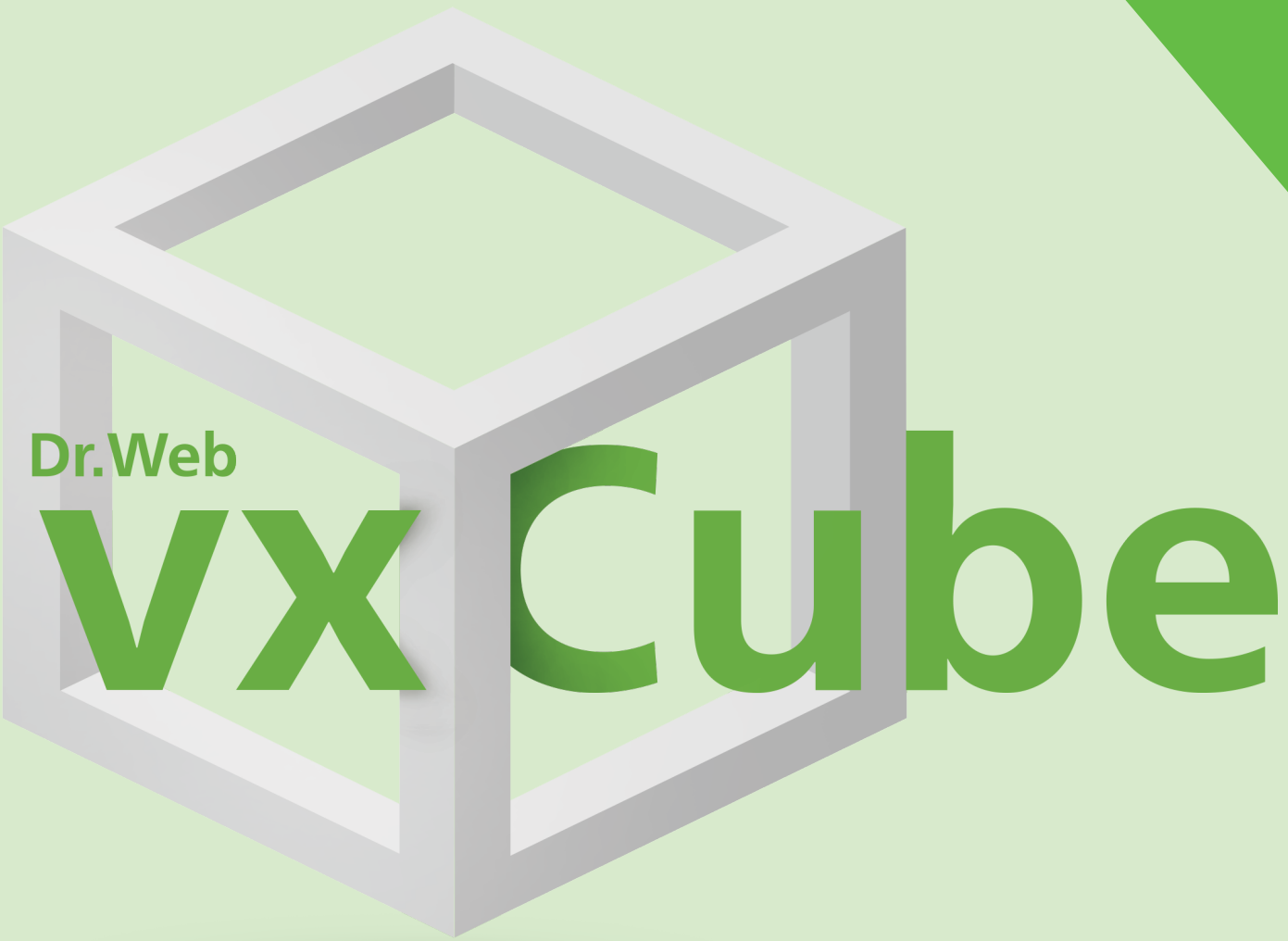
Dr.WEB



Песочница Dr.Web vxCube

Анализатор подозрительных файлов

О компании

«Доктор Веб» — российский разработчик антивирусных решений и технологий выявления, предупреждения и противодействия кибератакам под маркой Dr.Web. Наша компания — ключевой игрок на отечественном рынке программных средств обеспечения базовой потребности бизнеса — безопасности информации.

Собственные исследования в сфере ИБ и развитие технологий Dr.Web ведутся с 1992 года и направлены на то, чтобы отвечать на конкретные и актуальные угрозы, с которыми сталкиваются предприятия и частные пользователи. Мы посвятили более 30 лет разработке антивирусных решений, которые становятся первым барьером на пути вредоносного ПО и интернет-мошенничества.

Dr.Web соответствует концепции «внутри сложно, снаружи — просто». Им удобно пользоваться, его работа незаметна, поскольку мы исходим из того, что пользователь ищет продукт, который функционирует «бесшумно» и не отвлекает внимание.

«Доктор Веб» имеет свою антивирусную лабораторию, глобальную службу вирусного мониторинга и службу технической поддержки. ПО Dr.Web постоянно проходит сертификации у регуляторов, что позволяет применять его в системах с повышенными требованиями к безопасности.

Dr.Web vxCube: безопасность в кубе!

- Песочница тщательно маскируется под реальную систему.
- Она может противостоять более чем 370 техникам своего обнаружения.

Что делает

- Анализирует и регистрирует все действия подозрительного файла — в том числе изменения реестра, создание или изменение файлов, обращения к сетевым ресурсам, что позволяет сделать вывод в том числе о наличии недекларированных возможностей.
- Формирует подробные отчеты по результатам анализа — как в текстовом, так и в видеоформате, — а также карты сетевой активности.
- Предоставляет API-интерфейс для интеграции с ИТ-инфраструктурой компании.
- Интегрируется с Dr.Web для почтовых серверов UNIX для автоматической проверки почтовых вложений «на лету» или может анализировать копию почтового трафика, не влияя на скорость передачи писем.
- Создает специальную сборку утилиты Dr.Web CureIt! для нейтрализации выявленной угрозы.

Как делает

- Осуществляет одновременный анализ одного объекта в Windows XP (x32), Windows 7 (x32/x64), Windows 10 (x64) и в различных версиях приложений (подробный перечень программного обеспечения, установленного на виртуальных машинах, приведен в документации).
- Анализирует приложения для мобильной платформы Android в формате APK (включая списки разрешений и намерений — специальных механизмов, описывающих выполняемые программой операции и активности).
- Анализирует обращения подозрительного объекта к удаленным сетевым ресурсам на предмет наличия их в базах вредоносных ресурсов Dr.Web.
- Анализирует и оценивает вредоносность действий, выполняемых подозрительным объектом в виртуальной среде.
- Предоставляет выгрузку индикаторов компрометации в STIX/MAEC.
- Позволяет подключиться к виртуальной машине с помощью VNC-клиента (Virtual NetworkComputing) и влиять на процесс анализа.

Dr.Web vxCube не требует установки — достаточно авторизоваться на сайте и проверить любой файл, после чего пользователю выдается полный отчет о потенциальной угрозе.

Какие файлы проверяет

- Исполняемые файлы Windows
- Пакеты Android (APK)
- Документы Microsoft Office
- Файлы Acrobat Reader
- Установочные файлы Windows
- Исполняемые файлы Java
- Файлы сценарных языков
- Файлы .nix
- Исполняемые ELF-файлы
- Python, Perl и Bash-скрипты

Файлы в архивах (ZIP,RAR) и другие (HTA, LNK, MOF) проверяются только по API

Также Dr.Web vxCube поможет проверить применяемые в корпоративной сети программы — бывают случаи, при которых обновление софта оборачивается новыми, незадекларированными возможностями для вредоносного ПО.

Какие ОС поддерживает

- Windows XP (x32)
- Windows 7 (x32, x64)
- Windows 10 (x64)
- Android 7.1
- Astra SE 1.7 («Воронеж»)
- Astra CE 2.12 («Орел»)

Как лицензируется

Облачная версия

Подразумевает отправку файлов для анализа на серверах «Доктор Веб» (100/500/1000/3000 файлов) и генерацию лечащей утилиты Dr.Web CureIt! в случае обнаружения угроз.
Лицензируется сроком на 12 месяцев.

Локальная (on-premise) версия

Позволяет анализировать неограниченное количество подозрительных файлов в пределах собственной сети без их отправки на внешние сервисы, лицензируется сроком на 12, 24 или 36 месяцев.

Комплексная защита вашего бизнеса

drweb.ru

2024

0+