

Взгляд изнутри на технологию сканирования Emsisoft

1. Два ядра сканирования лучше, чем одно

Одним из компонентов, обеспечивающих нашему сканеру его расширенные возможности обнаружения, является его двойное ядро. Мы стремимся предоставлять наилучшие технологии сканирования, поэтому мы спроектировали нашу программу так, чтобы при необходимости менять сторонние ядра.

Вы, возможно, помните, что мы перешли с движка Ikarus на [Bitdefender](#) в 2012. Эффективное сочетание наших технологических разработок и тонкого чувствования будущего развития передовых антивирусных решений позволяет нам всегда быть на шаг впереди.

Расширенный сигнатурный метод обнаружения

Ядро, которое мы разработали, дополняет второе от BitDefender, и они объединены бесшовно, что позволяет максимизировать эффективность.

Сигнатурный метод обнаружения – один из способов, которые мы используем для обнаружения нежелательных программ. Это значит, что мы ищем программы через уникальные подписи, сигнатуры, которые сходны с отпечатками пальцев, и сканируем ваш компьютер на эти угрозы.

В Emsisoft большая часть времени нашей лаборатории идёт на создание сигнатур для обнаружения ПНП (потенциально нежелательных программ) и создание кодов удаления вредоносных программ для отдельных заражений. Мы проводили исследование в начале этого года и обнаружили, что более 74% от общего объема ПНП обнаруживаются с помощью нашего ядра сканирования собственной разработки.

Максимальная эффективность с двойным сканером

Наличие двух движков означает, что мы можем максимально эффективно обнаруживать новые сигнатуры угроз, которые появились совсем недавно. Это происходит так быстро, что порой разработчики обоих ядер добавляют сигнатуры, разработанные для одной и той же угрозы, в течение часа!



Два ядра сканирования более эффективны, чем одно

Беспокоетесь о повышенной нагрузке на память? Не стоит. Мы регулярно удаляем дублирующиеся сигнатуры, снижая нагрузку на память. 90% сигнатур, созданных ядром Emsisoft являются дубликатами и не используются в обнаружении вредоносных программ.

Не беспокойтесь и о времени сканирования: файлы на вашем жестком диске читаются лишь один раз, а затем сканируются обоими движками. Это гарантирует, что время сканирования будет минимальным, не смотря на то, что мы используем два ядра. То, что наша двухъядерная технология работает быстрее, чем продукты многих крупных брендов, использующие только одно ядро – не случайность!

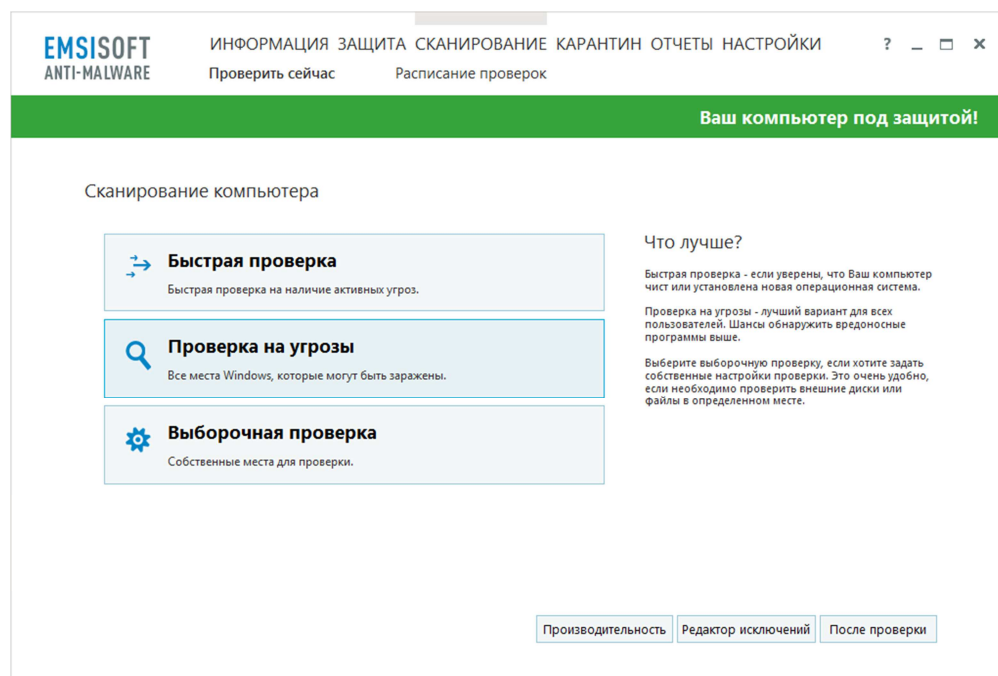
А как это работает на практике?

Все просто: все угрозы отмеченные буквой (A) обнаруживает наш движок, буквой (B) – ядро от Bitdefender.

В двух словах: Мы считаем, что два ядра лучше, чем одно, и мы используем нашу собственную технологию для обнаружения тех угроз на вашем компьютере, которые другие средства могли бы упустить. Но мы не готовы поступиться эффективностью этого процесса – Emsisoft не забивает собой память ПК и ищет угрозы оптимально быстро. Чтобы увидеть некоторые цифры о реальной мощности второго ядра сканирования в наших продуктах, вы можете заглянуть в [эту](#) статью, опубликованную ранее в этом году.

2. Доступные методы сканирования

На рисунке показан список методов сканирования доступных в Emsisoft Emergency Kit, так же, как и в Emsisoft Anti-malware и Emsisoft Internet Security:



Emsisoft Anti-Malware – Три типа проверок

Быстрая проверка

Быстрое сканирование помогает обнаружить любые активные заражения на вашем компьютере. Делается это путем сканирования всех запущенных программ и их модулей. Быстрая проверка также производит поиск следов. Следы – это известные пути к файлам и записям реестра вредоносных программ. Проще говоря, чтобы найти вредоносные программы, антивирус ищет их следы.

Кроме того, быстрая проверка использует драйверы для поиска активных руткитов. Руткит – это тип вредоносных программ, которые скрывают определенные файлы или ключи реестра от обычных методов обнаружения. Мы обсудим руткиты и как они работают далее, при рассмотрении особенностей Выборочной проверки.

Мы рекомендуем быструю проверку для автоматических / плановых проверок после загрузки или входа в систему. Она обычно занимает около 30 секунд, так что вам не придется долго ждать!

Проверка на угрозы

Проверка на угрозы похожа на быстрое сканирование, но она к тому же сканирует файлы во всех папках, в которых могут скрываться активные вредоносные программы. Наш сканер знает около сотни мест, где могут скрываться вредоносные программы. Одним из преимуществ здесь является то, что вредоносные программы действительно предсказуемы в выборе мест для установки. Наша команда постоянно обнаруживает новые места локализации заражений. Они могут обновить наше программное обеспечение в течение нескольких минут, чтобы продукты Emsisoft оставались актуальными.

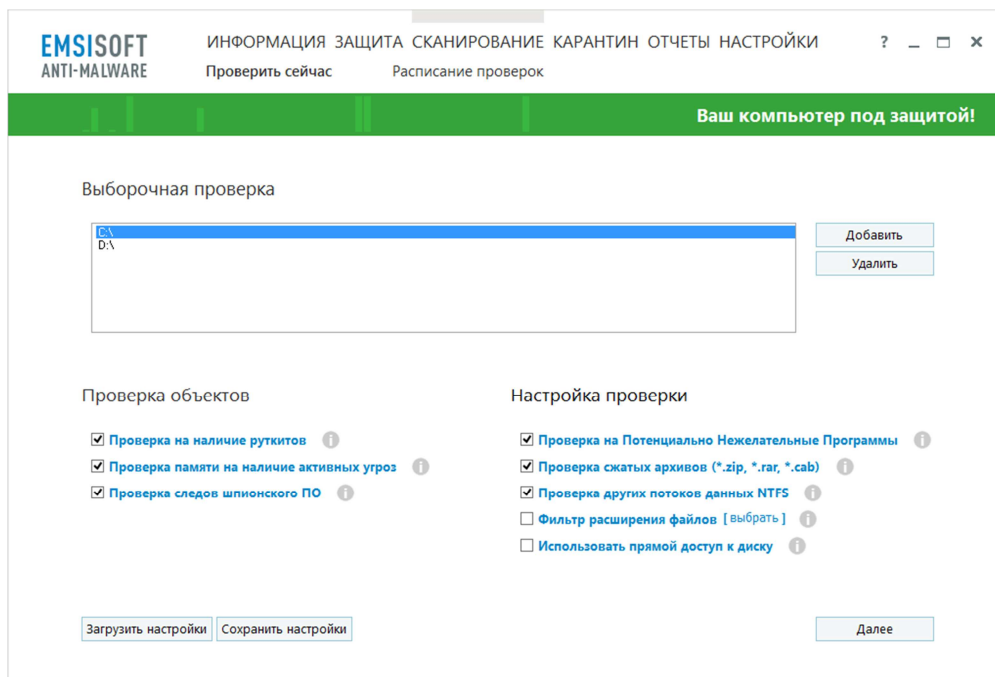
Мы рекомендуем проверку на угрозы как проверку по умолчанию, когда вы подозреваете, что в вашей системе есть активная угроза. Проверка на угрозы не обнаруживает файлы неактивных вредоносных программ, но, к счастью, неактивные файлы – это неактивные угрозы. Такие файлы можно просто удалить с ПК, как устаревший документ Word или неприглядные фото из отпуска.

Выборочная проверка

Так как режим Выборочной проверки по умолчанию настроен на выполнение полного сканирования, используйте эту опцию, если вы хотите произвести очень тщательную проверку на наличие вредоносных программ и сканирование всех файлов на всех дисках компьютера. Выборочная проверка занимает значительное количество времени, и не рекомендуется для частого или ежедневного использования. Это сканирование вы можете запускать несколько раз в год, чтобы быть абсолютно уверенным, что на вашем компьютере ничего вредоносного не скрывается.

3. Дополнительные функции сканера

Одним из замечательных особенностей выборочной проверки является то, что вы можете контролировать настройки сканирования. Если вы посмотрите на настройки, то вы увидите все доступные варианты. Некоторые из них включены по умолчанию, а другие нет. Мы подробно расскажем о них ниже, и вы сможете сориентироваться, какие из них могут быть полезными для решения ваших задач сканирования.



Поиск руткитов

Обычно сканирование файлов использует Windows API (Интерфейс прикладного программирования) для чтения файлов. Вы можете представить себе API как основу для создания приложений, которая состоит из подпрограмм и протоколов.

К сожалению, несмотря на то, что использование Windows API – зачастую оптимальное решение в плане обеспечения скорости и эффективности, API могут манипулироваться руткитами.

Что такое руткиты?

Руткиты, как солдаты в камуфляже. Они вписываются в систему с помощью ряда различных средств и делают это путем изменения списков и таблиц, которые говорят системе, где найти код (это называется “перехват”).

Когда антивирусное программное обеспечение обращается к этому списку доступных файлов, руткит манипулирует списком, чтобы пропустить файл – файл вредоносной программы. После того, как файл становится невидимым, его будет тяжело обнаружить простым сканером.

Чтобы найти скрытые руткиты, наш сканер использует собственную файловую систему NTFS при поиске руткитов. Этот код не зависит от общих API, что даёт нам преимущество перед скрытыми руткитами.

Пусть руткиты умеют маскироваться, супер-зрение сканера Emsisoft их обнаружит!

Удаление руткитов

Удаление руткитов, как правило, очень сложная процедура. Иногда руткиты скрываются даже в таких необычных местах как загрузочный сектор жесткого диска вашего компьютера. Простое удаление этих вредоносных файлов часто приводит к невозможности загрузки с диска.

Наши специалисты часто помогают пострадавшим от неудачных попыток очистки другими антивирусными продуктами, поэтому мы знаем не понаслышке, насколько важно использовать надежную программу.

Руткиты обычно требуют очистки вручную. Наш сканер посоветует вам проконсультироваться с нашими экспертами по удалению руткитов. Они проанализируют и идентифицируют тип руткита и предоставят вам подробную, пошаговую инструкцию как его удалить, без риска для стабильности работы вашего компьютера.

Вы могли бы задаться вопросом, почему все проверки не полагаются на собственный сканер? Потому, что чтение прямо из файловой системы (прямой доступ к дискам), как правило, очень сложный процесс и, часто, гораздо более медленный, чем при использовании Windows API. Иначе мы бы использовали наш собственный анализатор работающий под NTFS для всех проверок.

Сканирование следов

Сканирование следов (сканирование, которое ищет признаки оставшиеся от заражения) может быть одним из трех типов:

– **Следы файлов:** Это пути исполняемых файлов на жестком диске, которые используются исключительно вредоносными программами. Это, по существу, следы на жестком диске, которые существуют независимо от расположения папок других программ.

Пример: C:\Windows\explore.exe (можно перепутать с exploreR.exe).

-**Следы папок:** Они похожи на следы файлов, но существуют внутри папок других распространенных приложений, таких как папка настроек Google Chrome.

Пример: C:\Program Files(x86)\PUP Folder\.

-**Следы реестра:** Это записи в базе данных системного реестра, которые указывают на наличие вредоносных программ. След в реестре указывает на заражение внутри настроек компьютера. Это наиболее опасные следы, такой вирус может значительно замедлять работу вашего компьютера.

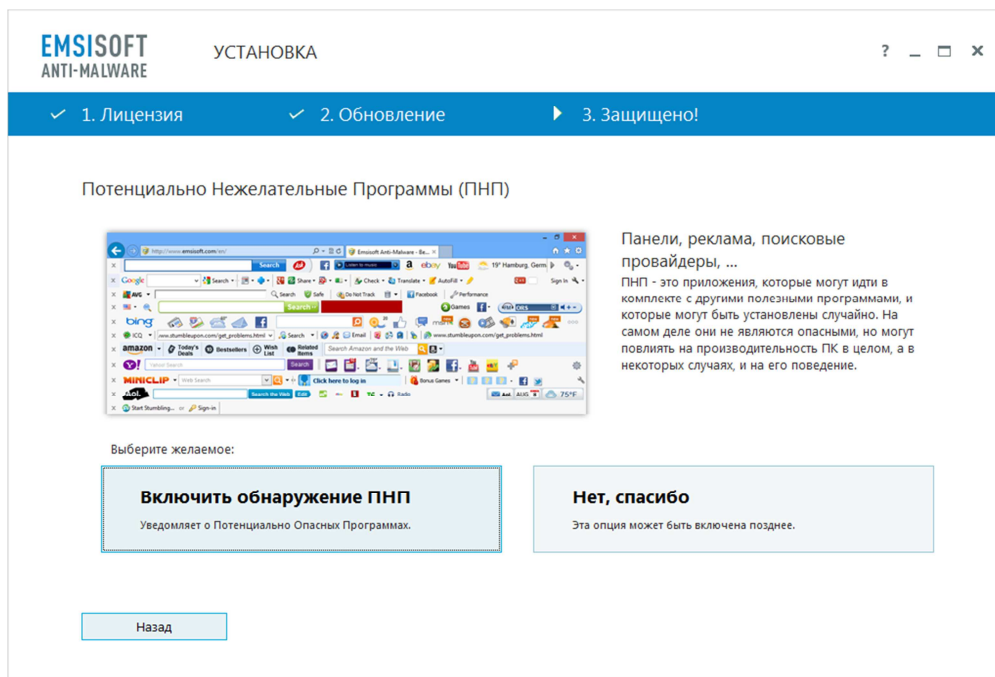
Пример: HKLM\Software\Windows\CurrentVersion\Run.

Важно отметить, что если след от вредоносной программы был обнаружен, это не обязательно означает, что есть активная инфекция. Вполне может быть – это остатки от предыдущей, неполной очистки.

В целом, когда есть активная инфекция, следы, как правило, находятся рядом. Вы можете очистить их в любое время.

Обнаружение ПНП

По юридическим причинам, мы не можем называть все нежелательные программы “вредоносными”. Термин ПНП был изобретён антивирусной индустрией несколько лет назад. Он обозначает потенциально нежелательные программы. Вообще, ПНП существуют для того, чтобы их создатели могли получать дополнительный доход от показа рекламы, изменения поиска по умолчанию, либо от сбора личных данных для продажи рекламодателям.



Emsisoft Anti-Malware – Потенциально Нежелательные Программы (ПНП)

Обнаружение ПНП должно быть включено при первой установке нашего программного обеспечения. В Emsisoft Anti-Malware и Emsisoft Internet Security может быть включена в настройках защиты.

Сканирование в сжатых архивах

Сжатые архивы – это файлы, в которых содержатся другие файлы в сжатом виде. Самые часто встречающиеся примеры: ZIP, RAR, или 7Z, но есть сотни других, менее известных сжатых архивов. Даже программы с расширением EXE могут быть на самом деле самораспаковывающимися архивами и содержать другие файлы (как правило, для наиболее эффективной передачи данных).

Вредоносные файлы, которые упакованы в архивный файл не могут напрямую запуститься изнутри сжатого архива. Из-за этого, архивы обычно не считаются опасными в самостоятельном виде. В результате, многие сканеры исключают из проверки архивы или устанавливают ограничения сканирования архива размером порядка 200 Мб.

Распаковка архивов занимает невероятно много времени и отнимает много системных ресурсов. Вы можете отключить функцию проверки архивов, если уверены, что архивы на вашем ПК совершенно безвредны.

Сканирование в альтернативных потоках данных NTFS

В 1993 году, с введением NTFS (файловая система Windows NT) по умолчанию в системах Windows NT (предшественник 2000, XP, 7, 8, и т.д.), была добавлена новая функция под названием “Альтернативные потоки данных”. Файлы теперь могли хранить мета-данные в скрытых слоях.

К сожалению, эти потоки также могут быть использованы для хранения других типов вредных данных, например целых вредоносных программ – *и всё это в текстовом файле весом в 0 байт.*

Перенесемся в сегодняшний день, и безобидное расширение файла может содержать опасный код, который может быть запущен автоматически через автозапуск ключа реестра.

Когда опция сканирования Альтернативных потоков данных NTFS включена, сканер исследует все слои данных на предмет скрытых угроз.

Использование фильтра расширений

С фильтром расширений файлов, Вы можете ограничить сканируемые файлы по типу. Многие типы файлов не могут быть использованы для размещения вредоносного кода, поэтому многие могли бы изначально думать, что их проверка – пустая трата времени.

Например, все исполняемые файлы Windows начинаются с последовательности байтов “MZ”, которые сообщают операционной системе, что файл может быть запущен на компьютере. Проверка этих последовательностей байтов (или “волшебных байтов”) является надежным методом, и почти таким же быстрым, как проверка самого расширения файла.

Но важно отметить: эта функция отключена в настройках по умолчанию и на то есть причина. Сканер не просто сверяет тип расширения файла по имени, но и ищет специфические маркеры типа внутри файла. Расширения можно легко подменить, чтобы обмануть сканер, а содержание файла подменить не получится.

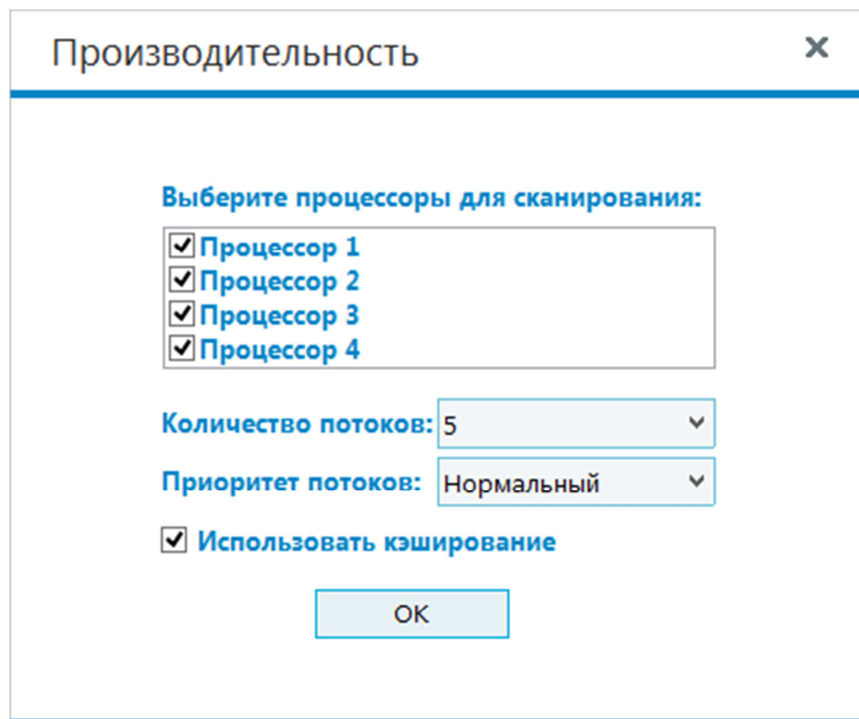
Режим прямого доступа к диску

Как упоминалось выше, сканер способен искать файлы, которые скрыты (руткиты), используя собственную файловую систему NTFS вместо API. Режим прямого доступа к диску позволяет сканеру Emsisoft обойти защиту руткита и перейти непосредственно к местоположению файла вредоносной программы.

Недостатком этого метода является затрата огромного количества времени. Поэтому его можно использовать только для определенных папок, которые могут содержать руткиты. Пользы от использования этого метода для сканирования всего диска мало, поэтому эта опция по умолчанию отключена. Поиск на руткиты всегда использует функцию прямого доступа к диску, поэтому будьте уверены, он будет автоматически использован в случае необходимости.

Настройки производительности

При просмотре области сканирования, вы увидите небольшую опцию “Настройки производительности” ниже трёх основных методов сканирования. Если вы щёлкните по ней, то откроется всплывающее окно с расширенными функциями для настройки скорости сканера:



– Процессоры

По умолчанию, все доступные процессоры используются для сканирования. Обратите внимание, что четырёхъядерные процессоры, как правило, отображаются в виде 8 виртуальных процессоров. Вы можете отключить один или два из них, если планируется долгое сканирование, а вам нужно работать в какой-то программе.

– Количество потоков

Потоки могут быть представлены как процессы, которые работают параллельно. Представьте себе дороги, по которым информация движется к ядру.

Если сканер однопоточный (использует один поток), файл будет считываться с диска, а затем сканироваться и так далее. Используя многопоточную технологию каждый виртуальный процессор может сканировать файл параллельно, не прерывая других.

По умолчанию, количество потоков равно количеству доступных процессоров + 1. Причина в том, что один поток с низкими требованиями к процессору используется для чтения данных с жесткого диска (как правило, параллельное чтение – не вариант), а затем файлы распределяются по всем процессорам для одновременного сканирования. Это самая сложная часть задачи для процессора.

– Приоритеты

По умолчанию, Windows определяет, какие программы получают какой процент от общих имеющихся аппаратных ресурсов (процессорного времени). Но вы можете определить больший или меньший приоритет для сканера Emsisoft. Используйте приоритет выше среднего чтобы сканирование было завершено в кратчайшие сроки (даже если параллельно работают другие программы). Используйте приоритет ниже среднего, если вы работаете с программами, которые требуют более высокого приоритета. Это хороший вариант, когда вам всё равно сколько будет работать сканер, лишь бы он не мешал работать вам.

– Использование расширенного кэширования

Кэширование означает, что файлы, которые были проверены и признаны безопасными, не сканируются снова и снова. Например, если файл был на вашем компьютере в течение очень долгого времени, и уже отсканирован много раз без каких-либо обнаружений, то маловероятно, что он вредоносный. Умный алгоритм оценивает вероятность того, что файл безопасен, а затем пропускает его при последующем сканировании.

4. Дополнительные функции

Контекстное меню сканирования в проводнике (не доступно в Emsisoft Emergency Kit)

Интернет кишит троянами и вирусами, которые только и мечтают попасть внутрь вашей системы. Но сканирование через контекстное меню может выступить как средство профилактики заражения вирусами в первую очередь.

Emsisoft Anti-Malware и Emsisoft Internet Security имеют полезную опцию интеграции в Windows Explorer, которая сможет сэкономить вам много времени, если вы выполняете частые сканирования. Просто кликните правой кнопкой мыши на любом файле или папке в Проводнике и выберите опцию “Сканировать в Emsisoft” в контекстном меню, чтобы запустить выборочную проверку.



```
Administrator: C:\Windows\System32\cmd.exe
Emsisoft Commandline Scanner v. 10.0.0.5401
©© 1987-2015 Emsisoft - www.emsisoft.com
ahdoo.exe [path] [parameters]

Scan parameters (can be used together):
/?:-? /file:[path] Scan files. Full path to file or folder required.
/quick Tests all active processes. Ignores traces and
tracking/tracklog.
/outline Tests all active processes, but only important folders will
be scanned.
/ht, /trackhits Tests for active hostkeys.
/so, /memory Tests memory for active malware.
/so, /traces Tests for ignored traces.
/so-[handle] /pid-[PID] Scan file by handle. Process ID of the
handle is required.
/so-[pointer] /so-[size] /pid-[PID] Scan buffer. Buffer size and process ID
are required.

Scan settings parameters (used with scan parameter):
/so, /elnet Potentially unwanted programs (PUP).
/so, /archives Tests in compressed archives (zip, rar, cab).
/so, /url Tests in HTTP/HTTPS/FTP sites.
/so, /subdomains Tests subdomains.
/so, /http[headers] Use direct link access.
/so-? /http[headers] Use a header in HTTP/HTTPS format.
/so-? /http[headers] Use a header in XML format.
/so-? /http[headers] Use only specified file extensions, comma
delimited.
/so-? /http[headers] Use all except the specified file extensions.
/so-? /whitelist-[file] Load whitelisted items from the file.
/so, /elnet Deletes found objects including references.
/so, /elnetquick Deletes found objects quickly.
/so-? /quarantine-[folder] Put found malware into quarantine.
/whitelist[load] Allow automatic OR restore, if this is required
to remove found treats/objects.

Malware handling parameters (commandline parameters):
/ol, /quarantine-list List all quarantined items.
/ol-? /quarantine-restore=[n] Restore the item number n of the quarantine.
/ol-? /quarantine-delete=[n] Delete the item number n of the quarantine.

Update settings parameters:
/so, /update Update Malware signatures.
/so, /update[meta] Update Malware signatures (meta).
/so-? /update[part] Proxy address and port number.
/so-? /update[server] Proxy server name.
/so-? /update[password] Proxy user password.

General parameters:
/?, /help Show help message.

Result codes:
0 - No infections were found.
1 - Infections were found.

C:\BBS\kko>
```

Emsisoft Commandline Scanner

Сканер, управляемый с помощью командной строки

Commandline Scanner подходит для профессионалов, которые не нуждаются в графическом интерфейсе для выполнения сканирования.

Commandline Scanner обеспечивает полный интерфейс командной строки, который включает в себя все функции сканера на основе ОС Windows. Прежде всего, он предназначен для автоматических проверок, инициированных другими программами или сценариями, которые требуют возвращаемого значения для дальнейшей обработки. Узнайте больше о доступных параметрах Commandline Scanner [здесь](#).

5. Очистка заражений

Обнаружение активных угроз лишь один из этапов на пути к очистке компьютера. Очистка на самом деле более сложный процесс, поскольку вредоносные программы всячески пытаются препятствовать извлечению. Вот несколько механизмов, используемых вредоносными программами для предотвращения обнаружения и самообороны:

- Блокировка файла

Некоторые вредоносные программы могут заблокировать файл. Если файл заблокирован, он не может быть удален. Блокировка может быть достигнута путем обеспечения постоянной работы программы.

- Watchguards

Это метод, в котором инфекция содержит в себе 2 программы. Если вы очистите одну программу, другая заметит это и запустится немедленно. Когда вы удалите вторую, перезапустится первая, и так далее.

- Скрытие

Как уже упоминалось выше, руткиты манипулируют API, и остаются скрытыми в системе. Если файл не может быть виден, то и не может быть удален, не так ли?

Автозапуск в качестве компонента системы

Некоторые угрозы загружают себя в программы, чтобы операционная система запускала их автоматически, когда вы включаете ваш компьютер. Если вы пытаетесь очистить их, вы получите синий экран. Если вы удаляете пункт автозагрузки, вредоносные программы мгновенно восстанавливают его.

Как Emsisoft очищает угрозы



Чтобы справиться с вредоносными программами, мы разработали собственную систему очистки. Она очищает около 100 мест в реестре и файловой системе, которые могут быть использованы вредоносными программами для запуска при старте системы.

Если файл заблокирован, наше чистящее ядро планирует удаление вредоносной программы при следующей загрузке системы методом, который не позволяет вредоносной программе снова заблокировать удаление. Кроме того, наш движок восстанавливает значения по умолчанию в ряде мест автозапуска, которые испортили бы систему, если бы вы просто удалили записи вредоносной программы. Во время удаления, в карантине создается копия каждой угрозы для последующего анализа или восстановления (если вы не выберете опцию “Удалить” вместо “Карантин”).

Как работает помещение файла в “карантин”? Файл шифруется и помещается в файл-контейнер, где он не может причинить вред другим файлам и приложениям в вашей системе. Мы всегда рекомендуем использовать функцию карантина, потому что существует небольшая вероятность, что файл, который был обнаружен, безвреден (ложное обнаружение), или, что файл может быть необходим для дальнейшего исследования или экспертизы. Вы можете удалить файлы карантина через пару недель, если выясняется, что файл на самом деле безобидный.

Сканирование и очистка файлов на сетевых ресурсах

Хотя сканирование файлов на сетевых ресурсах, которые находятся на других ПК и возможно, мы его не рекомендуем. Это может сэкономить вам немного времени на поездке к физическому компьютеру, но имейте в виду, что сканирование файлов удалённой машины имеет некоторые серьёзные ограничения:

- Сканирование памяти, руткитов и следов невозможно, так как они требуют доступа к системным API, которые могут быть доступны только локально. Вы ограничены в сканировании файлов с помощью стандартных процедур чтения файла, что означает отсутствие режима прямого доступа к диску.
- Очистка вообще невозможна, потому что удаление обнаруженной активной вредоносной программы без удаления его записи в автозапуске, скорее всего, может привести к сбою в работе компьютера, он может перестать загружаться.

Всегда сканируйте и очищайте ПК локально. Если вы не хотите устанавливать наше программное обеспечение, загрузите [Emsisoft Emergency Kit](#), он полностью портативный и не требует установки.

Независимо от того являетесь ли вы экспертом в области удаления вирусов или простым пользователем, мы надеемся, что эта информация поможет вам понять, как работает передовая технология Emsisoft, защищая ваш компьютер от вредоносных программ.

Желаем хорошего и безвирусного дня!