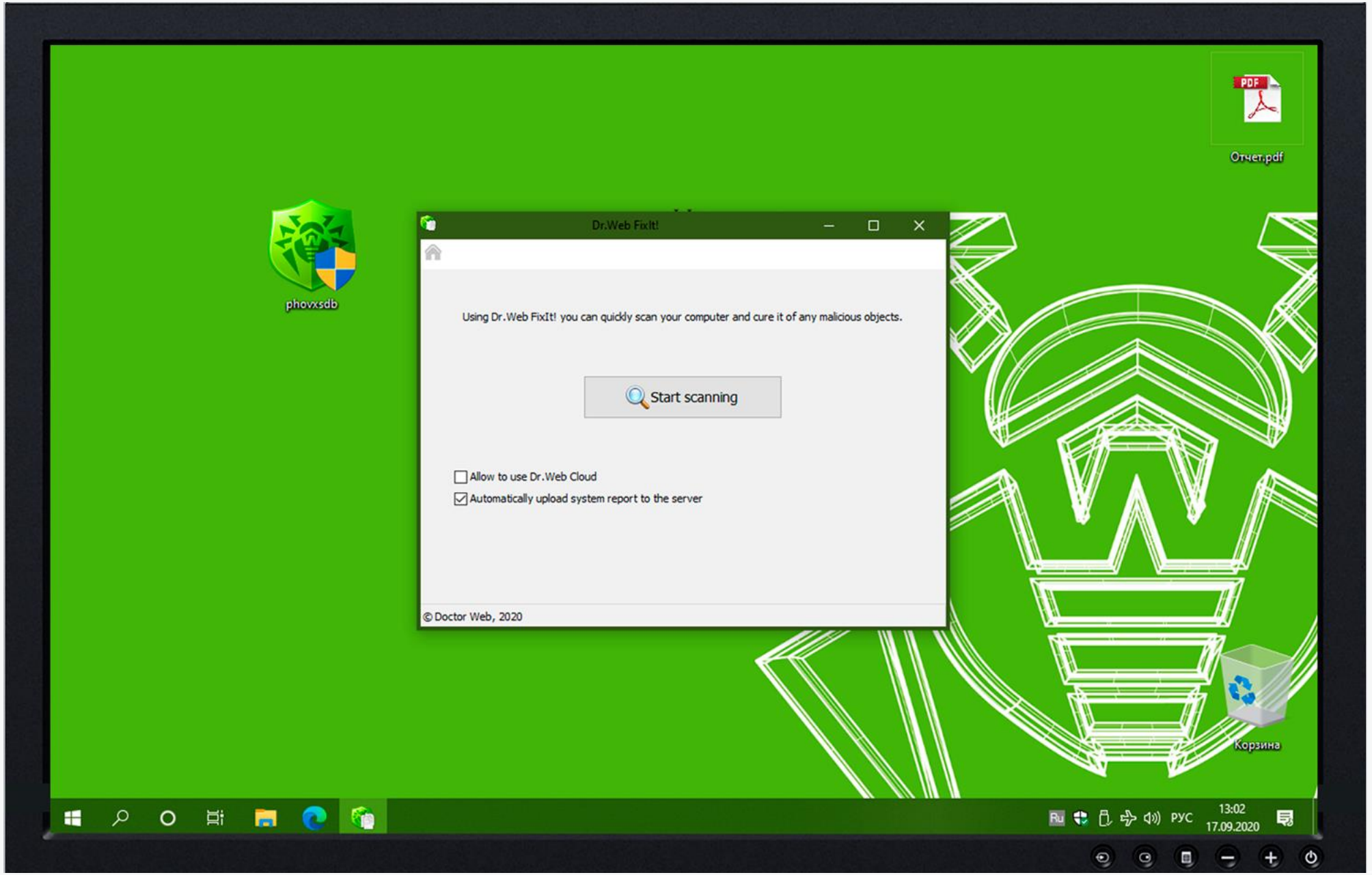

Dr.Web FixIt!
https://la.drweb.com/login
Dr.WEB FixIt!
Вход
Электронная Почта
Пароль
Войти
Запомнить меня
ENG
12:56
17.09.2020

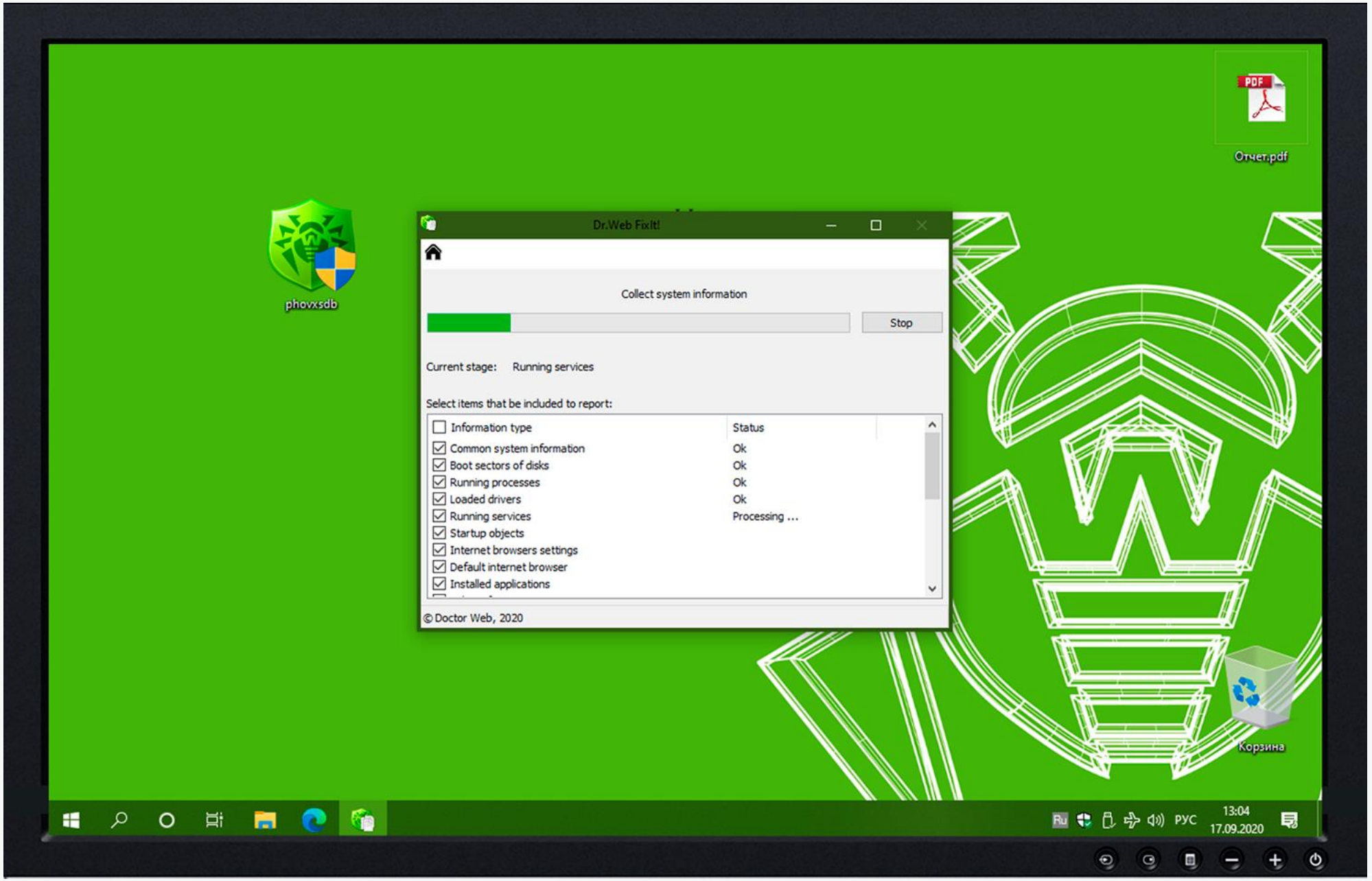


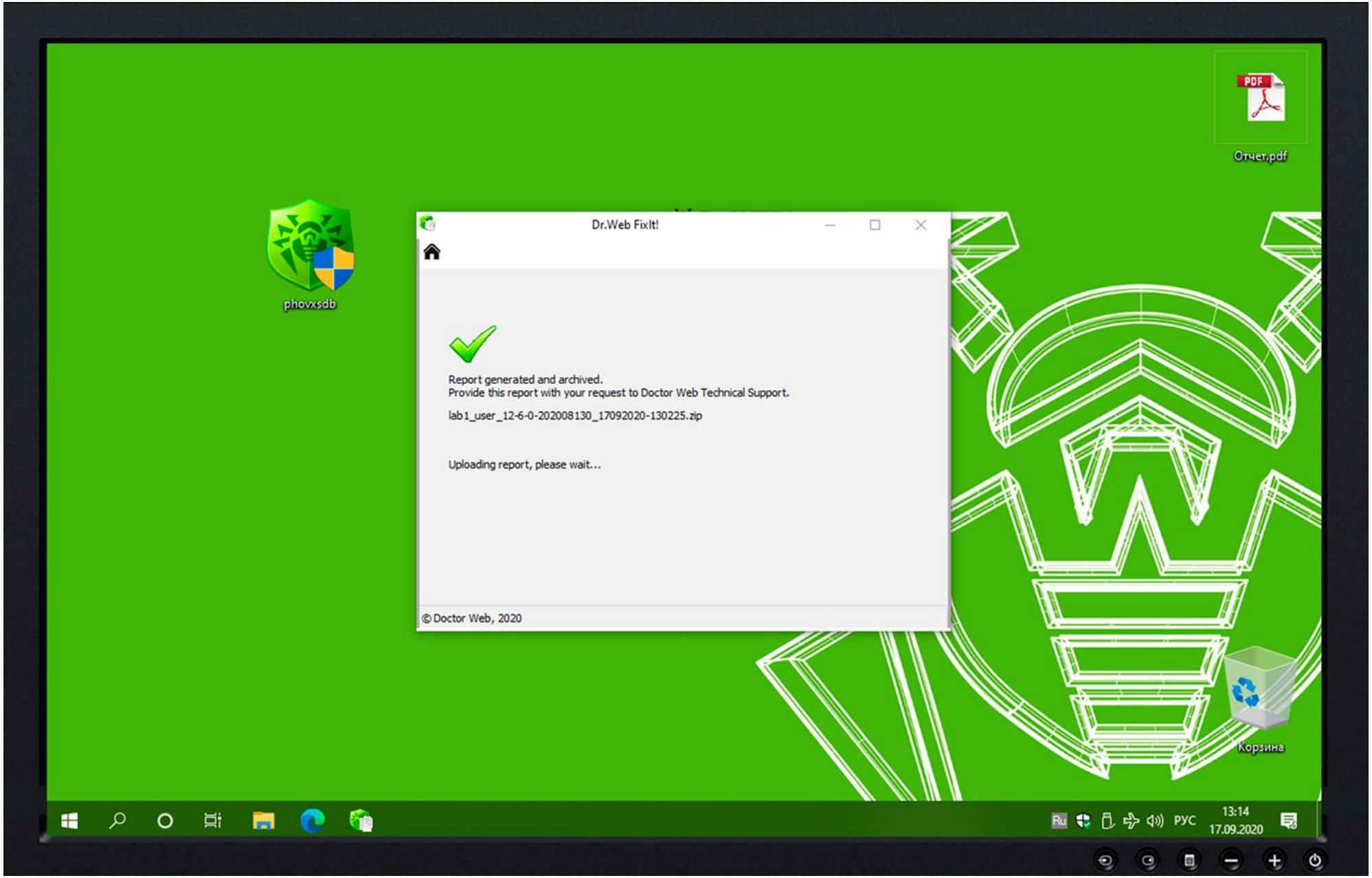


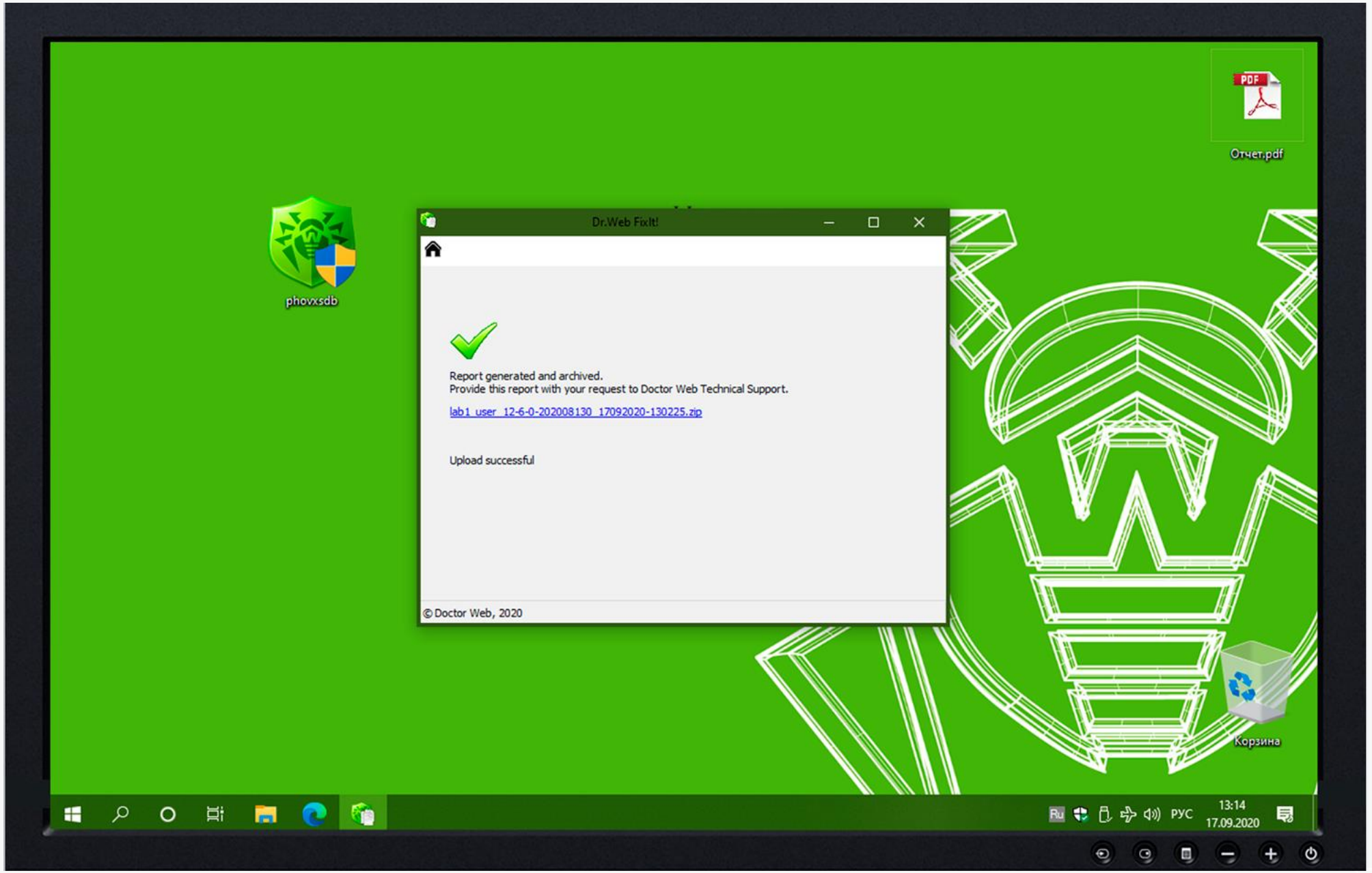


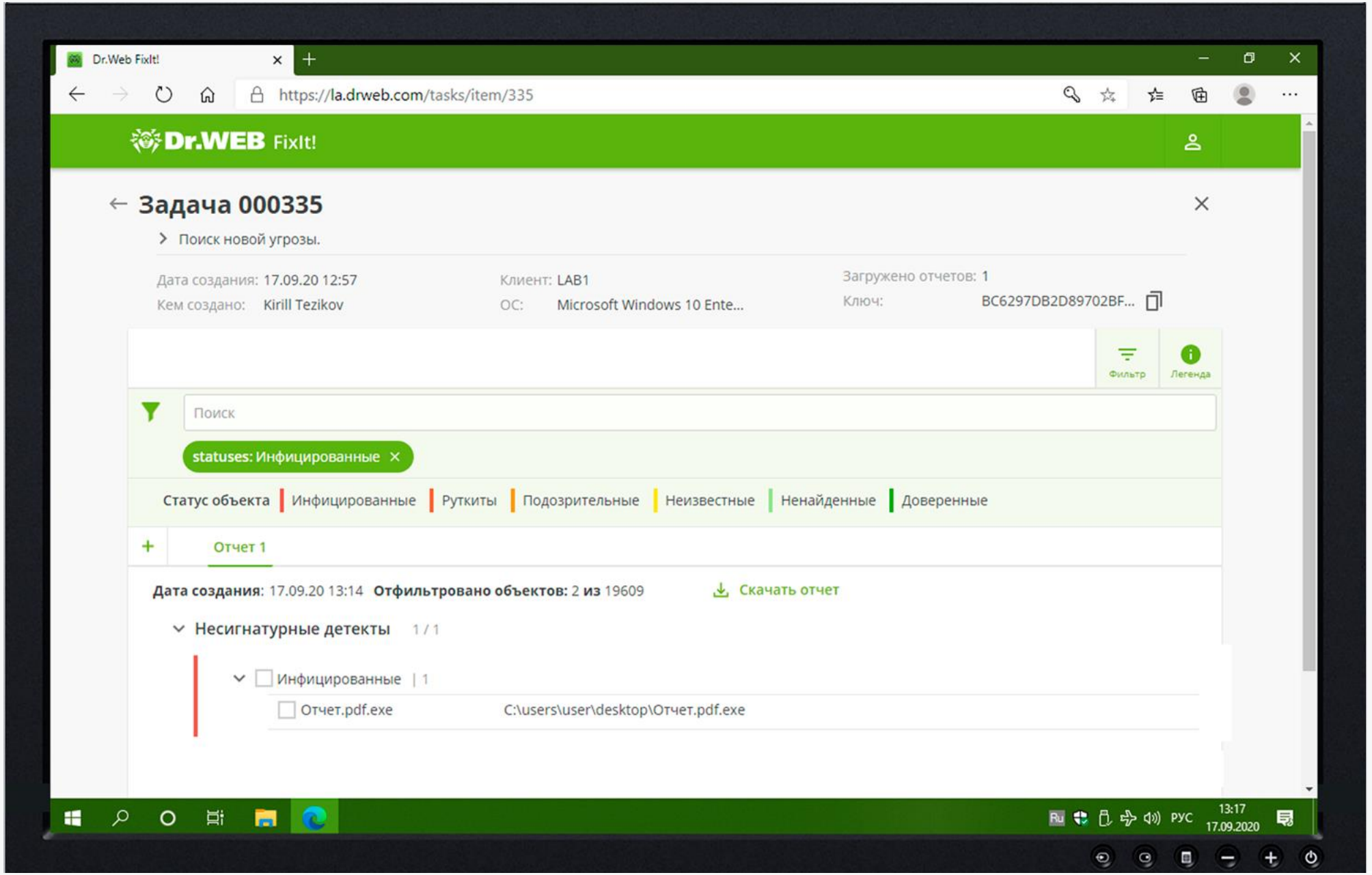


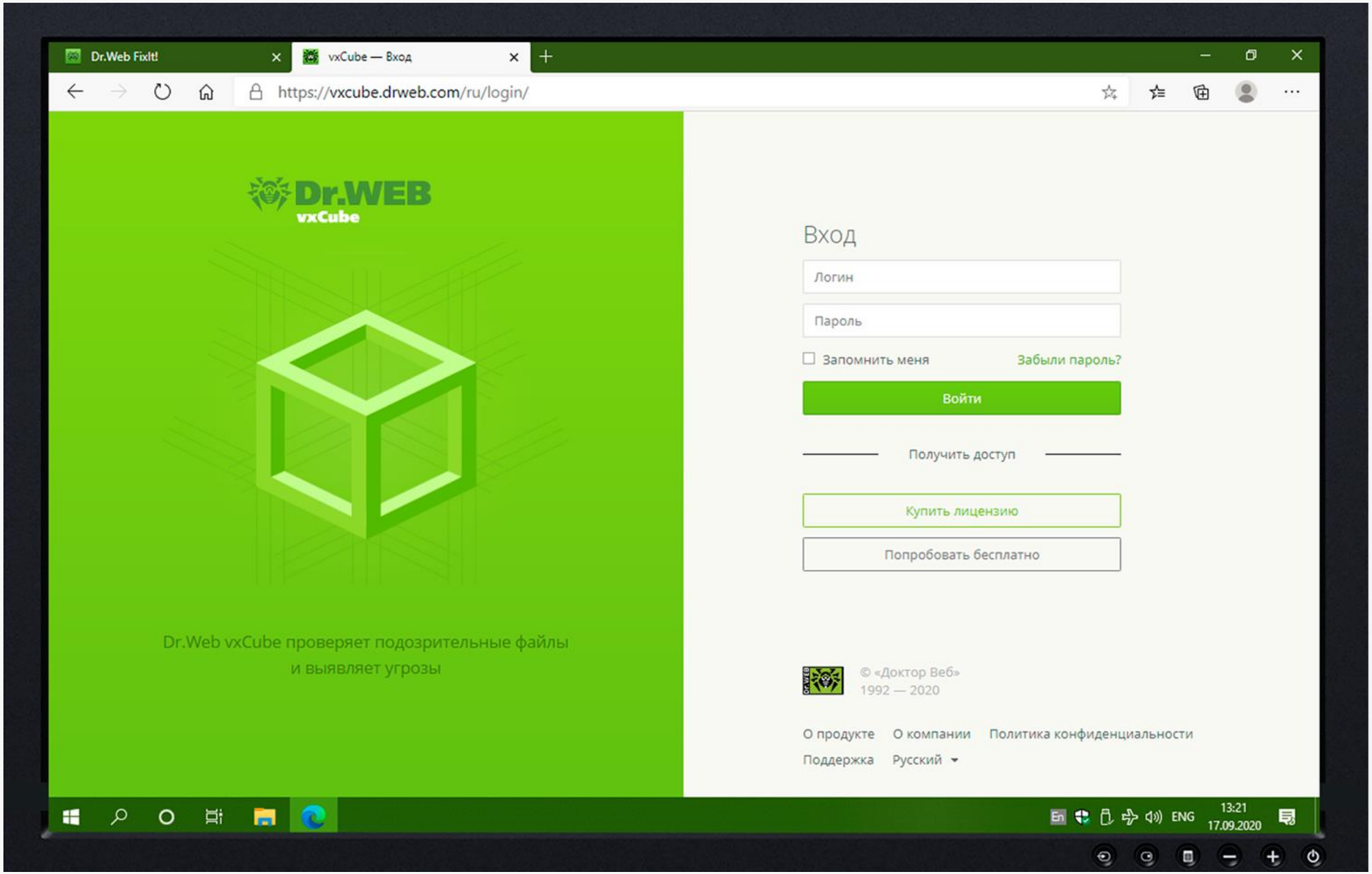

Отчет.pdf
phovxsdb
Dr.Web FixIt!
Using Dr.Web FixIt! you can quickly scan your computer and cure it of any malicious objects.
Start scanning
Allow to use Dr.Web Cloud
Automatically upload system report to the server
© Doctor Web, 2020
Корзина
РУС
13:02
17.09.2020

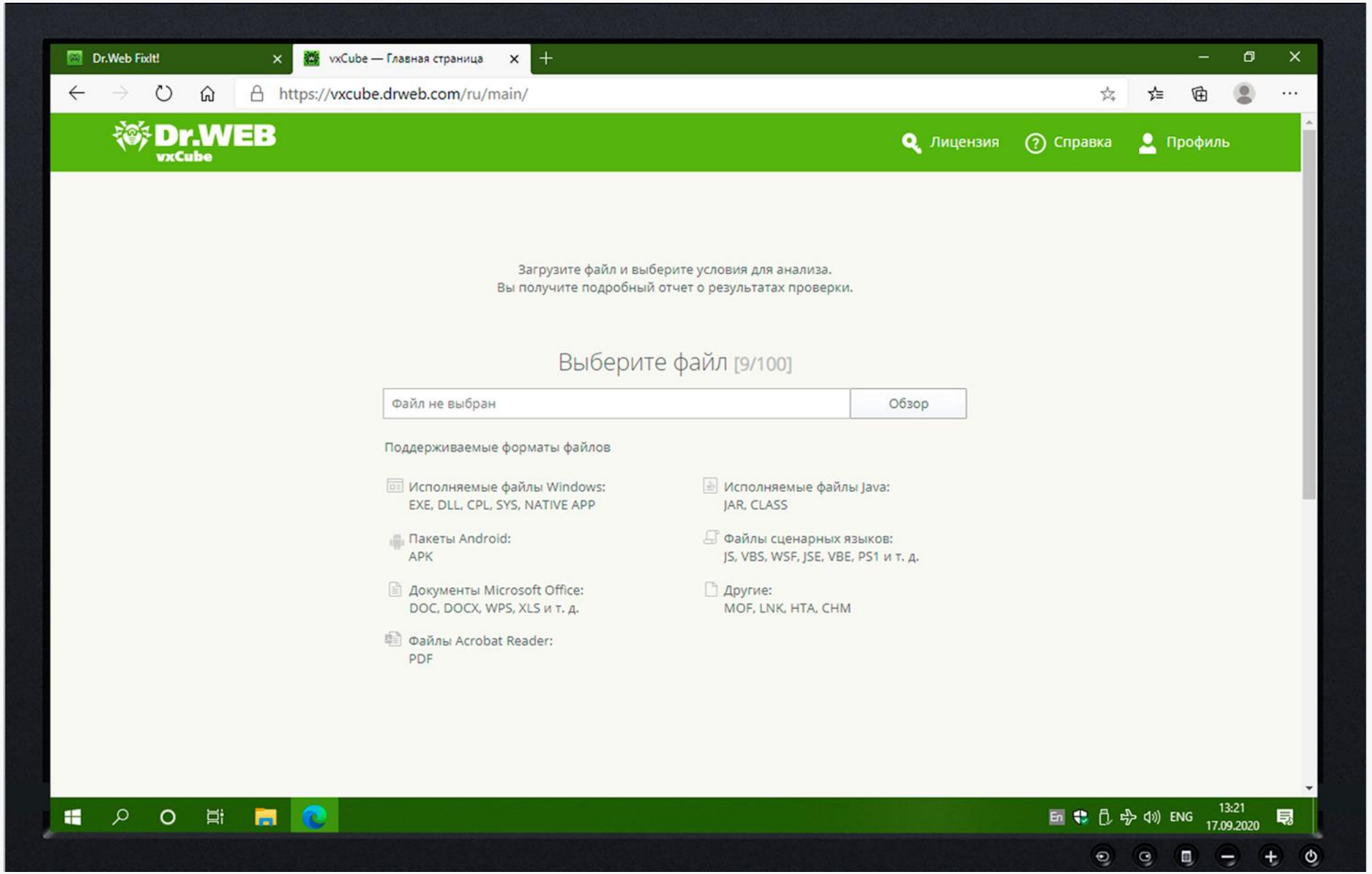

Отчет.pdf
phovxsdb
Dr.Web FixIt!
Collect system information
Stop
Current stage: Running services
Select items that be included to report:
Information type
Status
Common system information
Ok
Boot sectors of disks
Ok
Running processes
Ok
Loaded drivers
Ok
Running services
Processing ...
Startup objects
Internet browsers settings
Default internet browser
Installed applications
© Doctor Web, 2020
Корзина
РУС
13:04
17.09.2020

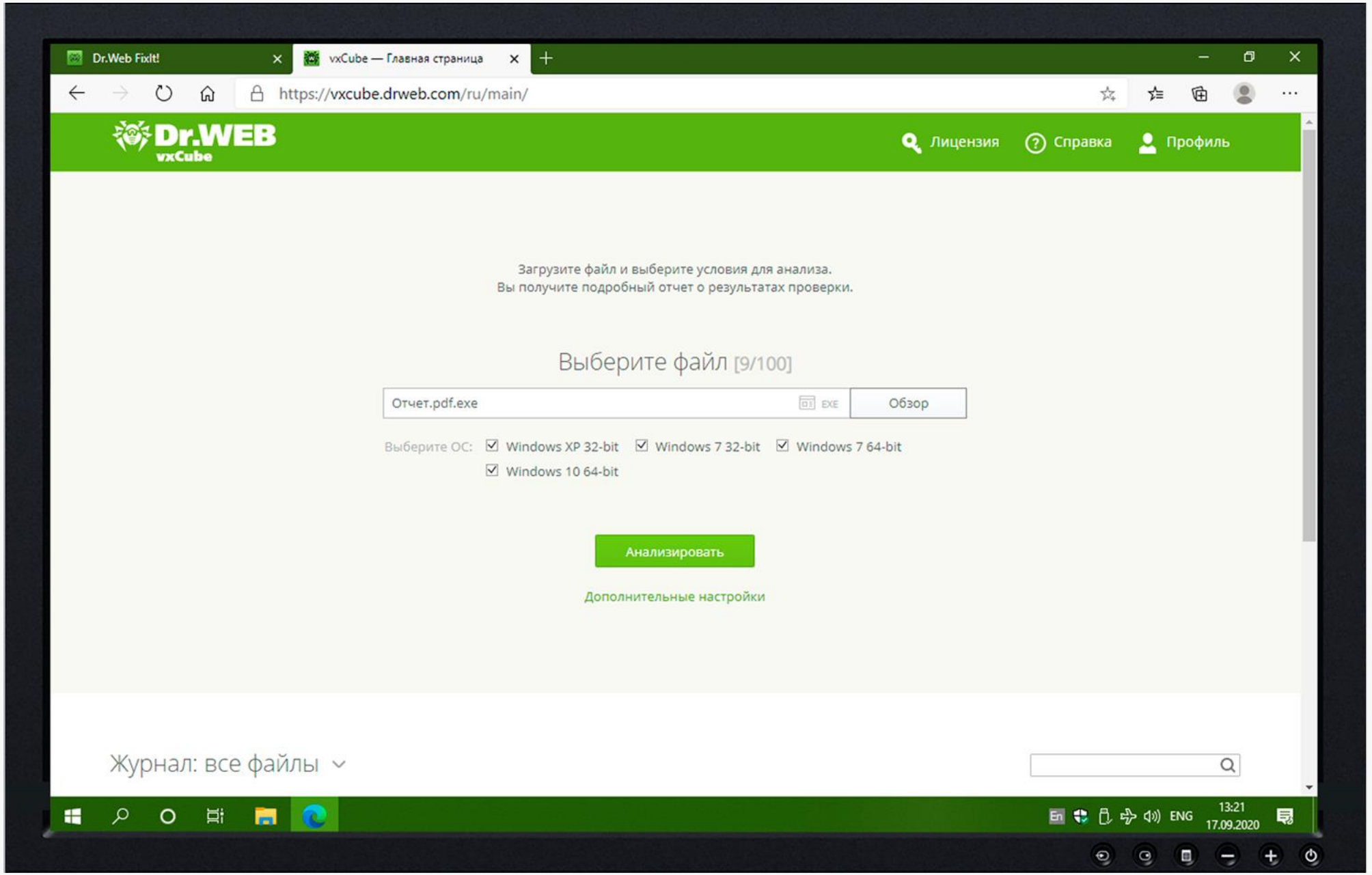

Отчет.pdf
phovxsdb
Dr.Web FixIt!
Report generated and archived.
Provide this report with your request to Doctor Web Technical Support.
lab1_user_12-6-0-202008130_17092020-130225.zip
Uploading report, please wait...
© Doctor Web, 2020
Корзина
РУС
13:14
17.09.2020

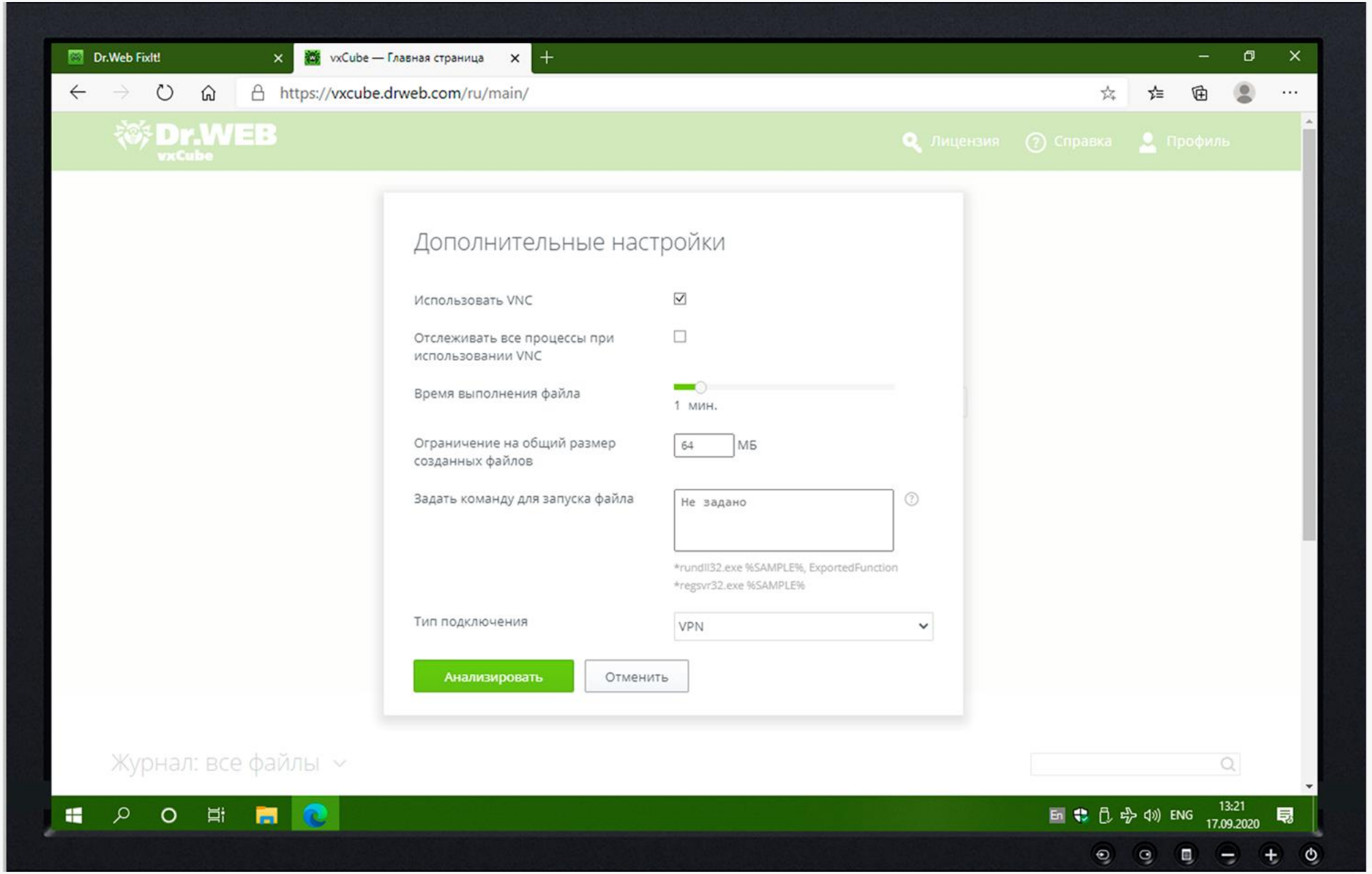

Отчет.pdf
phovxsdb
Dr.Web FixIt!
Report generated and archived.
Provide this report with your request to Doctor Web Technical Support.
lab1_user_12-6-0-202008130_17092020-130225.zip
Upload successful
© Doctor Web, 2020
Корзина
РУС
13:14
17.09.2020

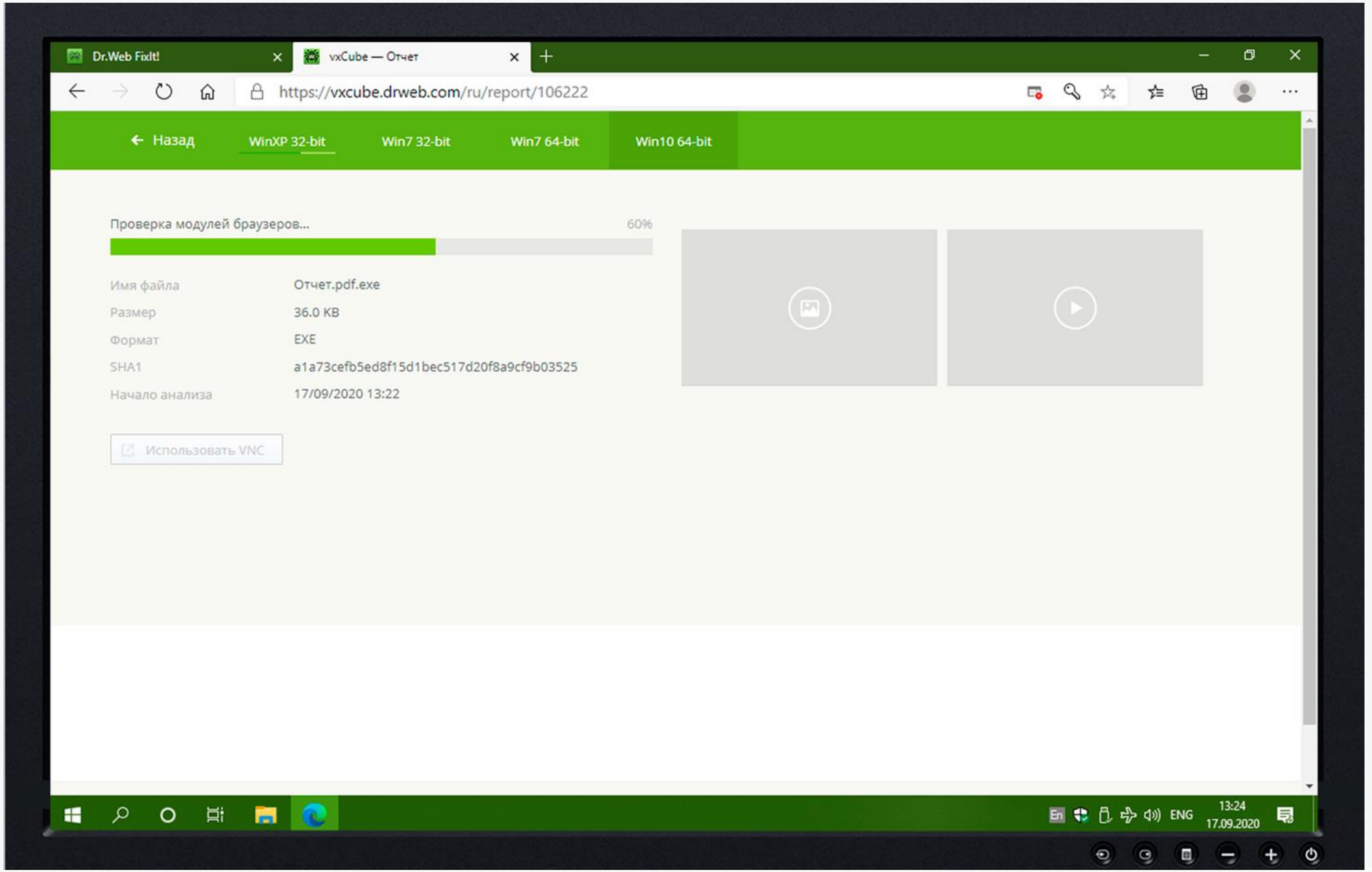

Dr.Web FixIt!
https://la.drweb.com/tasks/item/335
Dr.WEB FixIt!
Задача 000335
Поиск новой угрозы.
Дата создания: 17.09.20 12:57
Кем создано: Kirill Tezikov
Клиент: LAB1
ОС: Microsoft Windows 10 Ente...
Загружено отчетов: 1
Ключ: BC6297DB2D89702BF...
Фильтр
Легенда
Поиск
statuses: Инфицированные
Статус 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
РУС
13:17
17.09.2020

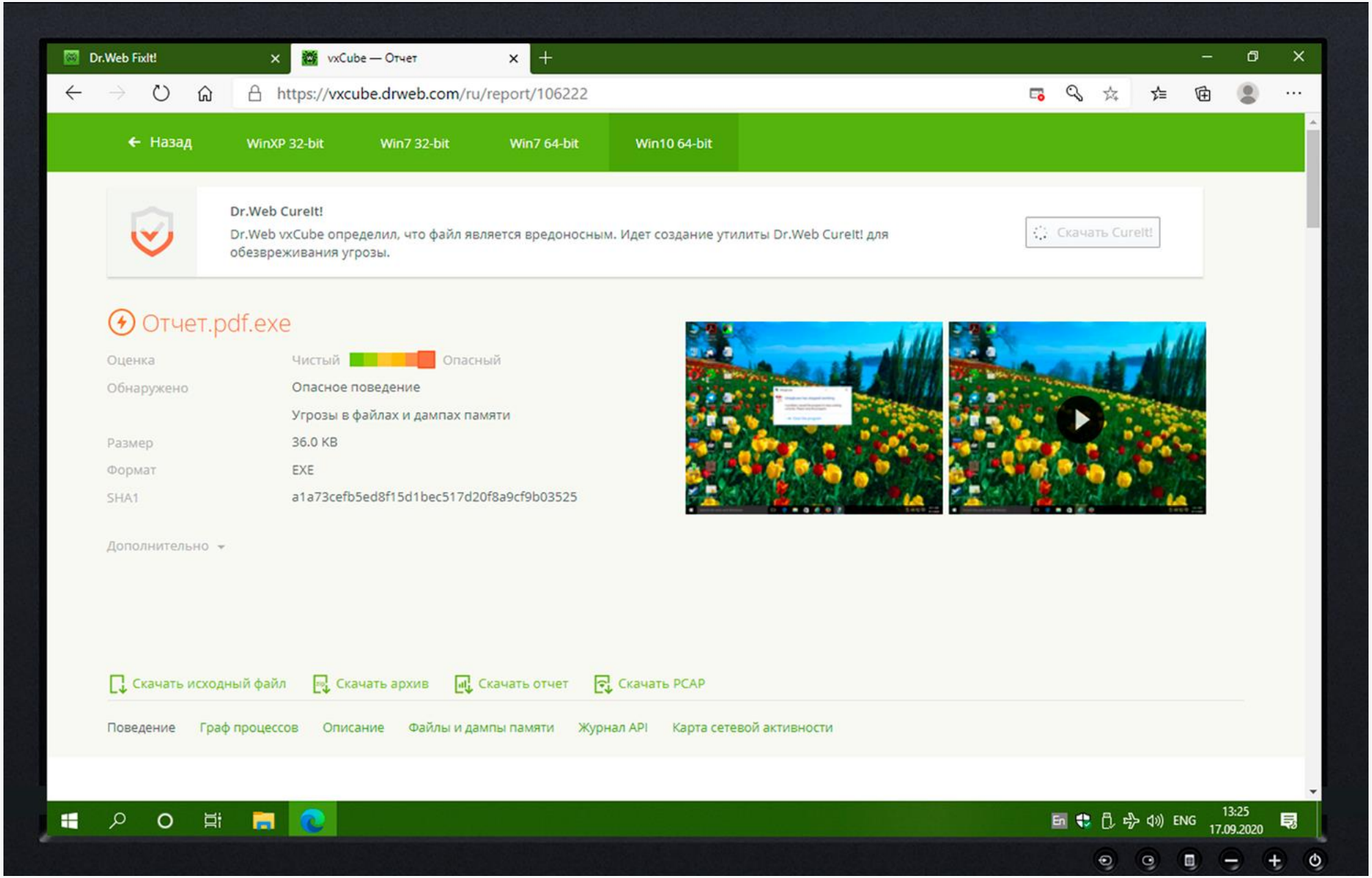

Dr.Web FixIt!
vxCube — Вход
https://vxcube.drweb.com/ru/login/
Dr.WEB
vxCube
Dr.Web vxCube проверяет подозрительные файлы
и выявляет угрозы
Вход
Логин
Пароль
Запомнить меня
Забыли пароль?
Войти
Получить доступ
Купить лицензию
Попробовать бесплатно
© «Доктор Веб»
1992 — 2020
О продукте
О компании
Политика конфиденциальности
Поддержка
Русский
ENG
13:21
17.09.2020

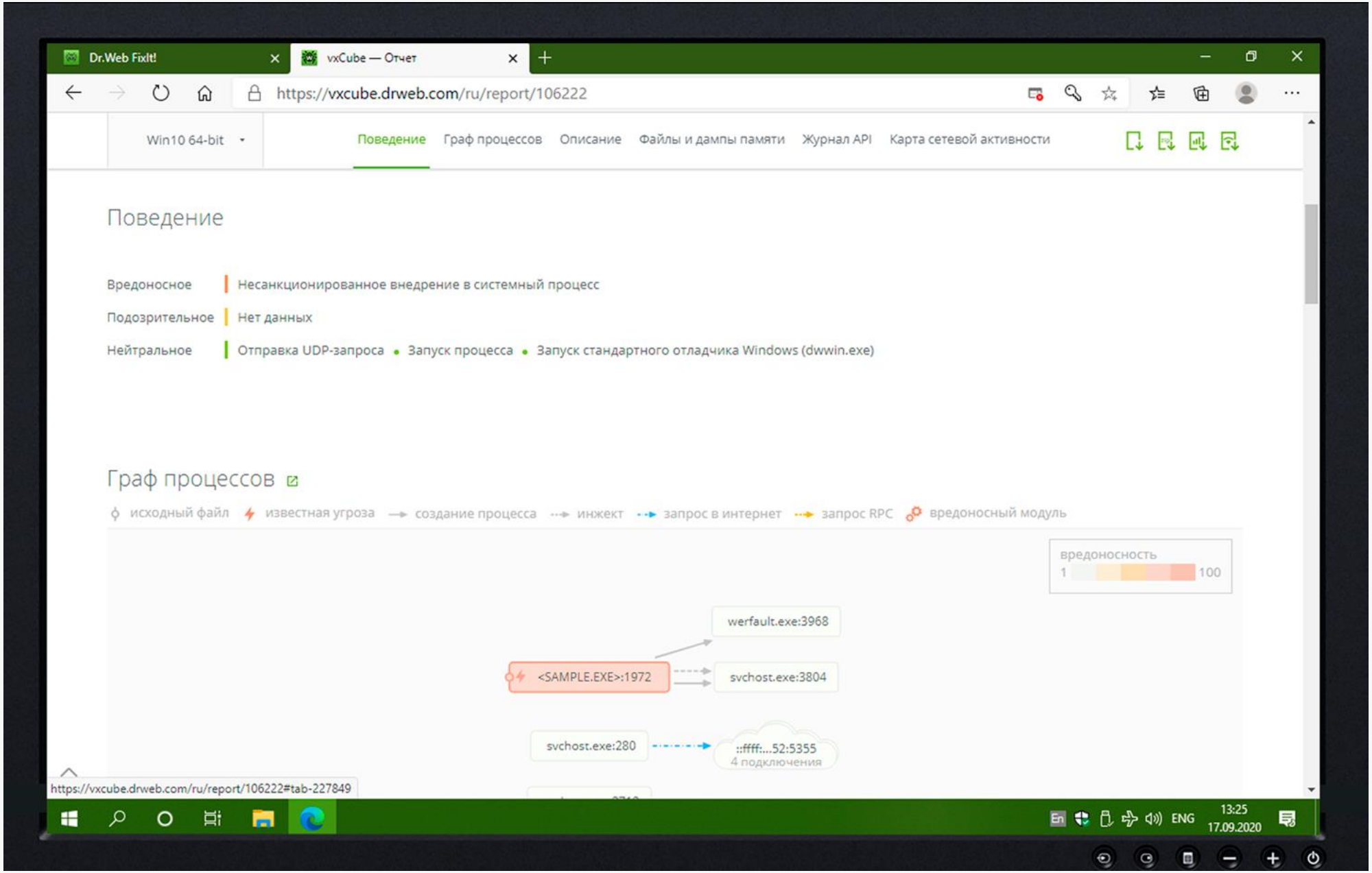


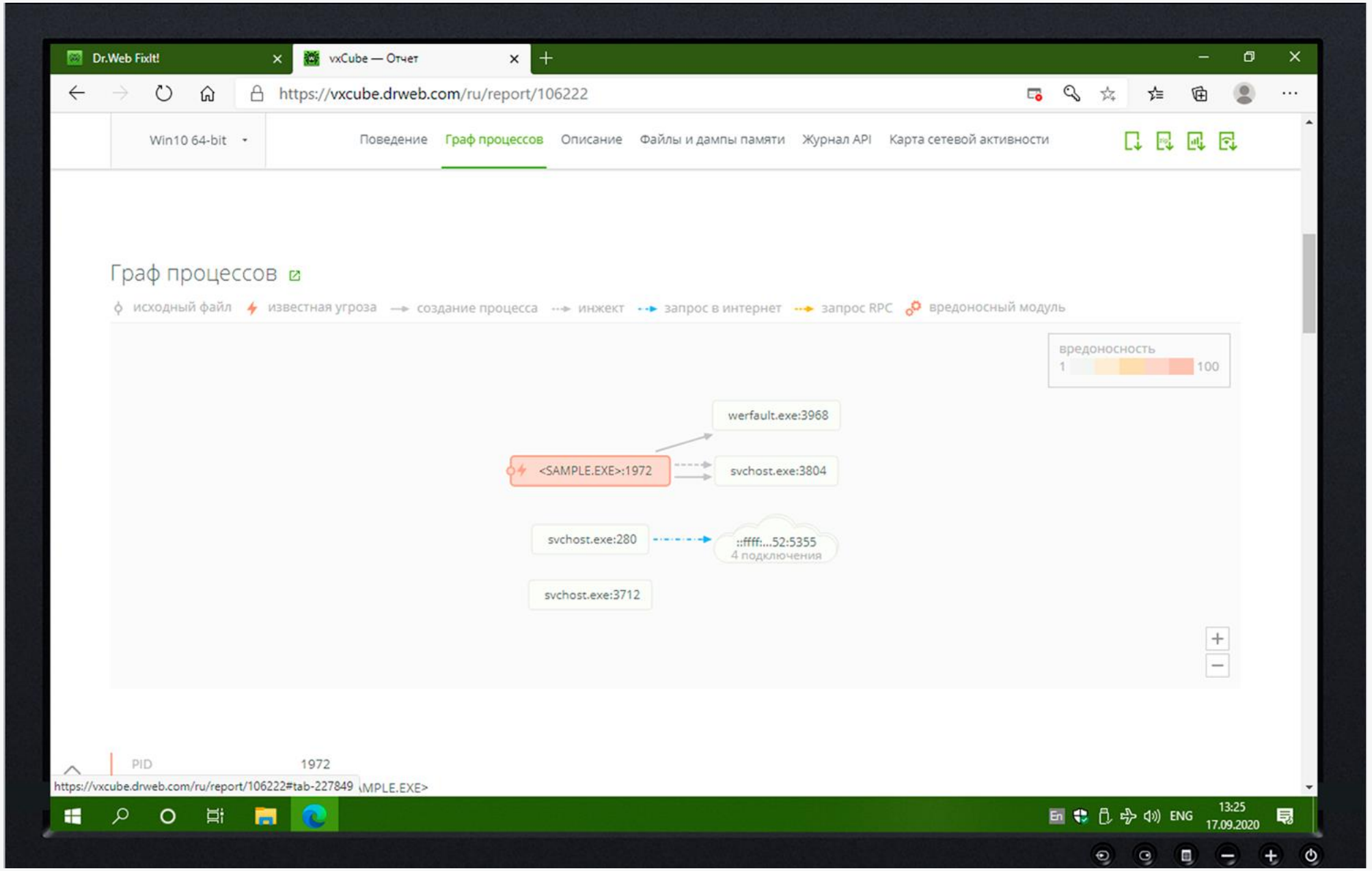


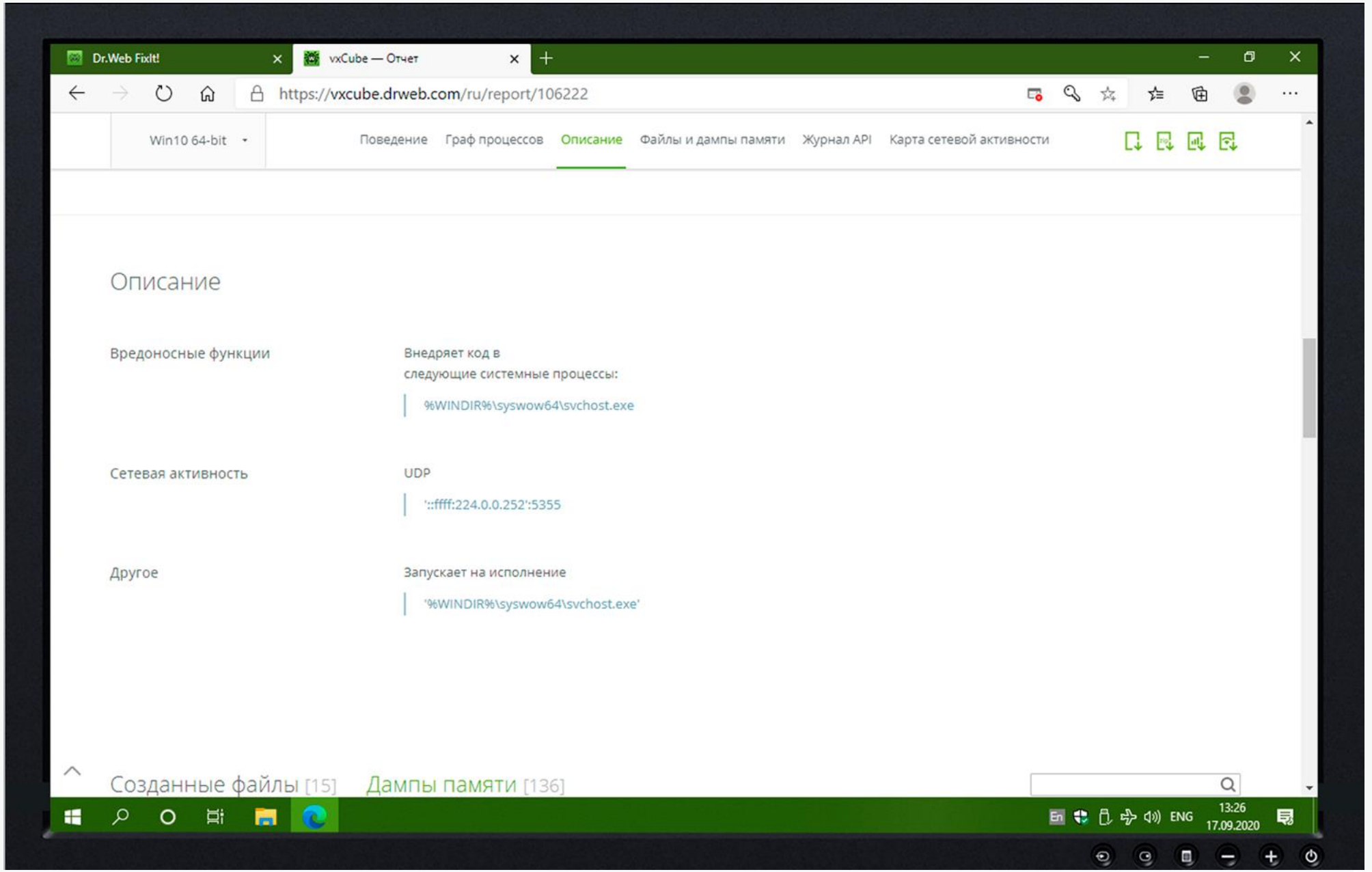


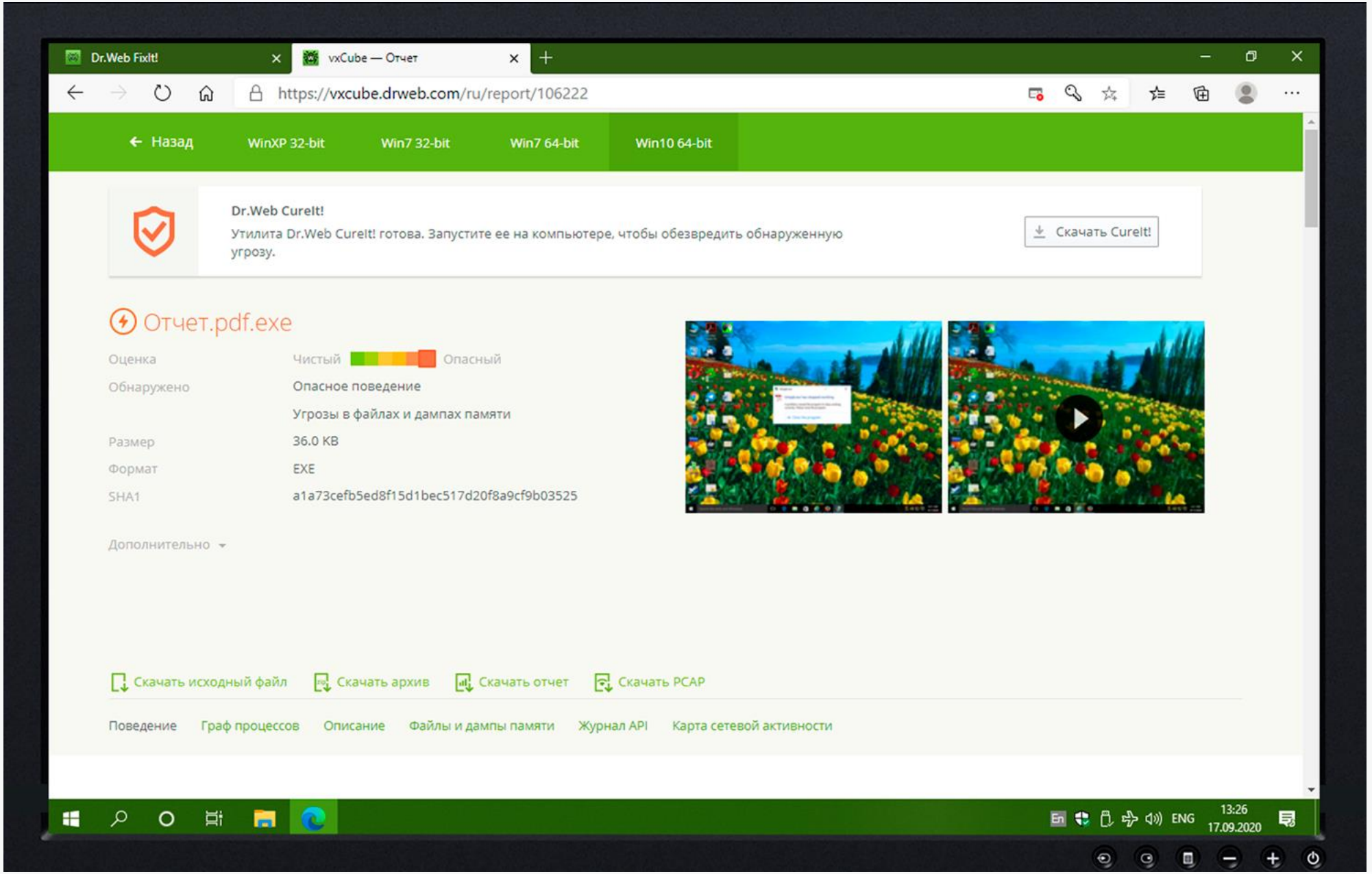


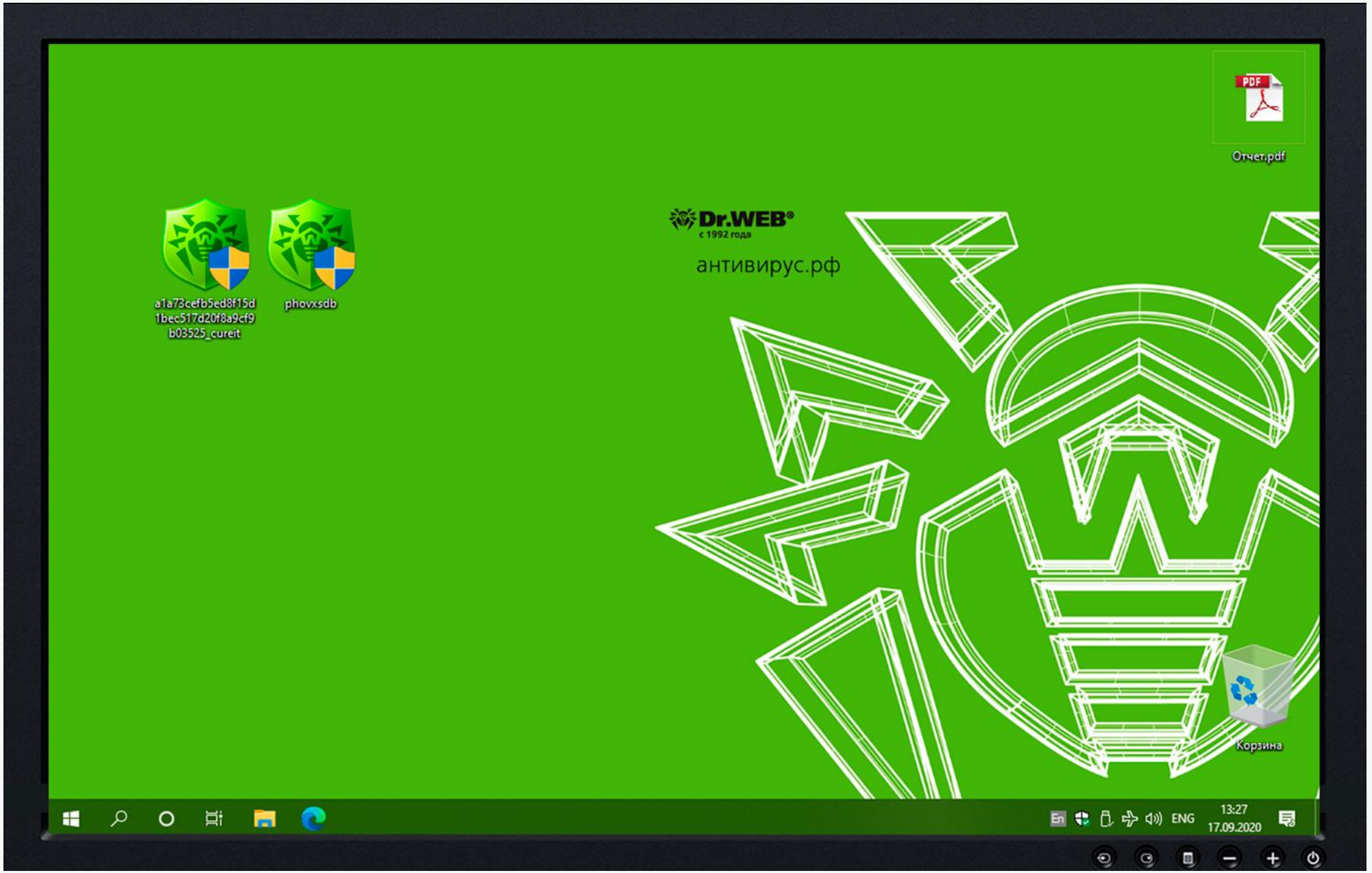


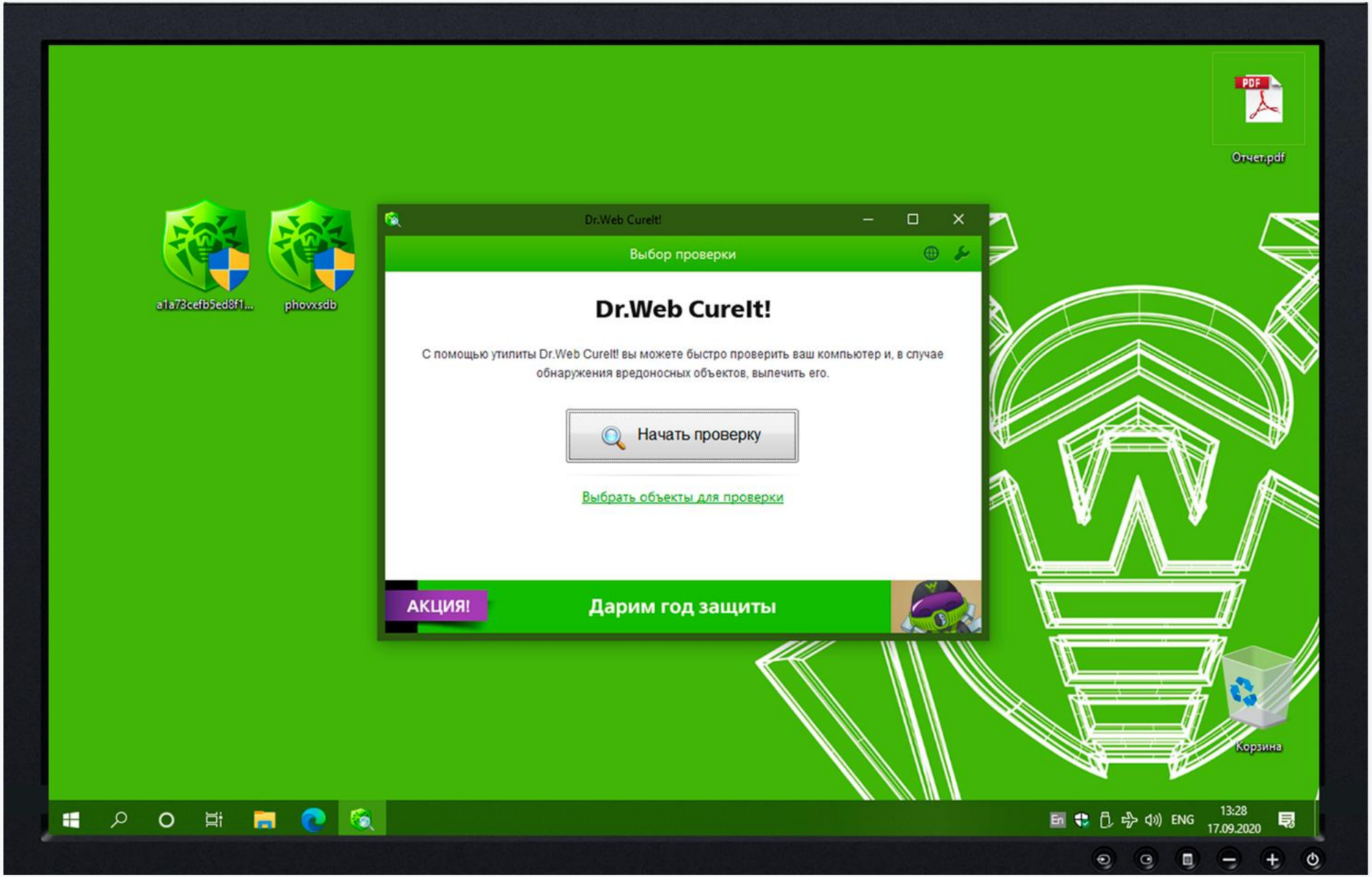

Dr.Web FixIt!
vxCube — Отчет
https://vxcube.drweb.com/ru/report/106222
Win10 64-bit
Поведение
Граф процессов
Описание
Файлы и дампы памяти
Журнал API
Карта сетевой активности
Поведение
Вредоносное
Несанкционированное внедрение в системный процесс
Подозрительное
Нет данных
Нейтральное
Отправка UDP-запроса • Запуск процесса • Запуск стандартного отладчика Windows (dwwin.exe)
Граф процессов
исходный файл
известная угроза
создание процесса
инжект
запрос в интернет
запрос RPC
вредоносный модуль
вредоносность
1
100
werfault.exe:3968
<SAMPLE.EXE>:1972
svchost.exe:3804
svchost.exe:280
::ffff:...52:5355
4 подключения
https://vxcube.drweb.com/ru/report/106222#tab-227849
ENG
13:25
17.09.2020

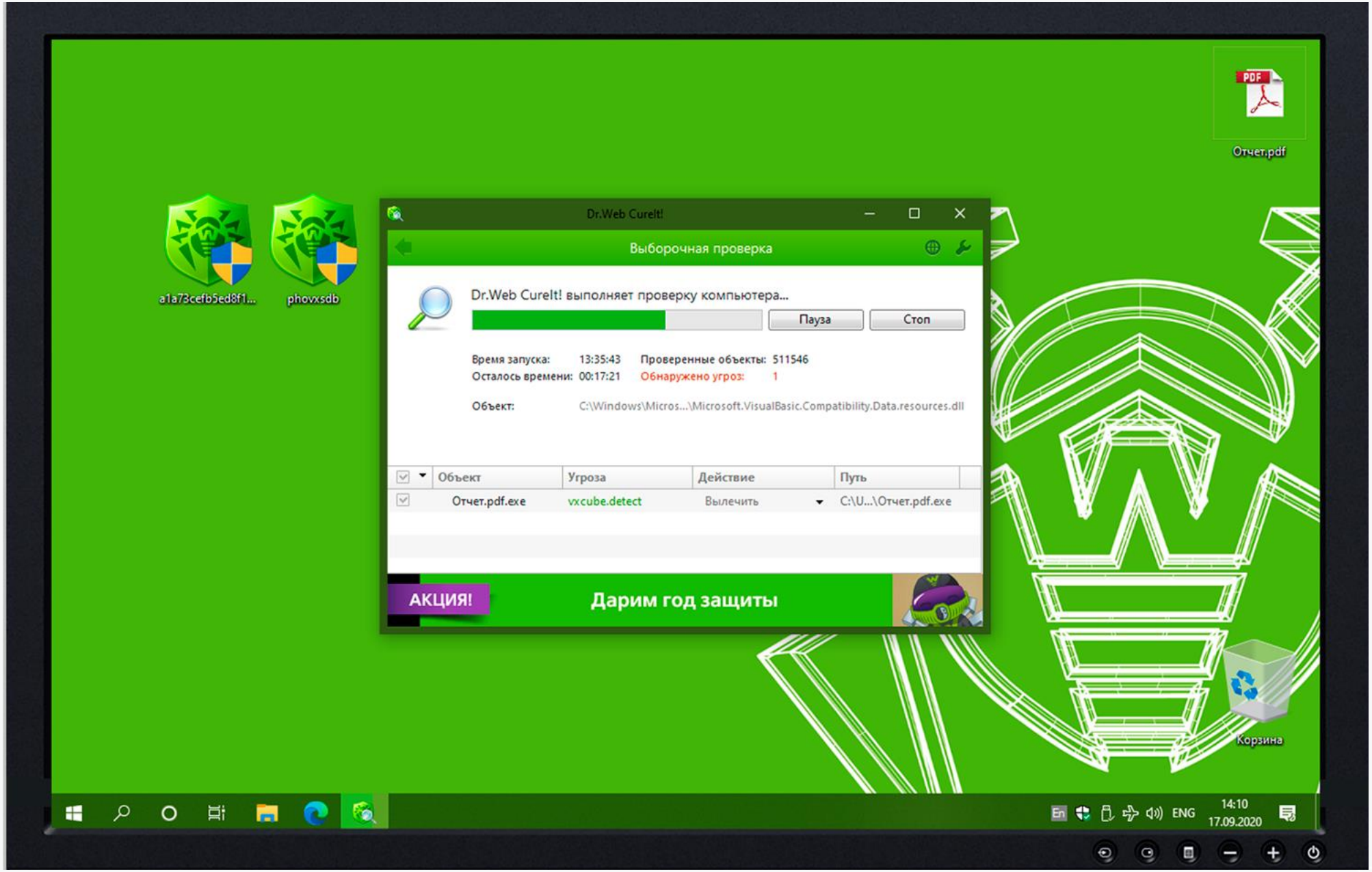


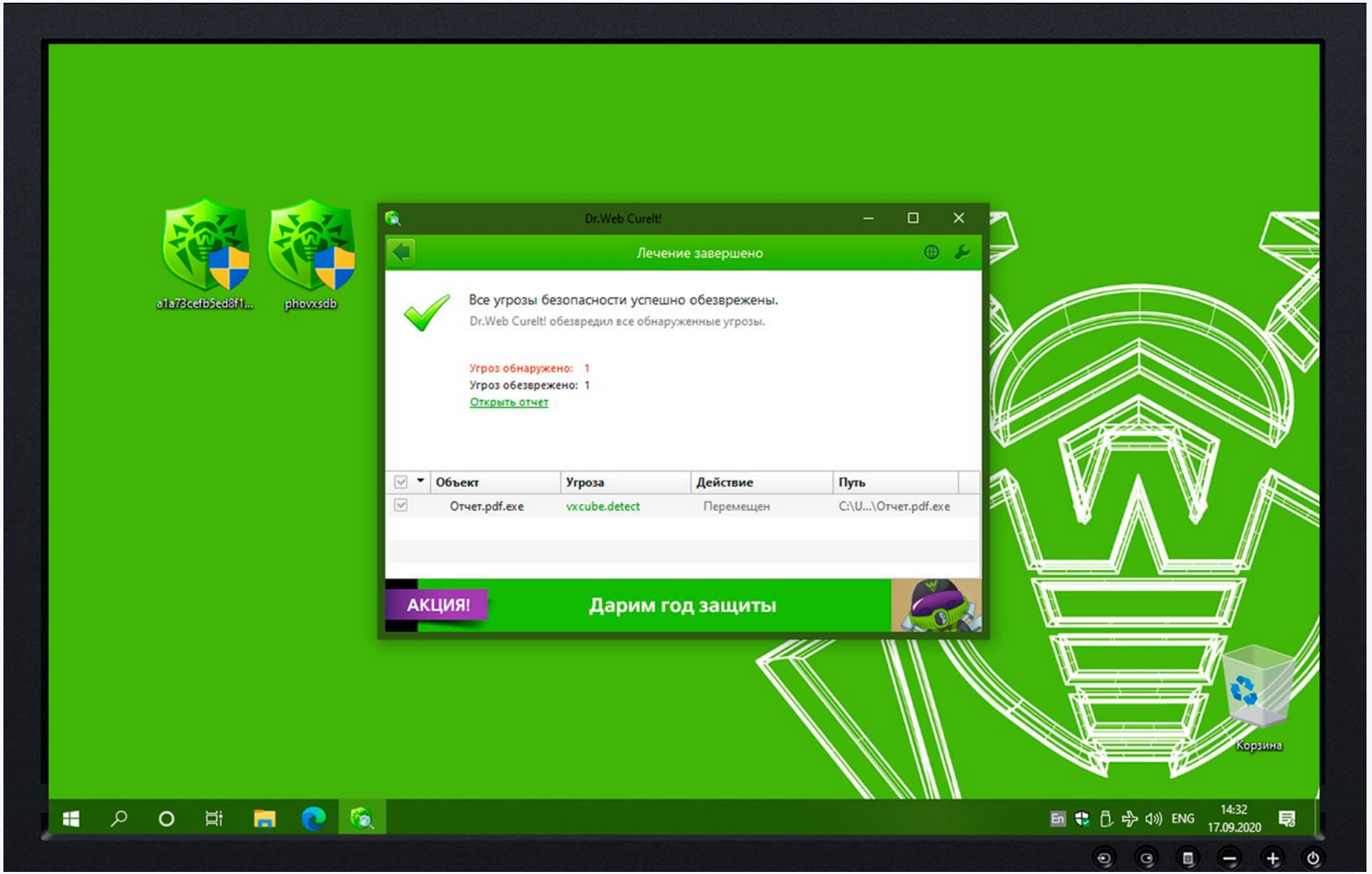





Отчет.pdf
Dr.WEB®
с 1992 года
антивирус.рф
a1a73cefb5ed8f15d1bec517d20f8a9cf9b03525_cureit
phovxsdb
Корзина
En
ENG
13:27
17.09.2020







Dr.WEB®
с 1992 года

А если угроза перехитрит Dr.Web vxCube?

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

Dr.WEB®
с 1992 года

Как устроена песочница

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

Dr.WEB®
с 1992 года

Как устроена песочница: Агент

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

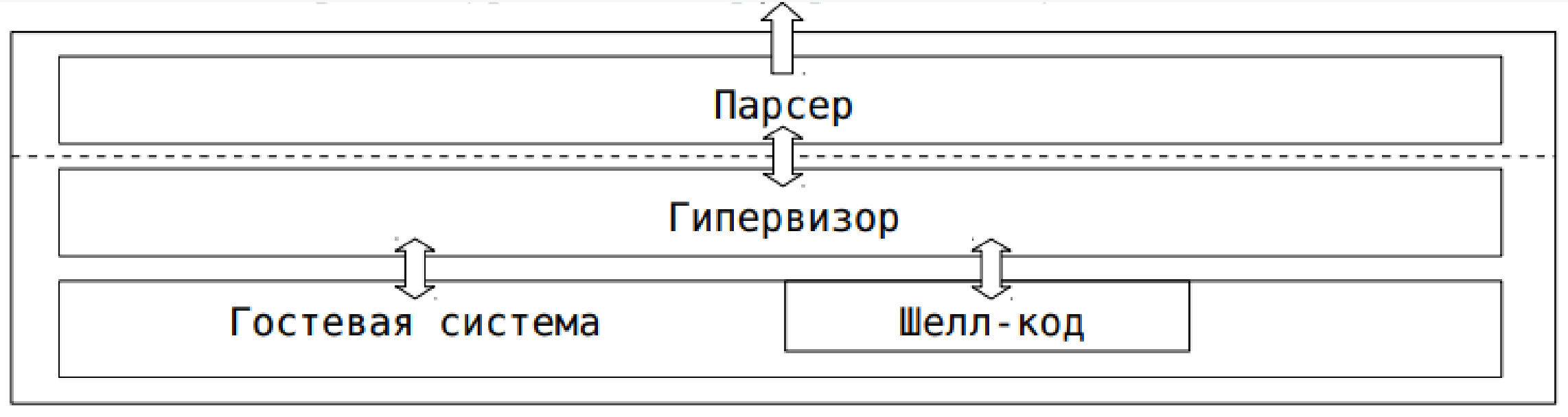
Dr.WEB®
с 1992 года

Как устроена песочница: Гипервизор

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

Dr.WEB®
с 1992 года

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



А теперь о подарке

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

Dr.WEB®
с 1992 года

Вопросы?