

КОД  
ИНФОРМАЦИОННОЙ  
БЕЗОПАСНОСТИ

27 СЕНТЯБРЯ 2018  
ЕКАТЕРИНБУРГ

#CODEIB

# Как разобрать троян (и зачем это нужно делать)



Вячеслав Медведев  
ООО «Доктор Веб»

**ТЕЛЕФОН:** +7 495 789-45-87

**EMAIL:** [v.medvedev@drweb.com](mailto:v.medvedev@drweb.com)

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

## Но что же послужило причиной для успешных атак?

- Отсутствовало сегментирование локальных вычислительных сетей (в частности, АРМ КБР и компьютер, используемый для подготовки XML-документа, находились в пользовательской локальной вычислительной сети);
- В ряде случаев отсутствовала блокировка автоматического запуска макросов в документах Microsoft Office;
- Пользователям были избыточно присвоены права локального администратора;
- В ряде случаев на атакованных рабочих станциях отсутствовали средства антивирусной защиты, либо их базы были устаревшими;
- Человеческий фактор — ненадлежащий контроль ответственными работниками кредитной организации установленной технологии подготовки, обработки и передачи электронных сообщений, содержащих распоряжение клиентов.

<https://bankir.ru/publikacii/20160721/spasibo-chto-fincert-10007831>

Так или иначе, но компьютер в сети заражен и нужно вычистить заражение *полностью*.

Что делать?

---

#CODEIB

---

Использовать сервис анализа потенциально вредоносных  
файлов

---

#CODEIB

---

# Отправляем файл на анализ, задав тестовое окружение

Dr.WEB vxCube

Справка Пользователи Выход

Выберите файл и условия, в которых его нужно исследовать, и вы получите подробный отчет о его поведении.

Выберите файл

Файл не выбран Обзор

Поддерживаемые типы файлов:

- Исполняемые файлы Windows (EXE, DLL, SYS, CPL)
- Документы Microsoft Office (DOC, DOCX, WPS, XLS, XLSX, PPT, PPTX, MHT, XML, ...)
- Файлы Acrobat Reader (PDF)
- JAVA исполняемые файлы (JAR, CLASS)
- Файлы сценарных языков (JS, VBS, WSF)

Журнал: все файлы ▾

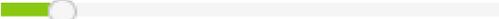
Пользователь	Имя файла	Тип	SHA1	Результаты анализа	Дата ▾	
admin@drweb.com	7ac27e518e66b2...	doc	3a6a51d704dd5cfe18968c29a5274521870b7540	Win7 32-bit	17 дек	...
admin@drweb.com	5928c5f4f16d014...	exe	5928c5f4f16d014aa9daa266b0fed1ebcbe4fc70	Win7 32-bit Win7 64-bit	16 дек	...

## Сервис анализирует самые опасные типы файлов:

- ✓ Исполняемые файлы Windows
- ✓ Документы Microsoft Office
- ✓ Файлы Acrobat Reader
- ✓ Исполняемые файлы JAVA
- ✓ Скрипт-файлы

### Дополнительные настройки

Управлять в интерактивном режиме

Время анализа  1 мин.

Задать команду для запуска файла  

\*rundll32.exe %SAMPLE%, ExportedFunction  
\*regsvr32.exe %SAMPLE%

## Dr.Web vxCube: анализ файла

Определение имен DNS-серверов... 28 %



Имя файла	core_image.js
Размер	12.1 Кб
SHA1	b4daf1293a881b272cee0a8218691b4faac9ea67

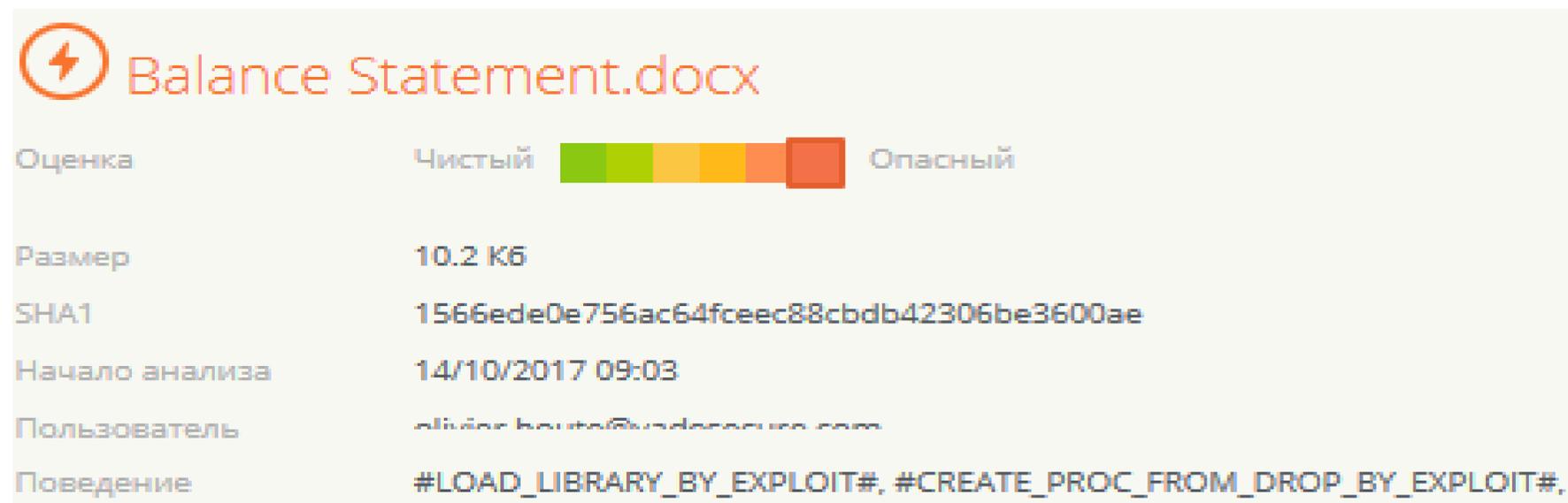
Как правило, проверка занимает не более одной минуты, но если исследователь считает, что этого недостаточно для полного анализа поведения подозрительного файла, желаемое время проверки можно задать в настройках.

Исследователь имеет возможность подключения к анализатору через VNC 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.



The screenshot shows a file analysis report for 'Balance Statement.docx'. At the top left is a lightning bolt icon in a circle. The file name 'Balance Statement.docx' is displayed in orange. Below it is a risk assessment section with a color-coded bar ranging from green ('Чистый') to red ('Опасный'). The bar is currently yellow-orange, indicating a medium level of risk. The report includes the following details:

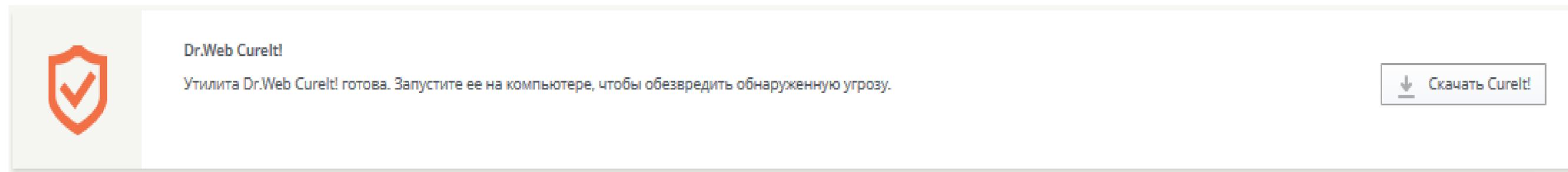
Оценка	Чистый  Опасный
Размер	10.2 Кб
SHA1	1566ede0e756ac64fceeec88cbdb42306be3600ae
Начало анализа	14/10/2017 09:03
Пользователь	ali@hackerone.com
Поведение	#LOAD_LIBRARY_BY_EXPLOIT#, #CREATE_PROC_FROM_DROP_BY_EXPLOIT#,

---

#CODEIB

---

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



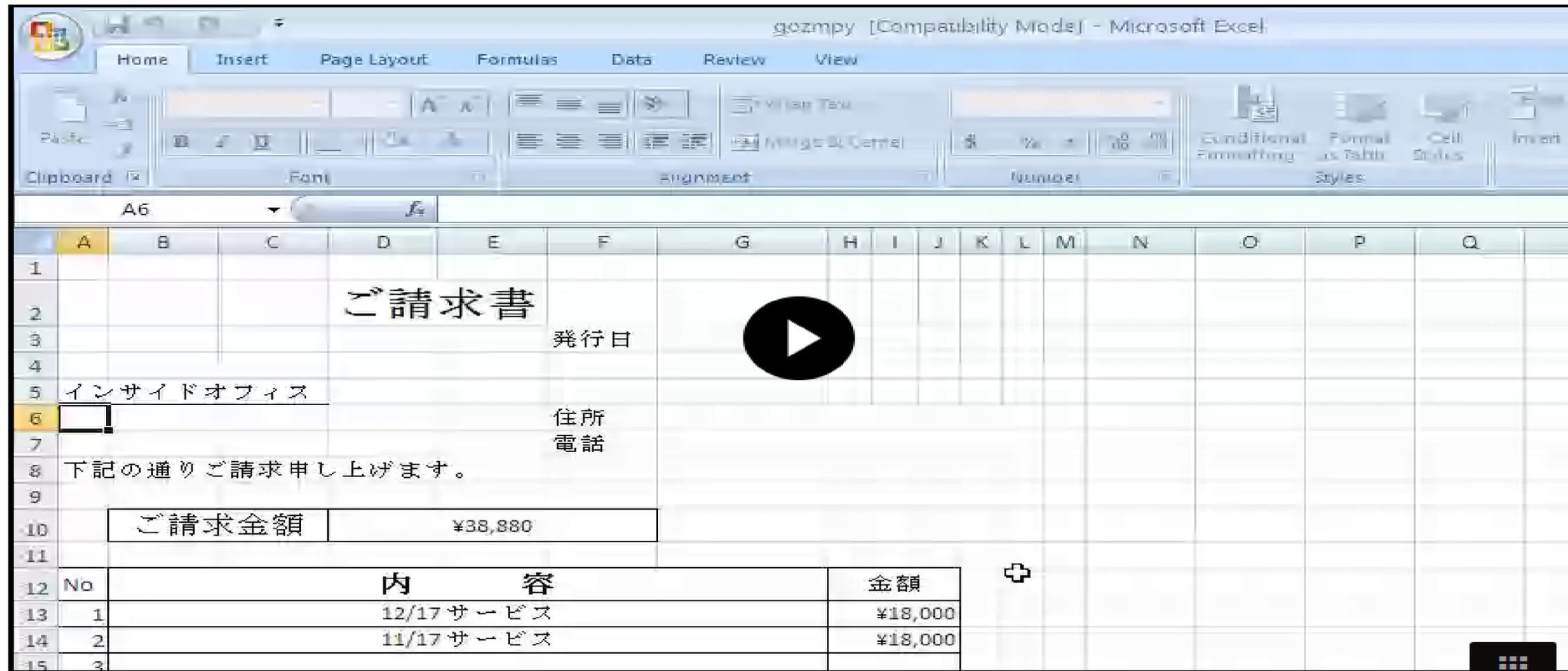
Dr.Web CureIt!  
Утилита Dr.Web CureIt! готова. Запустите ее на компьютере, чтобы обезвредить обнаруженную угрозу.

[Скачать CureIt!](#)

The image shows a notification banner for Dr.Web CureIt!. On the left is a shield icon with a checkmark. The text in the center states that the utility is ready and provides instructions to run it. On the right is a button with a download icon and the text 'Скачать CureIt!'.

#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

---

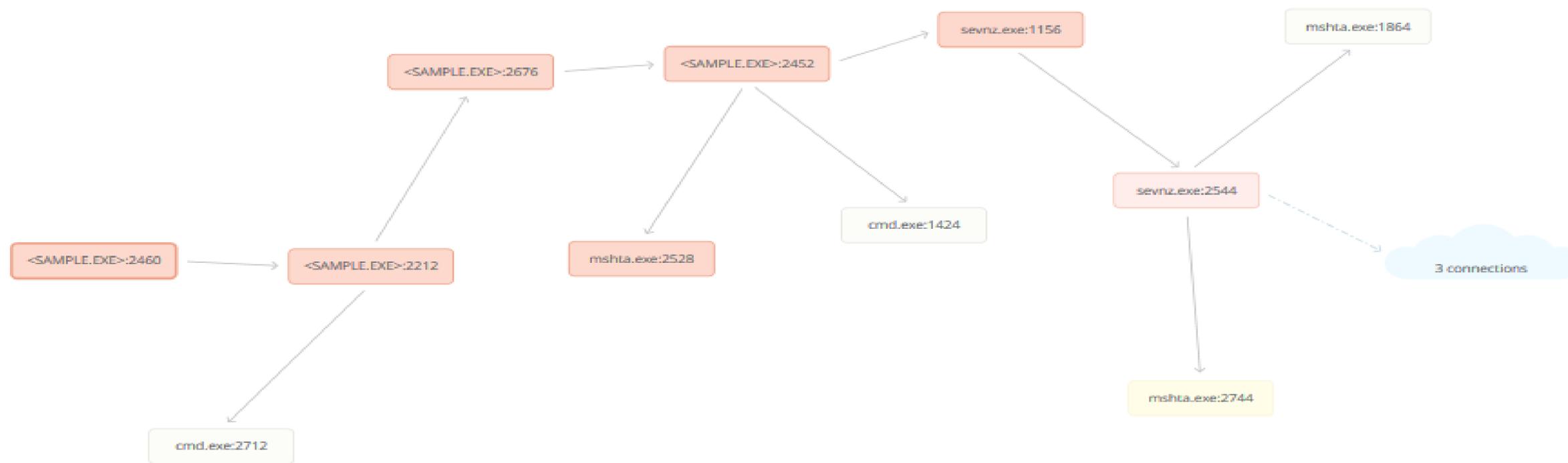
#CODEIB

---

# Примеры выявленных связей

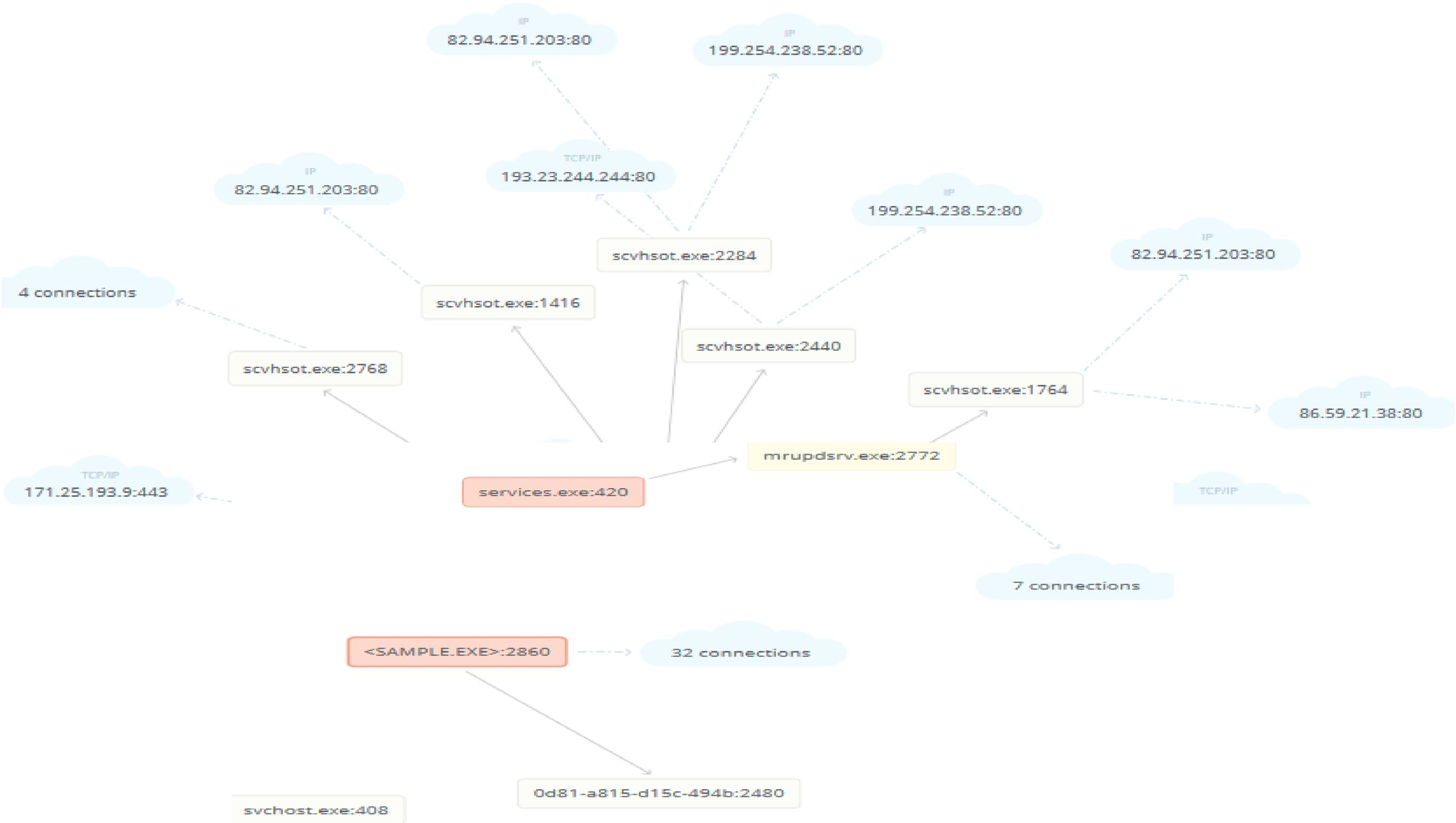
Overview [🔗](#)

→ process creation    - - - - -> injection    - · - · -> web query    1  100 process maliciousness



PID	2460
Full path	<PATH_SAMPLE.EXE>
Detected	Trojan.PWS.Papras.2923

# 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\sevzn.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()}catch(e){}.10);"" (со скрытым окном)
```

```
'%WINDIR%\syswow64\mshta.exe' "javascript:o=new ActiveXObject('WScript.Shell');x=new ActiveXObject('Scripting.FileSystemObject');setInterval(function(){try{f=x.GetFiles('sevzn.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\sevzn.exe' ' (со скрытым окном)
```

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

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

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

Запускает на исполнение:

```
'%WINDIR%\syswow64\mshta.exe' "javascript:o=new ActiveXObject('WScript.Shell');x=new ActiveXObject('Scripting.FileSystemObject');setInterval(function(){try{f=x.GetFiles('sevzn.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\sevzn.exe"
```

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

# 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

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	f683eb85535e34c41e5bf5da535d9dcc4ae8b2	—	↓
%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

Win7 32-bit      Обзор    Техническая информация    **Файлы и дампы памяти**    Журнал API    Карта сетевой активности

## Техническая информация

Вредоносные функции:

Создает и запускает на исполнение:

- '<LS\_APPDATA>\help.exe'
- '%TEMP%\tmpb117.exe' (загружен из сети Интернет)

Создает и запускает на исполнение (эксплоит):

- '%TEMP%\tmpb117.exe'

Создает и загружает библиотеки (эксплоит):

- %TEMP%\tmpb117.exe
- <SYSTEM32>\com\soapassembly\http10023492421142150tutu4png.dll

Запускает на исполнение:

- '%WINDIR%\microsoft.net\framework\v2.0.50727\vcsc.exe' /noconfig /fullpaths @"%TEMP%\9kf7tiw.cmdline"
- '%WINDIR%\microsoft.net\framework\v2.0.50727\cvtres.exe' /NOLOGO /READONLY /MACHINE:IX86 "/OUT:%TEMP%\RESB1A3.tmp" "%TEMP%\CSCB1A2.tmp"
- '%WINDIR%\microsoft.net\framework\v2.0.50727\vcsc.exe' /noconfig /fullpaths @"%TEMP%\uv9ghegw.cmdline"
- '%WINDIR%\microsoft.net\framework\v2.0.50727\cvtres.exe' /NOLOGO /READONLY /MACHINE:IX86 "/OUT:%TEMP%\RESAF7D.tmp" "<SYSTEM32>\com\SOAPAssembly\CSCAF67.tmp"

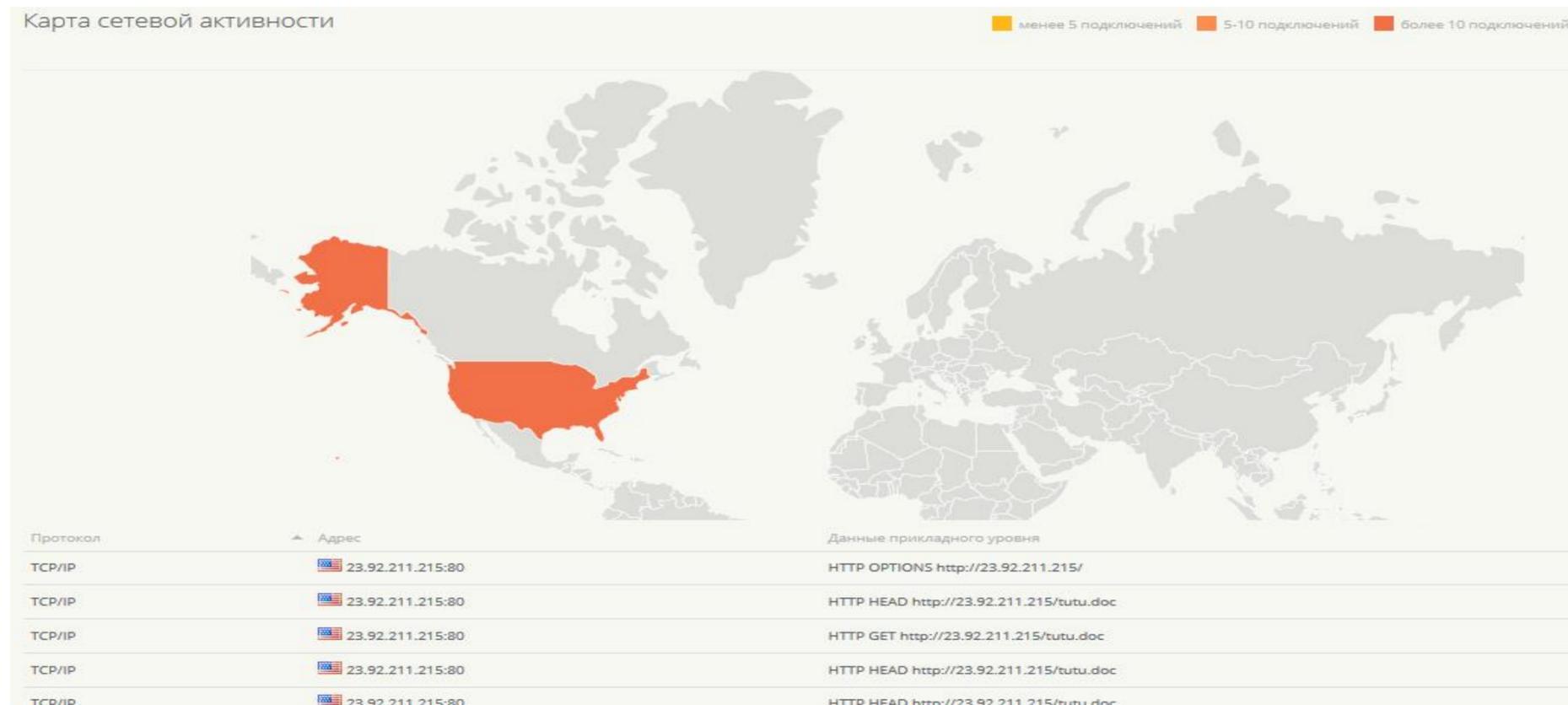
Изменения в файловой системе:

Создает следующие файлы:

- %TEMP%\cscb1a2.tmp
- %TEMP%\resh1a3.tmp

## 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.



## ДемOVERсия

ДЕМО ДЛЯ ДОМА    ДЕМО ДЛЯ БИЗНЕСА    СКАЧАТЬ    СЕРВИСЫ    РЕСУРСЫ    УТИЛИТЫ    БЕСПЛАТНО

### Демо Dr.Web vxCube

Чтобы отправить запрос на получение демо Dr.Web vxCube, заполните поля формы. Дальнейшую информацию вы получите на указанный вами адрес электронной почты.

Ваше имя\*

Ваша фамилия\*

Ваше отчество

Ваша должность или род занятий\*

Страна\*

Город\*

#CODEIB

Сервис имеет возможность интеграции с внутренними системами компании

Администратор компании может получать автоматический ответ о вредоносности файла

————— #CODEIB —————

## Лицензирование Dr.Web vxCube

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

————— #CODEIB —————

И немного о том, чтобы вам не пришлось пользоваться сервисом

— #CODEIB —

# Dr.Web Enterprise Security Suite 11

Dr.WEB Администрирование Антивирусная сеть Связи admin (drwcs) Выход

Администрирование > Журнал аудита

14-08-2014 00:00:00 - 14-08-2014 15:05:33 Обновить

Дата	Регистрационная линия	Адрес	Подсистема	Результат	Операция
14-08-2014 14:20:28	admin	tcp://192.168.150.20:1270	web	OK	группа, права, редактировать - группа Everyone, Изменение конфигурации SpIDer Guard для рабочих станций, Изменение конфигурации Сканера, Останов SpIDer Guard для рабочих станций группа, права, редактировать - группа Everyone, Запуск в мобильном режиме администратор, редактировать - администратор admin станция, принудительное обновление - станция XP-RU, только сбойные администратор, вход

Антивирусная сеть > Everyone > Статистика угроз

Сегодня 05-06-2018 00:00:00 - 05-06-2018 23:59:59 Обновить

### Классы угроз

- Инфицирован: 15
- Инфицированный архив: 4
- Инфицированный контейнер: 1

### Наиболее распространенные угрозы

- Trojan.Packed.29944: 3
- JS.Muldrop.18: 2
- Trojan.Carberp.30: 2
- Trojan.Download3.28161: 2
- Trojan.Encoder.25389: 2
- Trojan.Encoder.514: 2
- Trojan.Browseban.based.3: 1
- Trojan.Carberp.10: 1
- Trojan.Carberp.647: 1
- Trojan.KillAV.66: 1

Угроза	Тип	Станции	Итого
W97M.Siggen.1	Инфицирован	1	1

## Dr.Web Enterprise Security Suite 11

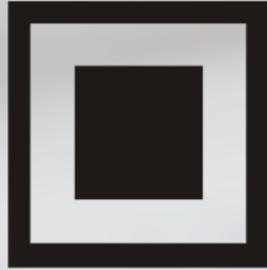
1. Обнаружение вредоносных программ с помощью машинного обучения
2. Новые функции безопасности
3. Защита от сканирования
4. Новый интерфейс
5. Новые возможности по работе на плохих линиях связи
6. Возможность настройки для каждого пользователя защищаемой станции
7. Новые возможности Брандмауэра Dr.Web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

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

27 СЕНТЯБРЯ 2018  
ЕКАТЕРИНБУРГ

#CODEIБ

**Благодарим за внимание!**

**Номер службы технической поддержки**  
**8-800-333-7932**

**Запомнить просто! –**  
**возникла проблема – набери DRWEB!**  
**8-800-33-DRWEB**

