



SpyShelter Firewall

Руководство Пользователя

(Kumga - <http://forum.ru-board.com/>)

SpyShelter Firewall

Оглавление

Введение:

Зачем вам это нужно?.....	3
Установка	4
История программы	5

Использование SpyShelter:

Оповещения	6
Оповещения - режим установки	8
Защита	9
Правила	11
Журнал	19
Ограниченные Приложения	20
Брандмауэр	26
Шифрование Нажатий Клавиш	30
Параметры	34
О Программе	38
Определяемые пользователем защищенные файлы	39
Советы	41

Модули:

Анти-шпион нажатий клавиш	42
Анти-шпион Режим Ядра	43
Анти-GetText	44
Анти-захват экрана	45
Анти-захват Веб-камеры	46
Анти-захват Буфера Обмена	47
Защита Системы	48
Анти-звукозапись	49
Анти-шпион сети	50
Брандмауэр	51
SpyShelter Брандмауэр и Лицензионное соглашение	52



Приступая к работе

У меня уже есть антивирусное программное обеспечение, почему по-прежнему необходим SpyShelter?

SpyShelter предлагает значительно более эффективные методы для защиты вашей конфиденциальности, чем те, которые доступны в традиционной продукции безопасности.

Обычные продукты безопасности чаще ищут вирус только по «отпечаткам пальцев» - вирусным сигнатурам, для устранения угроз и вредоносных программ. Прежде чем они могут быть найдены, эти «отпечатки пальцев» сначала должны быть определены, исследованы в лабораториях. Этот процесс создает опасное окно возможностей для этих угроз потому, что до определения этих отпечатков, они могут незаметно продолжать атаковать компьютеры.

SpyShelter лучше чем другое программное обеспечение безопасности, потому что, вместо того чтобы полагаться на «отпечатки пальцев», она на самом деле понимает как вредоносы работают внутри вашего компьютера, обнаруживает их перед любой атакой и останавливает их до повреждения компьютера.

SpyShelter использует технологию активной защиты, которая является защитным методом, делающим возможным защиту от известных и неизвестных угроз. Она не требует каких-либо баз данных, с целью обнаружения сигнатур вредоносных программ, и способна защитить ваши системы при использовании, только, минимального количества ресурсов вашей системы.

Эта проактивная защита в реальном времени защищает ваш персональный компьютер от недавно созданных и продвинутых угроз. Она мгновенно обнаруживает подозрительную активность в ваших компьютерах и блокирует их прежде, чем будет нанесен какой-либо вред

Почему так важна конфиденциальность?

Новые угрозы и вредоносные программы не нацелены на вашу систему только для развлечения их авторов или просто для краха вашей системы. Многие из этих угроз стремятся получить доступ к личной информации пользователя, такой как пароли, данные кредитной карточки и другим конфиденциальным данным. SpyShelter стремится обеспечить максимальную безопасность для вас.

Установка

SpyShelter имеет стандартный установщик программы.

Системные требования

Для плавного функционирования SpyShelter система должна отвечать следующим аппаратным и программным требованиям:

Минимальные аппаратные требования:

- Intel Pentium 350 MHz или выше (или эквивалент)
- 256 MB доступной оперативной памяти
- 25 MB свободного пространства на жестком диске
- CD-ROM (для установки программы с CD)

Поддерживаемые операционные системы:

- Windows XP 32 bit
- Windows XP 64 bit
- Microsoft Windows Vista 32 bit
- Microsoft Windows Vista 64 bit
- Microsoft Windows 7 32 bit
- Microsoft Windows 7 64 bit
- Microsoft Windows 8 32 bit
- Microsoft Windows 8 64 bit
- Microsoft Windows 8.1 32 bit
- Microsoft Windows 8.1 64 bit

Установка

1. Дважды щелкните файл **fwsetup.exe**.

2. Запустится программа установки. (При установке с компакт-диска: Если мастер не запускается автоматически при вставке компакт-диска, дважды щелкните значок компакт-диска.)

3. После установки программы, значек SpyShelter появится на панели инструментов. Перезагрузите ваш компьютер. После перезапуска можно дважды щелкнуть значек SpyShelter в панели инструментов для доступа к программе.

История программы

10.4 (12/Oct/2015)

- Extended configuration options for AntiNetworkSpy feature
- Fixed rare bug in Firewall WFP driver which caused very high CPU usage

10.3 (25/Sep/2015)

- Firewall network activity monitor now include UDP traffic
- Fixed bug with multiple instances on different accounts
- Fixed issue with account switching on Windows 10
- Decreased number of false alerts on Windows 10
- Added support for Windows 10 Insider Build 10547

10.2.1 (18/Sep/2015)

- Fixed problem with proper digital signatures recognition on some x64 systems

10.2 (18/Sep/2015)

- Added full Keystroke Encryption support for Edge browser
- Fixed numpad digits encryption on some systems with USB keyboards
- Fixed firewall bug with firewall packets filtering
- Improved protection on Windows 10
- Added support for Windows 10 Insider Preview build 10532
- Fixed problem with disabling shell context menu integration
- Fixed the update-installer on Windows 10

10.1 (28/Aug/2015)

- SpyShelter Free Anti-Keylogger now supports 64bit systems*
- Free version offers now limited keystroke encryption feature
- Fixed a crash that occurred in Network List
- Fixed a freeze problem in Windows 10
- Added early support for Windows 10 build 10520
- Other small improvements and fixes

*To learn more about the differences between Free and Paid editions, visit our [Download page](#).

10.0 (29/Jul/2015)

- Added support for Windows 10 system
- Small visual changes

9.9.1 (21/May/2015)

- Added support for East Asian languages to Keystroke encryption driver
- Fixed context menu handler bug when program starts from service
- Added French version of User's Manual
- Few small improvements
- Self defence improvements

9.7.2 (17/Mar/2015)

- Fixed security issue with password protection of GUI access
- Farsi installer language update

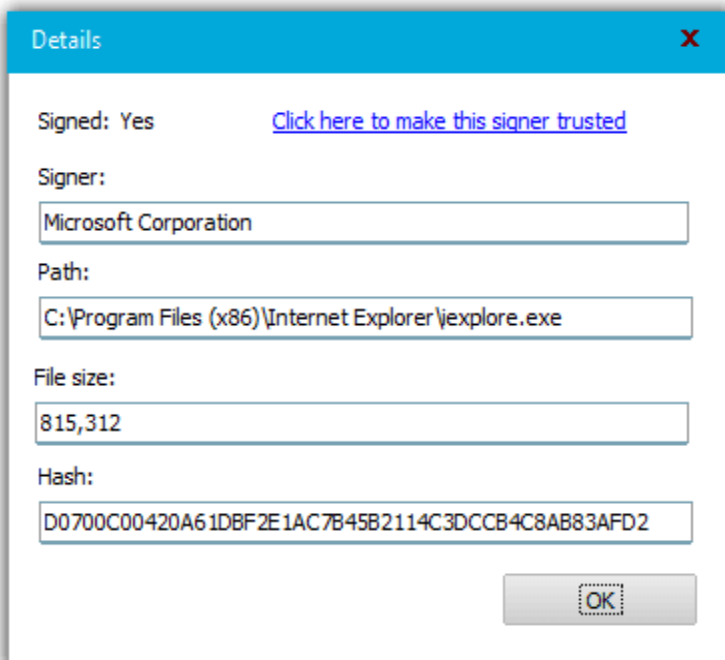
9.7.1 (13/Mar/2015)

- Fixed issue with process removing in KED
- Installer and general language updates
- Minor fixes

Оповещения

После обнаружения любой подозрительной активности, SpyShelter будет показывать это> окно предупреждения, которое содержит сведения о том, что происходит в системе.

После нажатия на «детали компонента», появится окно, подобное показанному ниже:



Подписано:

Возможные варианты Да или Нет.

Это означает, что приложение подписано цифровой подписью издателя. Обычно, подписанным приложениям можно доверять.

Подписи:

Содержит название компании [или имя подписавшего]. Вы можете, затем, проверить историю этой компании и узнать больше о типе их программного обеспечения.

Путь:

Путь к файлу

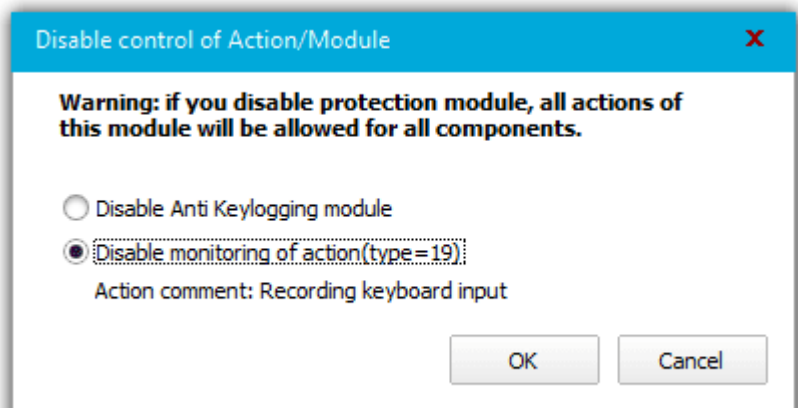
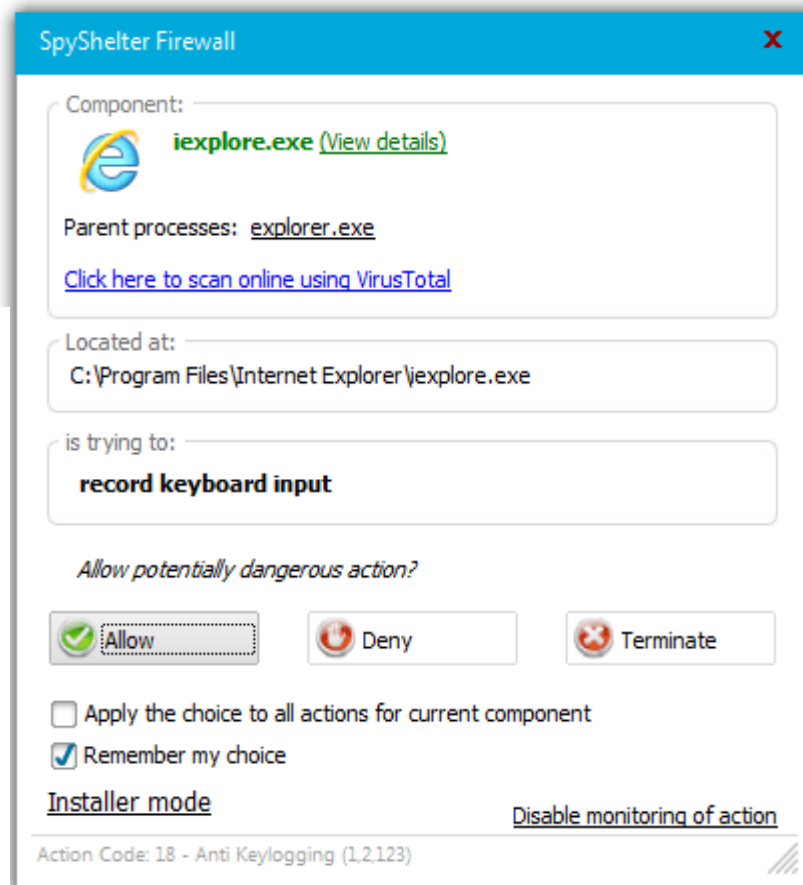
Размер файла:

Показывает размер файла в байтах.

Хэш:

Серия символов, которая определяет работающую программу.

Если вы нажмете на «отключить мониторинг», вы увидите следующее окно:



Здесь вы можете выбрать для отключения соответствующий модуль или отключить мониторинг текущего действия.

Если вы решите **отключить модуль**, все действия, контролируемые этим модулем, будут разрешены для всех компонентов, в то время как, если вы решите **отключить мониторинг действий**, тогда не будет отслеживаться конкретный тип действий.

В главном окне, также, у вас есть другие параметры:

Проверка Компонента на вирусы на www.virustotal.com

Проверка подозрительного файла антивирусами на VirusTotal - проверяется файл несколькими антивирусами на веб-сайте VirusTotal.com.

Примечание: Отрицательный результат (0 найденных вирусов) не всегда означает, что файл является законным и не содержит вредоносного кода.

Помните также, что многие антивирусные сканеры часто выдают ложные срабатывания, особенно, на защищенный/сжатый код. Для получения дополнительной информации обращайтесь на VirusTotal.com

Применить выбор ко всем действиям текущего модуля:

Когда этот параметр выбран, SpyShelter будет применять ваш выбор на другие действия для текущего модуля (он будет разрешать или блокировать все виды деятельности, в зависимости от вашего выбора).

Запомнить мой выбор:

Когда этот параметр выбран, создается правило в закладке «**Правила**» и сохраняется в программе. Таким образом, в следующий раз, при запуске SpyShelter, программа будет автоматически принимать решения на основе сохраненного правила.

У вас также есть возможность ввода Installer mode — режима инсталляции (Смотрите соответствующий раздел).

Пожалуйста, имейте в виду, что SpyShelter иногда подскажет вам, даже, в отношении традиционно «безопасной» программы. Это связано с многими параметрами программы, как глобальный hook . Поэтому рекомендуется, чтобы вы читали всю информацию о личности подписавшего и путь, где приложение должно быть установлено.

Например, если появляется окно с сообщением о действии приложения, которому вы доверяете, то не нужно беспокоиться и его соответствующее действие может быть разрешено.

Когда вы не уверены, какие меры следует принять, обычно рекомендуется первоначально блокировать программу. Если ваша система остается стабильной, даже тогда, когда программа запущена, можно удалить это приложение из черного/белого списка и разрешить его запуск.

Как правило, подписанные программы являются безопасными. Однако, для дополнительной защиты, вы можете проверить имя подписавшего, чтобы увидеть, какой тип программного обеспечения эта компания производит и вы, также, можете проверить путь установки.

Рядом с «**Разрешить**» или «**Запретить**» действие у вас есть также возможность «**Прекратить**» процесс.

Примечание: Когда система завершает процесс, она не прекращает любые дочерние процессы, которые процесс создал.

ПРИМЕЧАНИЕ:

После того, как процесс завершается, создается правило и сохраняется в списке правил. Таким образом, в следующий раз, когда этот процесс будет пытаться запуститься, он будет автоматически прекращен.

В зависимости от параметра:

"Применить выбор ко всем действиям текущего модуля"

Будет прекращено одно указанное действие или все подозрительные действия.

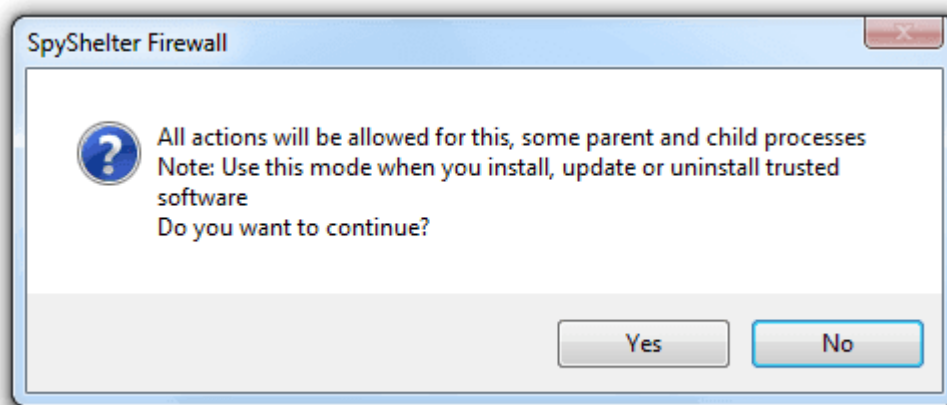
Оповещения - режим установки

Установщику приложения и обновления программного обеспечения может потребоваться авто-разрешение иметь возможность исполнить другие процессы (так называемые 'Дочерние процессы') для того, чтобы уменьшить количество ложных срабатываний.

Режим установки SpyShelter сделает процесс установки новых приложений проще.

При попытке установить новое приложение, SpyShelter будет пытаться обнаружить **режим установки** и покажет надпись **режим установки** полужирным шрифтом в нижней части окна, которое появится.

Нажатие на "режим установки" будет вызывать оповещение подтверждения, как показано ниже:



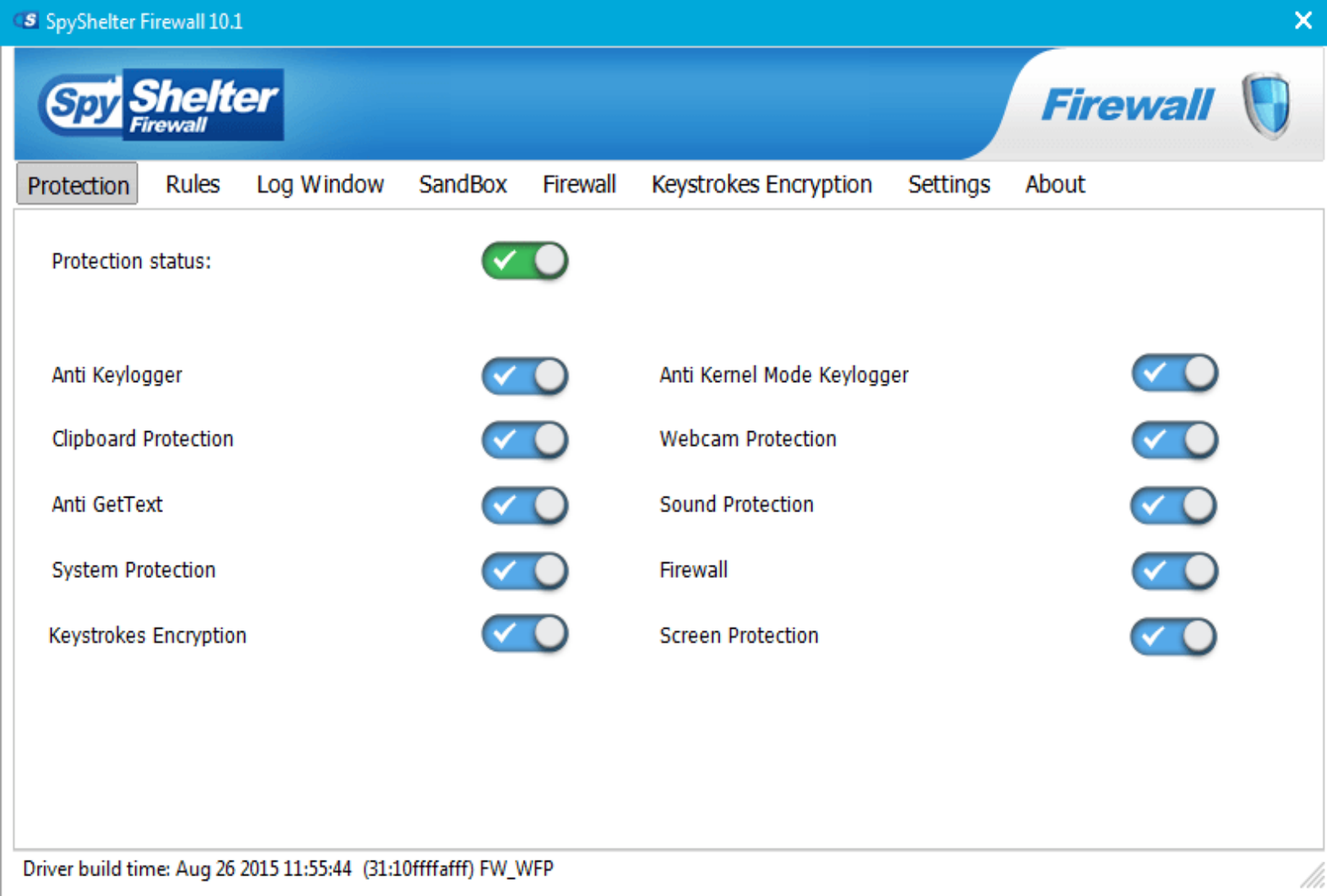
Выберите Да, чтобы разрешить выполнение дочерних процессов с теми же правами, что и родительский процесс




Вкладка Защита

SpyShelter имеет удобный интерфейс и очень прост в использовании. SpyShelter содержит множество различных модулей, предназначенных для защиты вашего компьютера от вредоносного программного обеспечения и предоставляет ему полную защиту от угроз и атак. Эти модули защищают вашу информацию и личные данные от незаконной и вредоносной атаки.

Пользовательский интерфейс программы состоит из нескольких разделов. Первым из них является **Вкладка Защита**:



Здесь вы можете начать или остановить общую защиту для всех модулей, а также включить или отключить модули безопасности. Чтобы сделать это, нужно просто нажать на маленький значок с шариком справа от имени модуля.

Этот  индикатор показывает Выкл/Вкл общей защиты для всех модулей, (вы можете нажать на индикатор).

Если вы хотите просто временно отключить защиту, пожалуйста, следуйте инструкциям в окне, которое появится (вы можете увидеть это ниже).



Примечание:

При отключении защиты на вашей машине, вредоносные программы, которые были заблокированы, могут, затем, заразить вашу систему и могут быть заблокированы вновь, только, при повторном запуске SpyShelter.

Рекомендуется перезагружать систему для того, чтобы обеспечить полную защиту приложения, когда есть запрос сделать это.



SpyShelter защита состоит из нескольких модулей, которые выполняют различные функции:

Клавиатурный Анти-шпион:

Защищает вашу систему от клавиатурных шпионов.

Анти-захват экрана:

Защищает вашу систему от захвата экрана.

Анти-захват буфера обмена:

Защищает вашу систему от захвата буфера обмена.

Анти-GetText:

Защищает вашу систему от захвата текста с помощью функции gettext.

Защита системы:

Защищает чувствительные области вашей системы от вредоносных приложений.

Анти-захват в Режиме Ядра:

Защищает систему от передовых кейлоггеров режима ядра.

Анти-захват веб-камеры:

Защищает вашу систему от захвата Web-камеры.

Анти-звукозапись:

Защищает вашу систему от голосовых регистраторов VOIP, например, при использовании сегодняшних интернет-мессенджеров.

Анти-шпион сети:

Защищает вашу систему от захвата SSL и HTTP/HTTPS/POP/SMTP/FTP.

Примечание:

Есть некоторые различия в 32 и 64-разрядных выпусках SpyShelter для Windows. 64 битное издание имеет встроенную защиту системы под названием patchguard, которая позволяет эти выпуски для работы с незначительной внешней защитой. Однако, SpyShelter по-прежнему обеспечивает очень важную расширенную защиту для 64 битных систем.

Вкладка «Правила»

Общие

Вкладка Общие отображает все правила, созданные в ответ на оповещения системы безопасности. Она содержит информацию о допущенных и не допущенных компонентах, которые были обнаружены SpyShelter, из-за своего подозрительного поведения.

Allow	ActionT...	Component na...	Component path	Hash	Protection Module	Date
✓	50	chrome.exe	C:\Program Files (x86)\Google\Chrome...	48...	Firewall	2015-08-26 14:21
✓	7	chrome.exe	C:\Program Files (x86)\Google\Chrome...	48...	Anti Keylogging	2015-08-26 14:21
✓	48	chrome.exe	C:\Program Files (x86)\Google\Chrome...	48...	Firewall	2015-08-26 14:21
a	51	chrome.exe	C:\Program Files (x86)\Google\Chrome...	48...	System Protection	2015-08-26 15:02
a	47	chrome.exe	C:\Program Files (x86)\Google\Chrome...	48...	System Protection	2015-08-26 15:13
a	31	chrome.exe	C:\Program Files (x86)\Google\Chrome...	48...	Webcam Protec...	2015-08-26 15:14
✓	24	dllhost.exe	C:\Windows\System32\dllhost.exe	00...	Clipboard Prote...	2015-08-26 14:16
✓	All actio...	explorer.exe	C:\Windows\explorer.exe	00...	All modules	2015-08-26 14:20
a	50	GWXUX.exe	C:\Windows\System32\GWX\GWXUX.exe	00...	Firewall	2015-08-26 18:12
a	48	GWXUX.exe	C:\Windows\System32\GWX\GWXUX.exe	00...	Firewall	2015-08-26 18:12
✓	50	iexplore.exe	C:\Program Files\Internet Explorer\iexp...	D0...	Firewall	2015-08-26 14:15
✓	26	iexplore.exe	C:\Program Files\Internet Explorer\iexp...	D0...	System Protection	2015-08-26 14:15
✓	51	iexplore.exe	C:\Program Files (x86)\Internet Explore...	D0...	System Protection	2015-08-26 14:16
✓	50	iexplore.exe	C:\Program Files (x86)\Internet Explore...	D0...	Firewall	2015-08-26 14:16

Search...

Driver build time: Aug 26 2015 11:55:44 (31:10ffffafff) FW_WFP

В верхней части этой вкладки вы можете увидеть серию иконок. Каждая из них выполняет определенные действия. В порядке слева направо:

Создать пользовательские правила:

Это позволяет создать полностью настраиваемые правила для любого файла. Просто выберите путь к файлу (компонент) и определите, какие действия вы хотите разрешить или запретить.

Component path:

Custom network rule:

Incoming network traffic: ☐ Default ☐ Custom

Outgoing network traffic: ☐ Default ☐ Custom

All general actions: ☐ Custom

Execution of an application: ☐ Default

Recording keyboard input: ☐ Default

Screenshots: ☐ Default

Global Hooks: ☐ Default

Modifying protected registry keys: ☐ Default

Clipboard monitoring: ☐ Default

Accessing to webcam: ☐ Default

Accessing to sound record device: ☐ Default

Getting text of other process window: ☐ Default

Changing properties of other process window: ☐ Default

Modifying protected files or folders: ☐ Default

Modifying memory of other processes: ☐ Default

Reading memory of protected processes: ☐ Default

Harddisk write access: ☐ Default

Physical memory access: ☐ Default

Inter-process communication: ☐ Default

Accessing to DNS Resolver network service: ☐ Default

Accessing to the system debugger: ☐ Default

Loading drivers: ☐ Default

Registering service or driver: ☐ Default

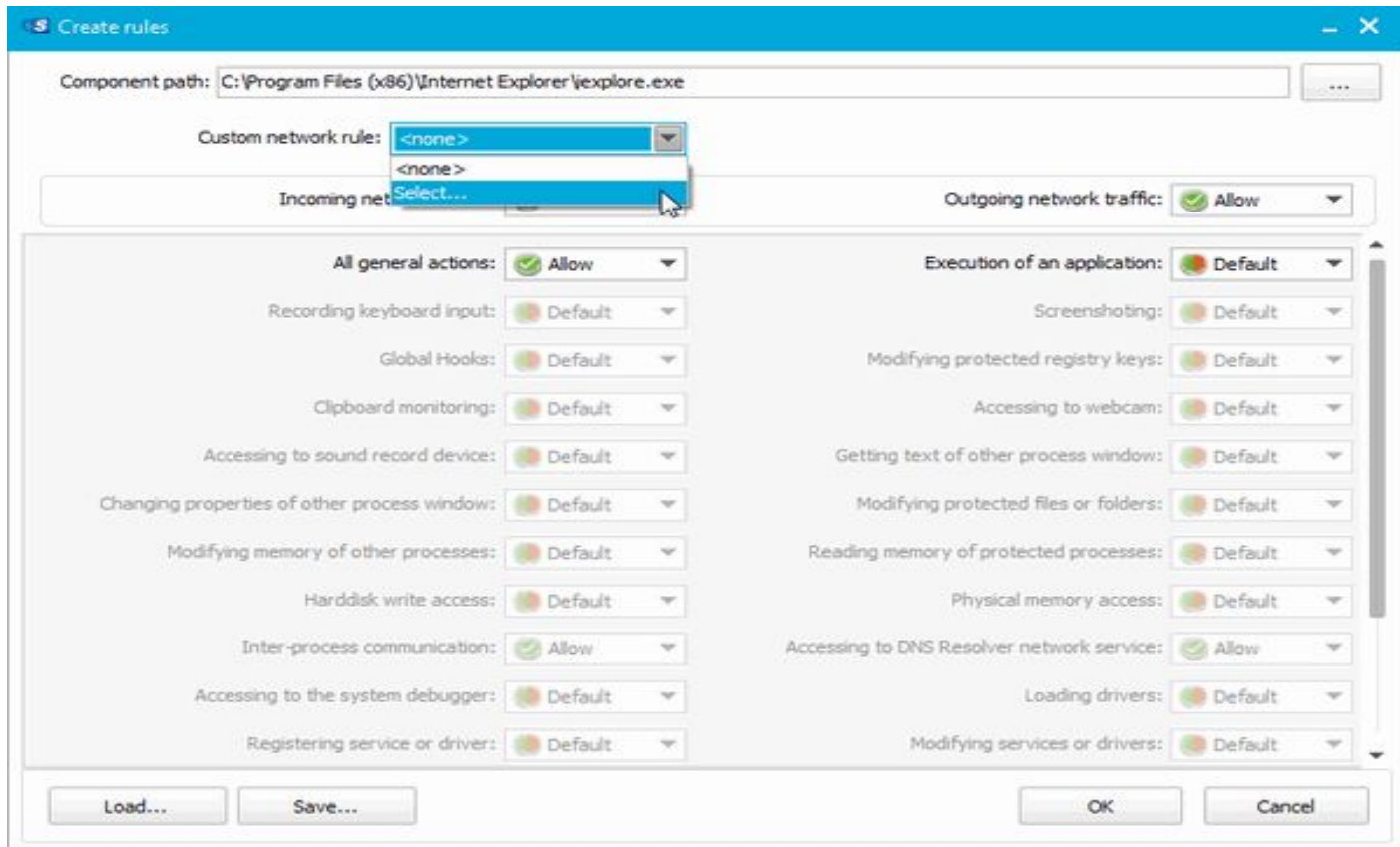
Modifying services or drivers: ☐ Default

Load... Save... OK Cancel

Пользовательское Сетевое Правило:

Эта функция позволяет определить расширенные сетевые параметры для компонента.

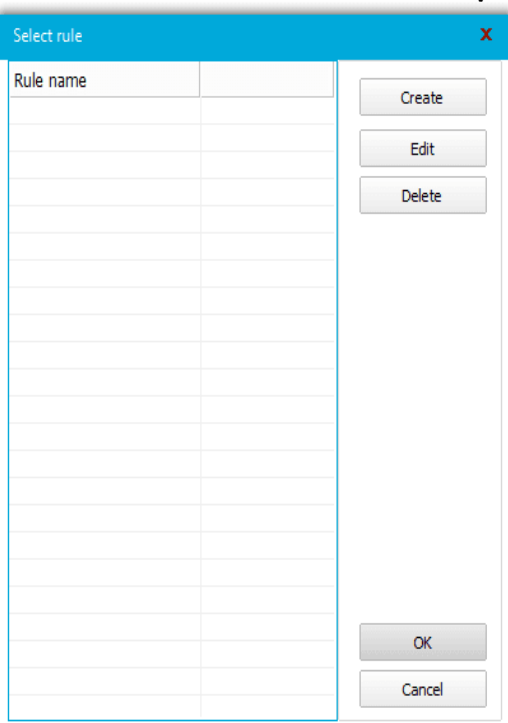
Для того, чтобы создать новое сетевое правило, выберите путь компонента (файла), щелкните на раскрывающемся списке «**Пользовательское сетевое правило**» и выберите команду **выбрать**.



Откроется новое окно, которое позволит вам управлять пользовательскими правилами пресетов. Нажмите на **Создать**, чтобы создать новое. Вы также можете редактировать существующее правило, выбрав его и нажав на кнопку **Изменить**.

▼

Общие>



Имя правила:

Можно задать любое имя для правила.

Тип правила:

Выберите, если вы хотите разрешить или запретить сетевой трафик в этом правиле.

Протокол:

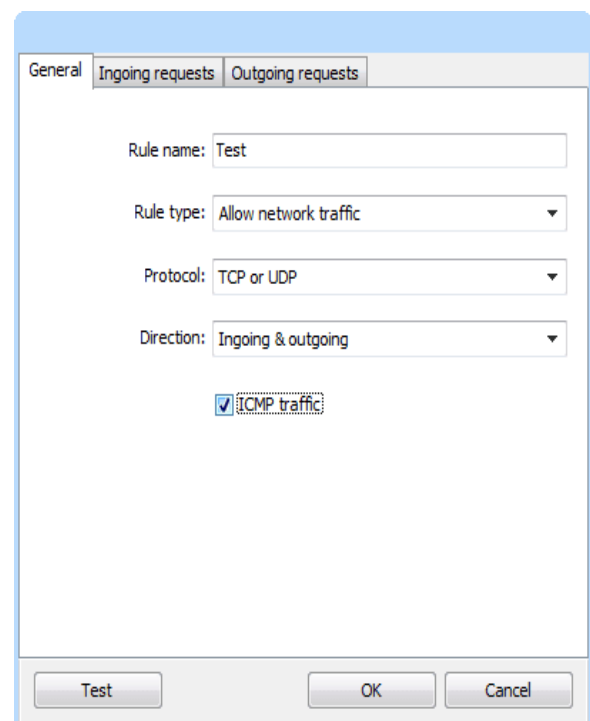
Выберите, какой протокол следует использовать.

Направление:



Выберите, если вы хотите создать правило для входящих, исходящих или для обоих направлений движения.

ICMP Трафик:

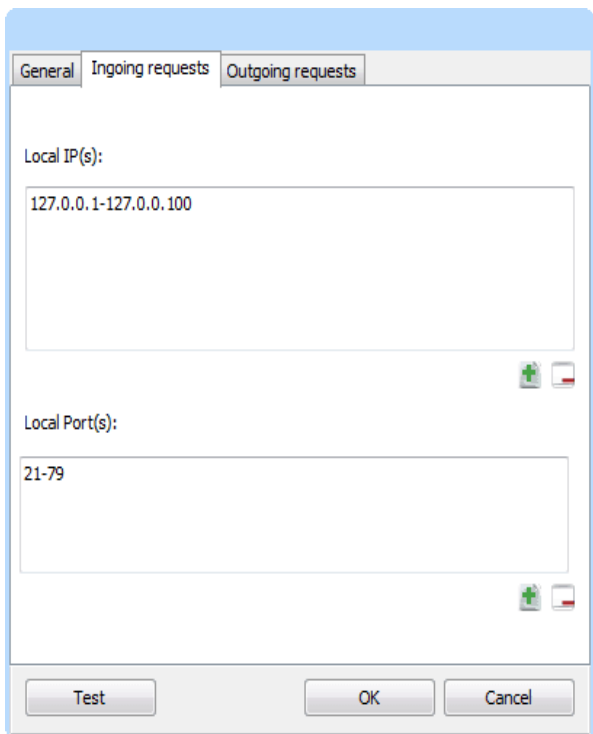
Отметьте это, если вы хотите применить правило к ICMP-трафику.




Входящие запросы

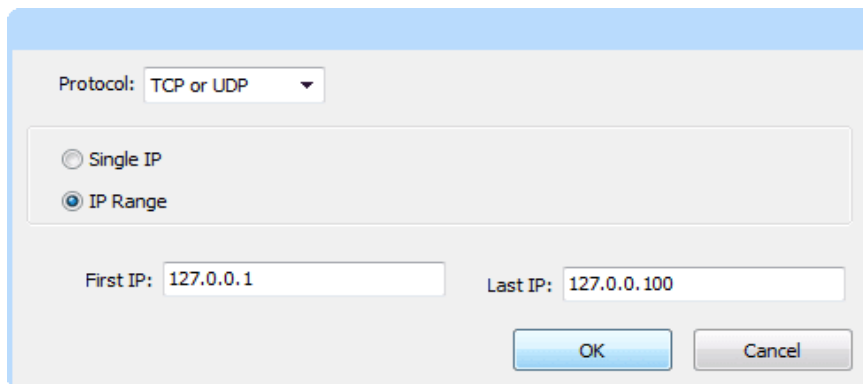
Предоставляет список IP-адресов и портов для всех входящих запросов, которые вы хотите фильтровать. Нажмите  значок, чтобы добавить новые адреса и , чтобы удалить один из существующих.

▼

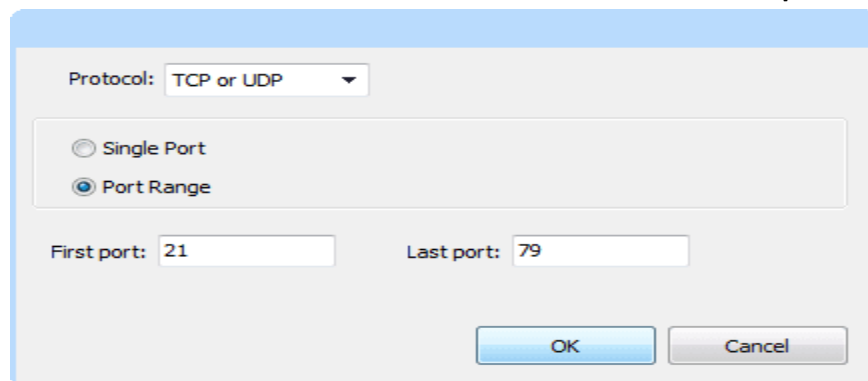


После того, как вы щелкните , откроется новое окно. Выберите протокол, один IP-адрес или диапазон IP-адресов и введите IP-номер(а).



▼



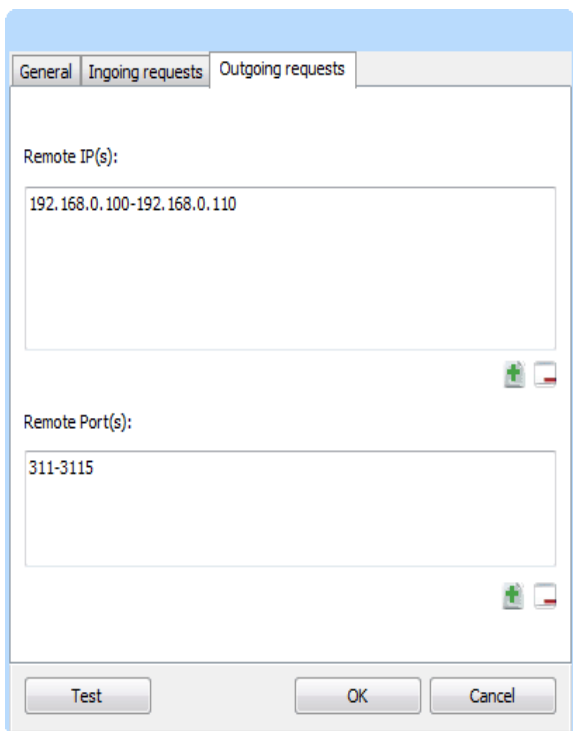
Настройка выполняется точно так же и для портов. ▼




Исходящие запросы

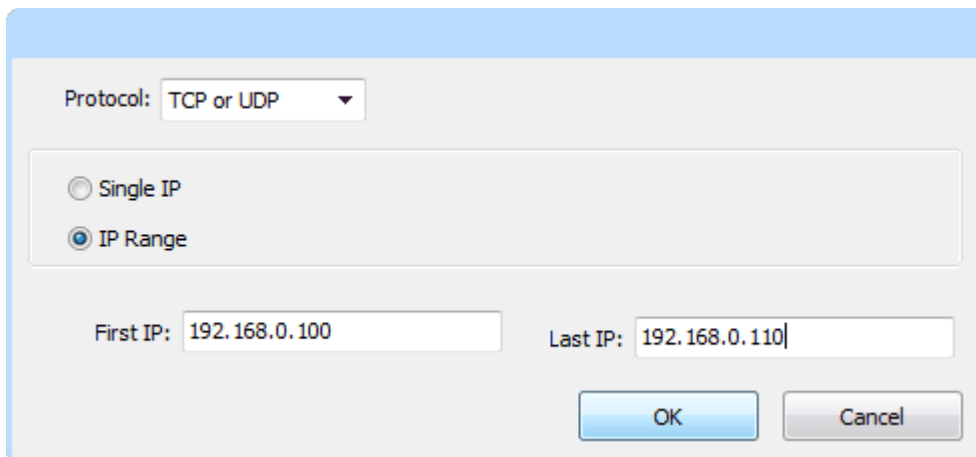
Предоставляет список IP-адресов и портов для всех исходящих запросов, которые вы хотите фильтровать. Нажмите  значок, чтобы добавить новый адрес и , чтобы удалить существующий.

▼



После нажатия кнопки , появится новое окно. Выберите протокол, один IP-адрес или диапазон IP-адресов и введите номер(а) IP.

▼



Настройка выполняется точно так же и для портов. ▾

Protocol: TCP or UDP ▾

☐ Single Port

☒ Port Range

First port: 3111 Last port: 3115

OK Cancel

Можно, также, выполнить **тест** вашего вновь созданного правила, нажав на кнопку тест. (см. на странице выше)

Выберите протокол, направление, введите IP и порт и нажмите кнопку **Тест**, чтобы увидеть, будет ли соединение заблокировано.

Редактор правил: Эта опция позволяет вам редактировать правила выбранного компонента.

Custom network rule: <none> ▾

Incoming network traffic: Default ▾ Outgoing network traffic: Allow ▾

All general actions: Custom ▾

Recording keyboard input: Default ▾

Global Hooks: Default ▾

Clipboard monitoring: Default ▾

Accessing to sound record device: Allow ▾

Changing properties of other process window: Default ▾

Modifying memory of other processes: Default ▾

Harddisk write access: Default ▾

Inter-process communication: Allow ▾

Accessing to the system debugger: Default ▾

Registering service or driver: Default ▾

Accessing to Raw Socket: Default ▾

Shutdown the system: Default ▾

Execution of an application: Default ▾

Screenshots: Default ▾

Modifying protected registry keys: Default ▾

Accessing to webcam: Default ▾

Getting text of other process window: Default ▾

Modifying protected files or folders: Default ▾

Reading memory of protected processes: Default ▾

Physical memory access: Default ▾

Accessing to DNS Resolver network service: Allow ▾

Loading drivers: Default ▾

Modifying services or drivers: Default ▾

Blocking keyboard input: Default ▾

Creating alternate data streams: Default ▾

Load... Save... OK Cancel

Сохранение правил:

После того, как вы настроите правила, у вас есть возможность сохранить их как шаблон, нажав на кнопку «Сохранить...» в нижнем левом углу окна. (см. выше)

Creating a rule template

New template name: test rule

OK Cancel

Загрузка правил:

Вы можете загрузить сохраненный шаблон правила, нажав кнопку "ЗАГРУЗИТЬ ...", расположенную в левом нижнем углу окна (см. выше). Выберите сохраненный шаблон правила и нажмите ОК. Загруженное правило перезапишет существующее правило. >

Импорт правил из файла:

Если у вас уже есть ряд правил, сохраненных в файл, вы можете импортировать их в приложение, без необходимости устанавливать правила по одному.

Экспорт выбранного правил(а) в файл:

Вы можете выбрать одно или несколько действий (если вы будете держать клавишу Ctrl во время нажатия на компоненты, вы сможете выбрать более одного) и экспортировать их в файл.

Экспортировать все правила в файл:

Это позволяет экспортировать все установленные правила в файл. Этот параметр может быть полезен, когда, например, вы хотите сделать резервную копию ваших правил.

Удалить правила:

Вы можете удалить одно или несколько правил из вашего списка. Если вы хотите удалить более чем одно правило за раз, нажмите клавишу Ctrl, выбирая элементы, которые вы хотите удалить.

Удалить все правила:

При выборе этого действия удалятся все правила, которые были ранее установлены.

Очистить правила:

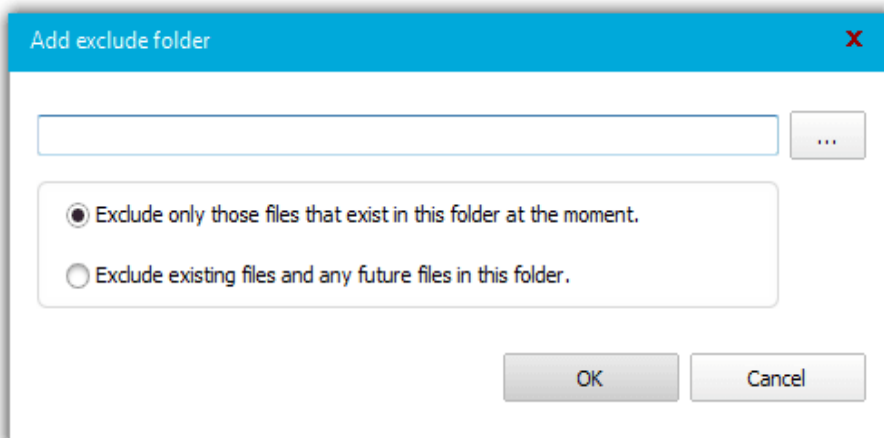
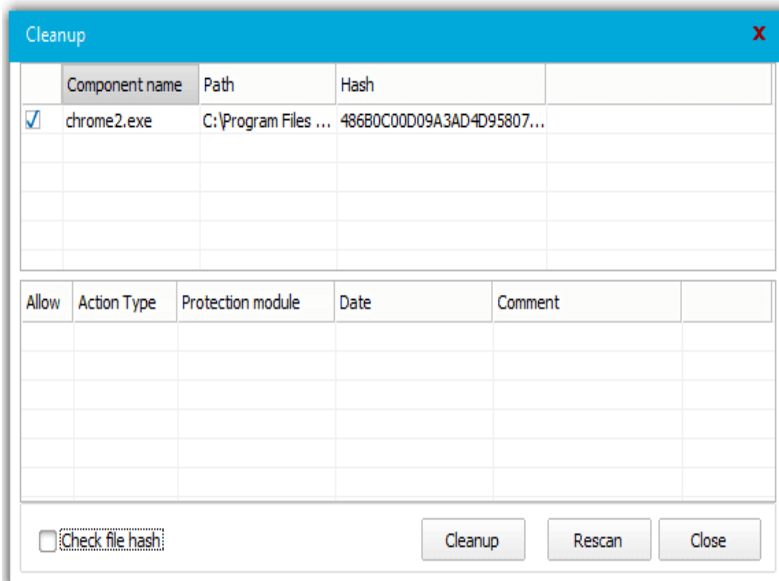
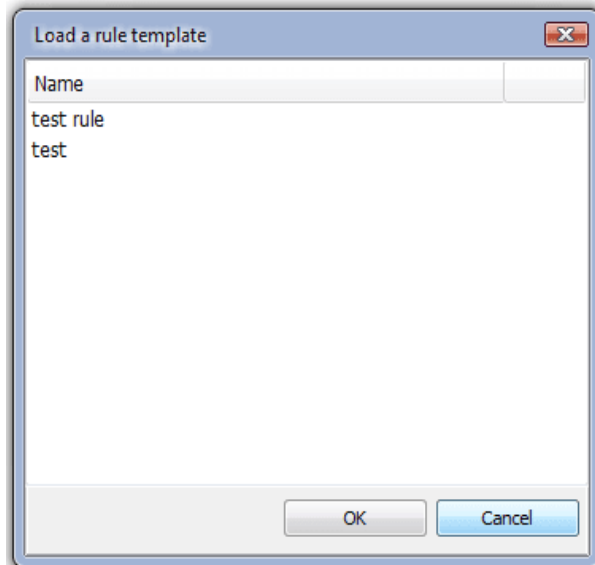
Если после добавления папки в список, вы будете удалять эту папку с жесткого диска, эта опция дает вам возможность очистить все правила, которые по-прежнему могут относиться к удаленной папке, потому что они больше не нужны.

Добавить файл в исключения:

Если есть некоторые файлы, которые вы хотите исключить (что означает, что вы не хотите, чтобы он блокировался), вы можете добавить их в список исключений. Таким образом, все действия для этих файлов будут разрешены.

Добавить папку в исключения:

Это действие является таким же, как предыдущее, но в этом случае, можно добавить целую папку в список исключений с двумя вариантами.



Исключить только те файлы, которые существуют на данный момент в этой папке- Эта опция будет исключать все файлы, присутствующие в папке при создании этого правила. Это означает, что если вы создадите/переместите новые файлы в эту папку после ее исключения, эти файлы не будут исключены. Это самый безопасный выбор.

Исключить существующие файлы и любые будущие файлы в этой папке - Эта опция будет исключать все существующие, в настоящее время, файлы в папке, а также все будущие файлы. Это менее безопасно, чем первый вариант; Однако, это может быть полезно для пользователей, которые часто изменяют файлы.

Примечание: Файл, который был отредактирован рассматривается как новый файл.

Найти все правила компонента:

Эта функция покажет вам все правила, созданные для выбранного, в настоящее время, компонента.

Проверить файл на VirusTotal.com:

Эта функция позволяет сканировать онлайн, в настоящее время выбранный компонент, более чем 40 различными антивирусами.

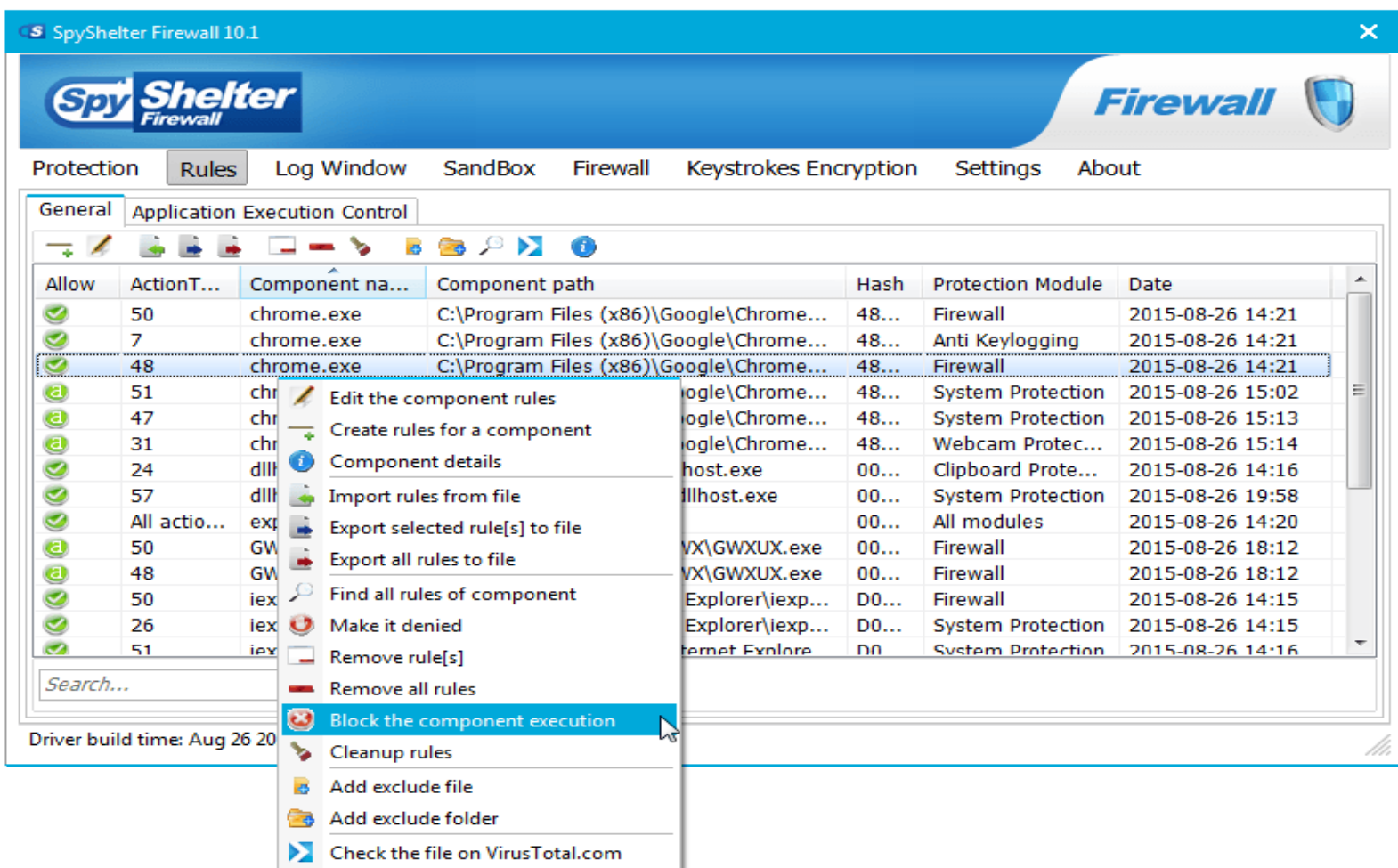
Детали компонентов:

Это действие позволяет увидеть детали выбранного элемента, в том числе подписано приложение или нет, подписавшее лицо (если таковое имеется), путь к файлу, размер файла и хэш файла.

Блокировать выполнение компонента:

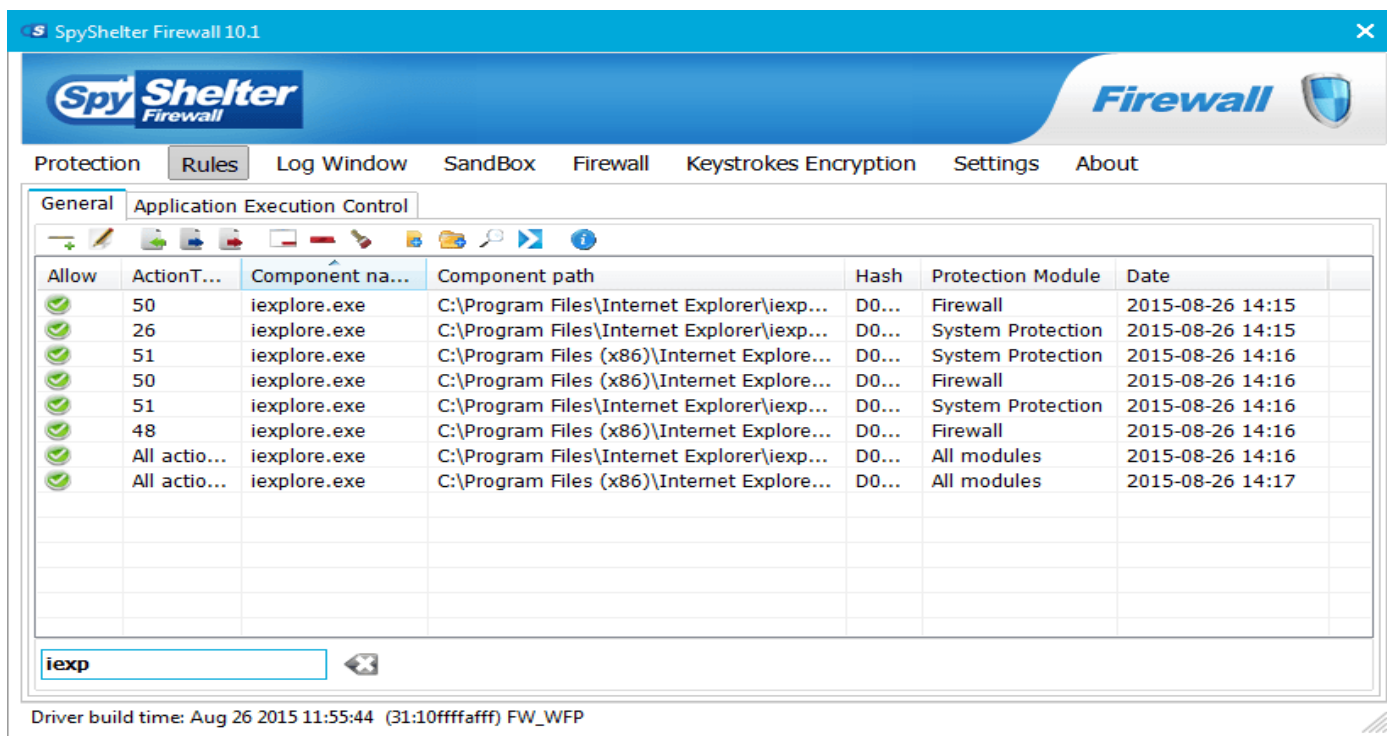
Позволяет полностью блокировать выполнение компонента.

Щелкнув правой кнопкой мыши на строке, вы вызовете меню, содержащее все эти действия, как вы можете видеть на скриншоте ниже:



Панель поиска:

Это поле позволяет вам фильтровать правила для того, чтобы найти конкретную запись. Вы можете искать путь и имя компонента.



При нажатии на элемент в списке, в нижней части окна, вы увидите комментарий, который будет объяснять, какие действия выбранный компонент пытается совершить.

Пример

Имя компонента: example.exe

Разрешить: Да означает, что вы позволили **Тип Действия:** номер типа действия для example.exe. Вы также можете увидеть путь к example .exe, а также **модуль защиты**, контролирующий действие компонента.

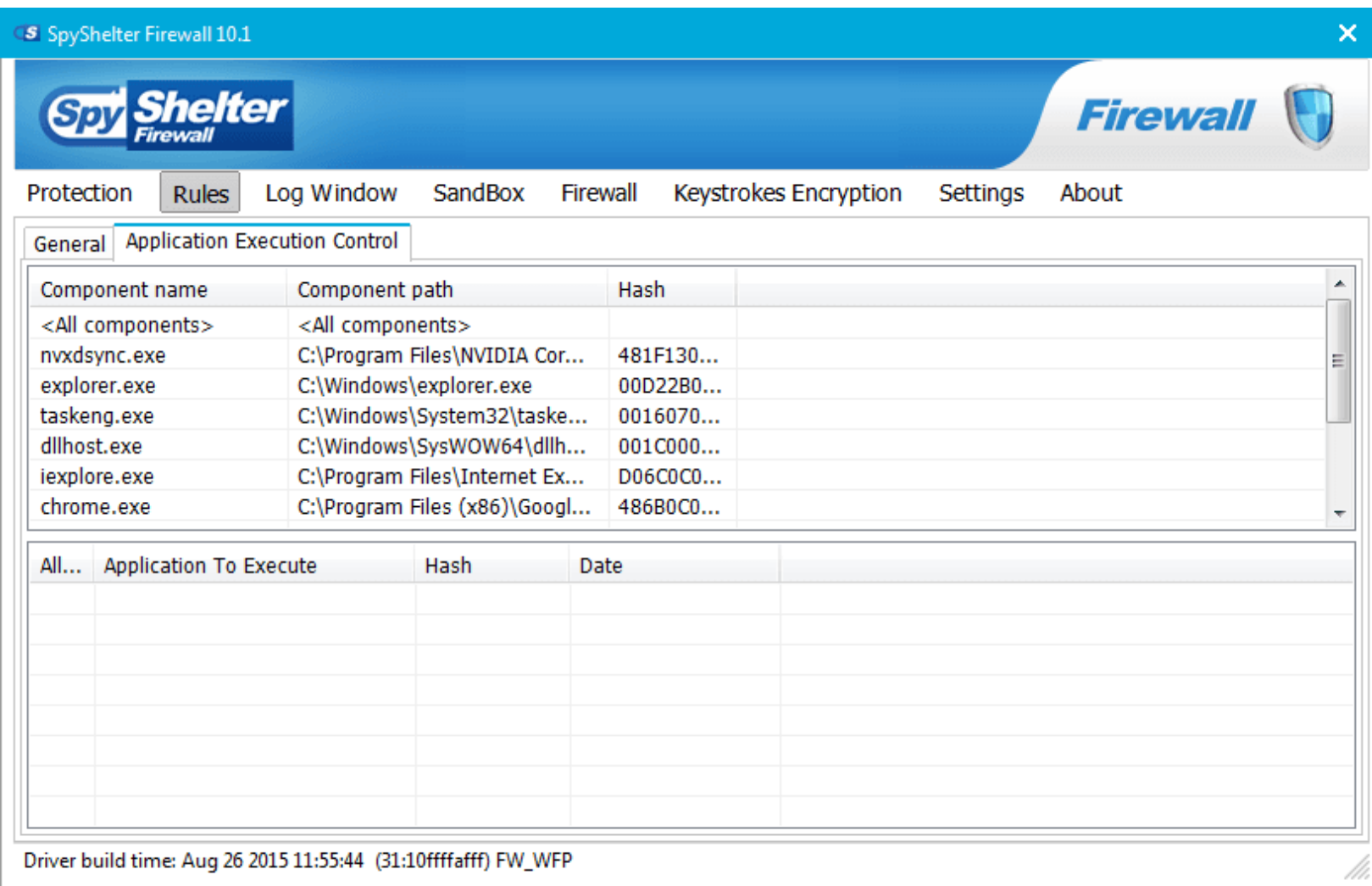
После удаления элемента из списка в рамках программы, будет автоматически проанализирован код после того, как вновь обнаружится этот компонент, и будет задан вам вопрос, хотите ли вы разрешить или запретить его работу в вашей системе.

Значки столбца Разрешить

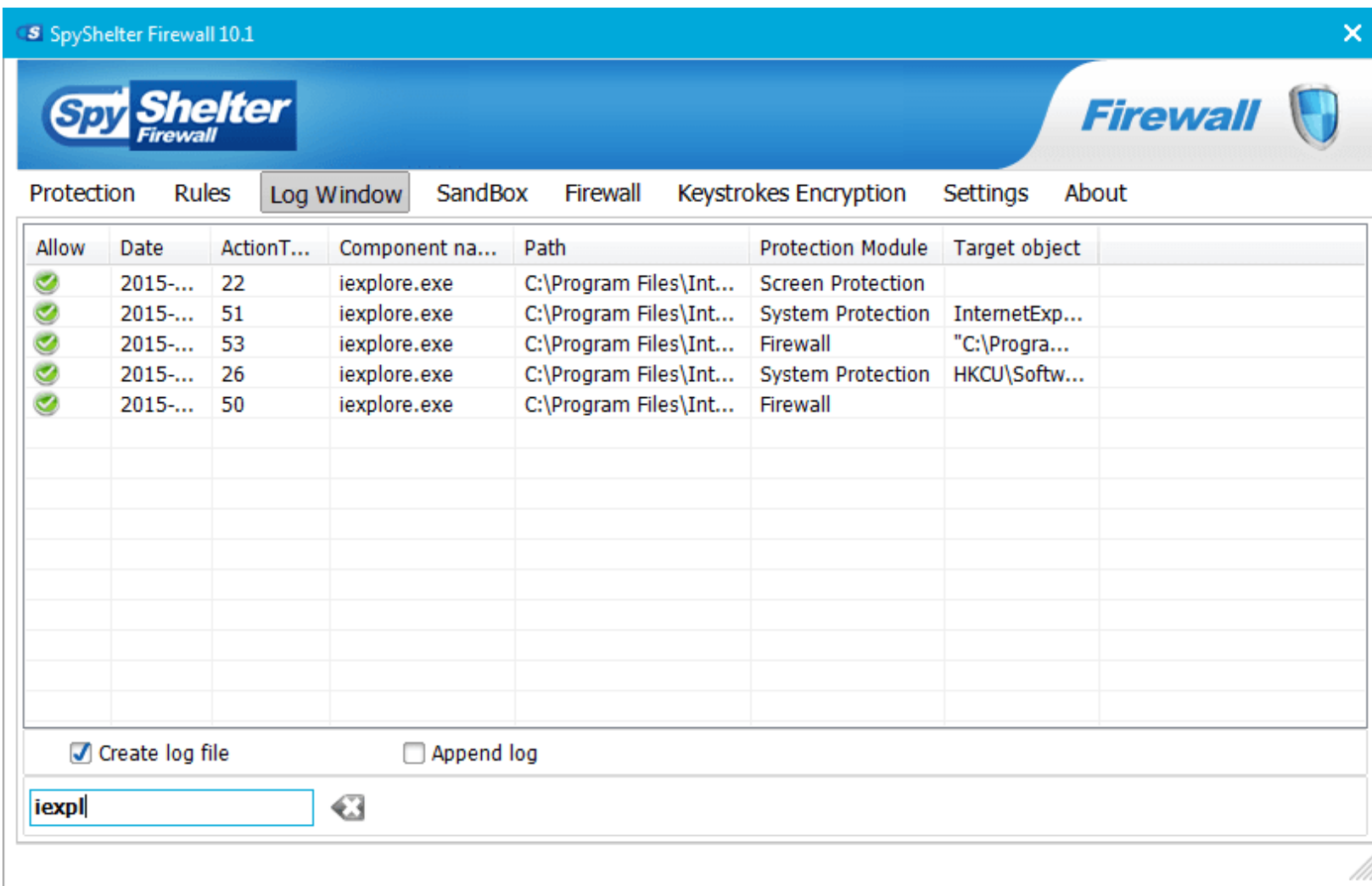
- ✓ Правило позволяет действие и было создано вручную пользователем в строке.
- а Правило позволяет действие и было автоматически создано на основе параметров безопасности
- ⛔ Правило блокирует действие и было создано вручную пользователем в строке.

Контроль выполнения приложения

Эта вкладка содержит правила, на основании которых SpyShelter принимает решение заблокировать или разрешить выполнение приложения. Верхняя часть содержит список родительских приложений процесса. Нижняя часть содержит список правил дочернего процесса для выбранного приложения (процесса) в верхней части. (см. ниже)



Вкладка Журнал



Здесь вы можете увидеть всю историю действий и приказов к тому времени, когда это произошло. Все записи хранятся только одну сессию приложения. Если вам нужно иметь полный журнал деятельности, вы должны использовать вариант, изложенный ниже.

Добавить журнал:

Когда этот флажок установлен, SpyShelter сохраняет лог файл. Можно просмотреть его позже, щелкнув правой кнопкой мыши на запись и выбрав **Просмотр файла журнала**.

Когда вы щелкните правой кнопкой мыши на элемент, вам будет предложено два варианта:

Просмотр файла журнала:

Этот параметр позволяет просмотреть файл журнала последней сессии программы.

Удаление журнала:

Эта опция сотрет все пункты, перечисленные в настоящее время, **и весь файл** журнала из последней сессии программы.

Панель поиска:

Это поле позволяет фильтрацию файла журнала для того, чтобы найти конкретную запись. Вы можете искать путь и имя компонента

При нажатии на элемент в списке, в нижней части окна, вы увидите комментарий, который будет объяснять, какие действия выбранный компонент пытался предпринять

Вкладка "Песочница — Ограниченные Приложения"

Песочница SpyShelter (Ограничение Приложений) использует ограничение SID и hooks для того, чтобы защитить ваш ПК. Это позволяет вам выбрать приложения, которые вы хотите запустить с более низким уровнем привилегий. Приложения, выполняющиеся в ограниченном режиме имеют ограниченный доступ к системным ресурсам, например, ключам реестра, файлам, веб-камере, микрофону, клавиатуре, установке hooks, обычным административным задачам (например, остановка, регистрация, службы и драйверы) и так далее.

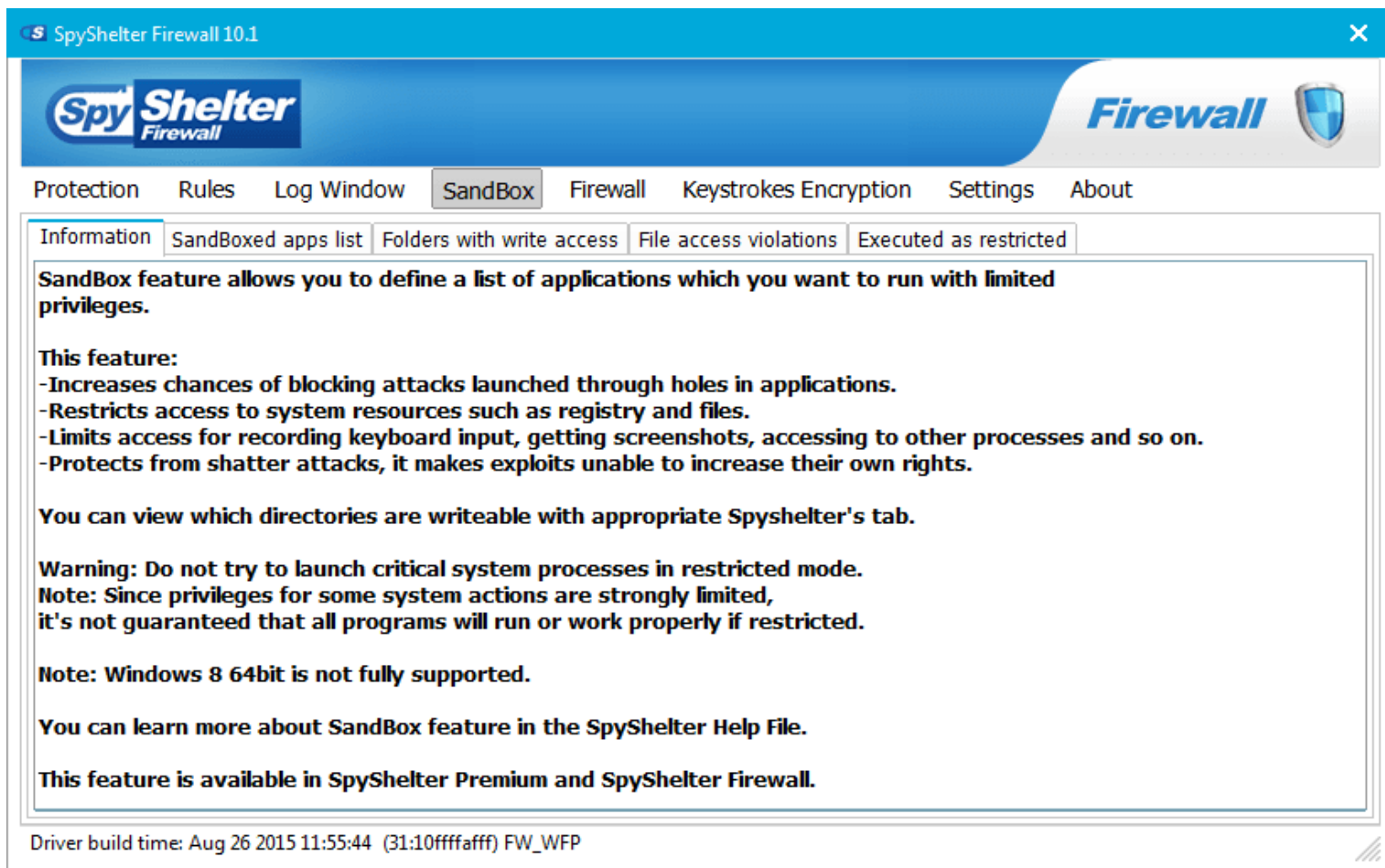
Другие ограничения для приложений, выполняющихся в ограниченном режиме:

- 1) Нет записи в куст реестра HKLM (доступ к другим разделам реестра может быть также ограничен).
- 2) Ограниченный доступ к файлам (как вы можете видеть на соответствующей вкладке SpyShelter).
- 3) Ограничения на другие системные объекты (на основе параметров системы безопасности).
- 4) Все опасные действия блокируются автоматически для приложений, выполняющихся в ограниченном режиме.
- 5) Дочерние процессы ограниченных процессов также ограничены.

Этот режим может быть использован для запуска веб-браузера, почтовых клиентов, мгновенных сообщений или любых неизвестных программ.

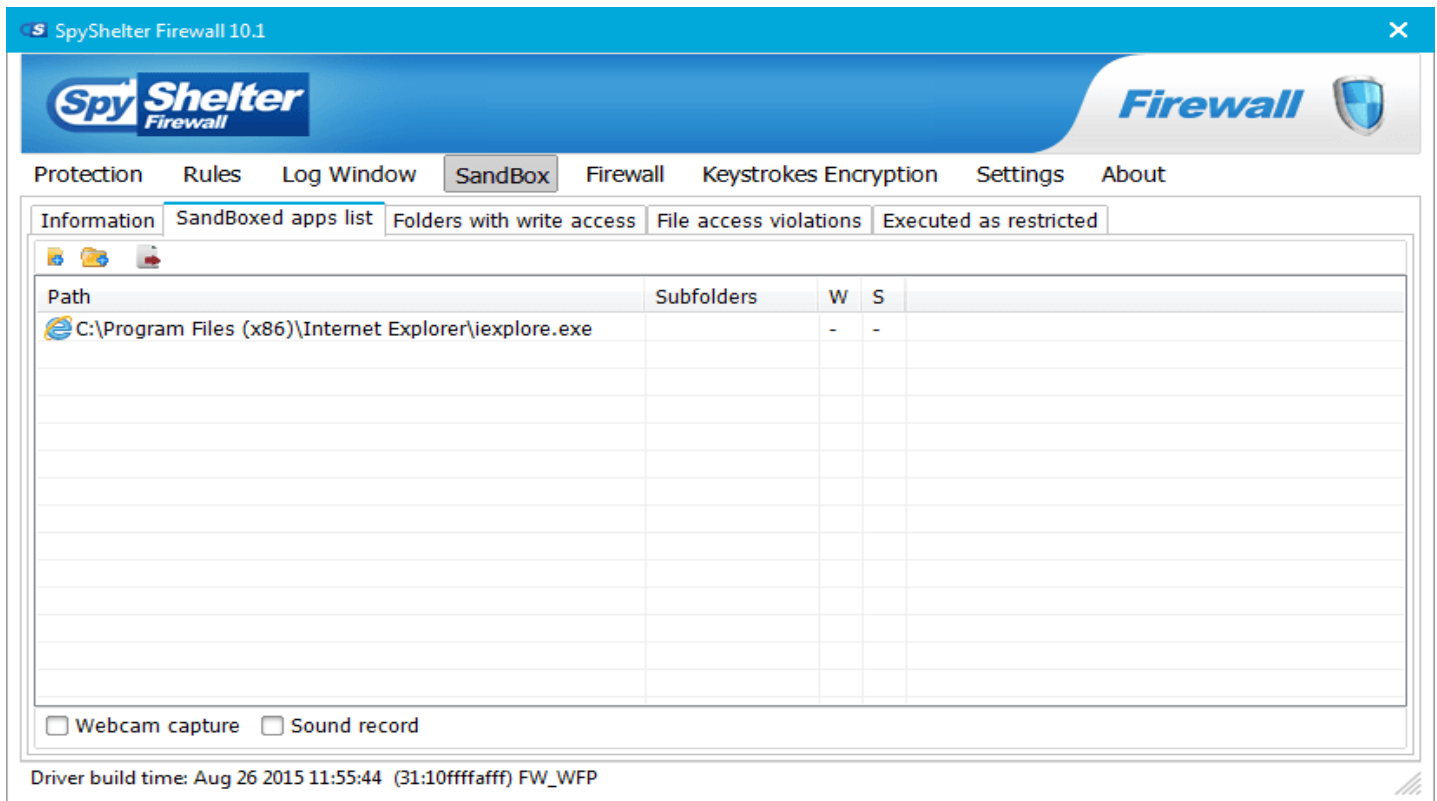
Вкладка Информация

Эта вкладка содержит сведения об этой функции.



Вкладка Список Ограниченных Приложений

Эта вкладка содержит список ограниченных приложений.



Три маленьких значка в верхней части позволяют вам выполнить несколько действий:

Добавить файл:

Вы можете выбрать файл для добавления в список (то есть приложение, которое вы хотите выполнить как ограниченное).

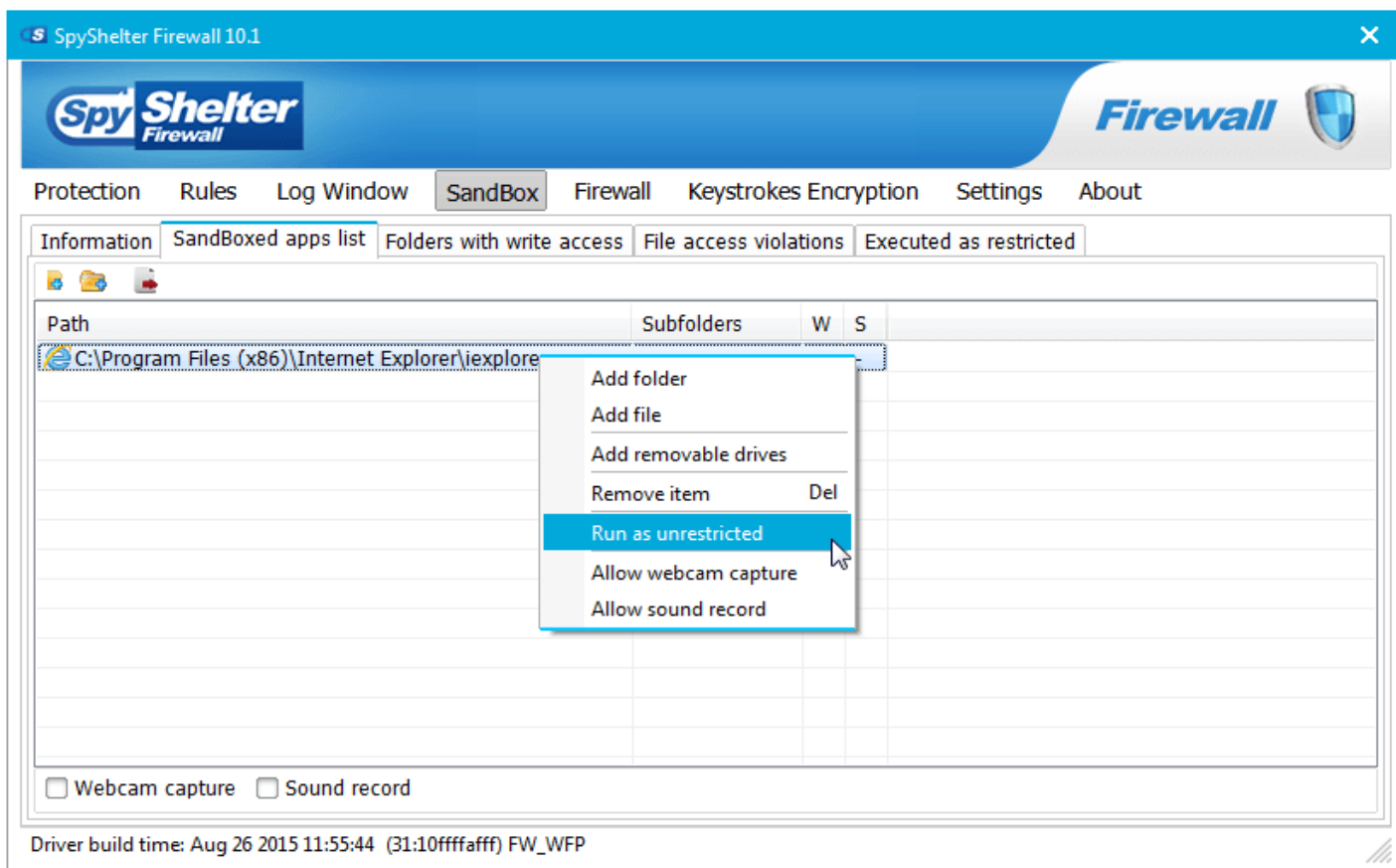
Добавить папку:

Можно также добавить целую папку, вместо одного файла. В этом случае, все приложения, содержащиеся в выбранной папке будут выполняться как ограниченные.

Удалить элемент:

Удаляется элемент из списка, если вы хотите отменить ограничения при выполнении приложения.

Если вы щелкните правой кнопкой мыши на элементе или внутри окна, появится меню с большим числом вариантов (как вы можете видеть на скриншоте ниже):



Добавление съемных дисков:

У вас также есть возможность добавления съемных дисков (CD-ROM, флоппи-дисков и флэш-накопителей) в ограниченном режиме. Таким образом, все приложения, содержащиеся на этих дисках будут выполняться как ограниченные.

Выполняться как неограниченное:

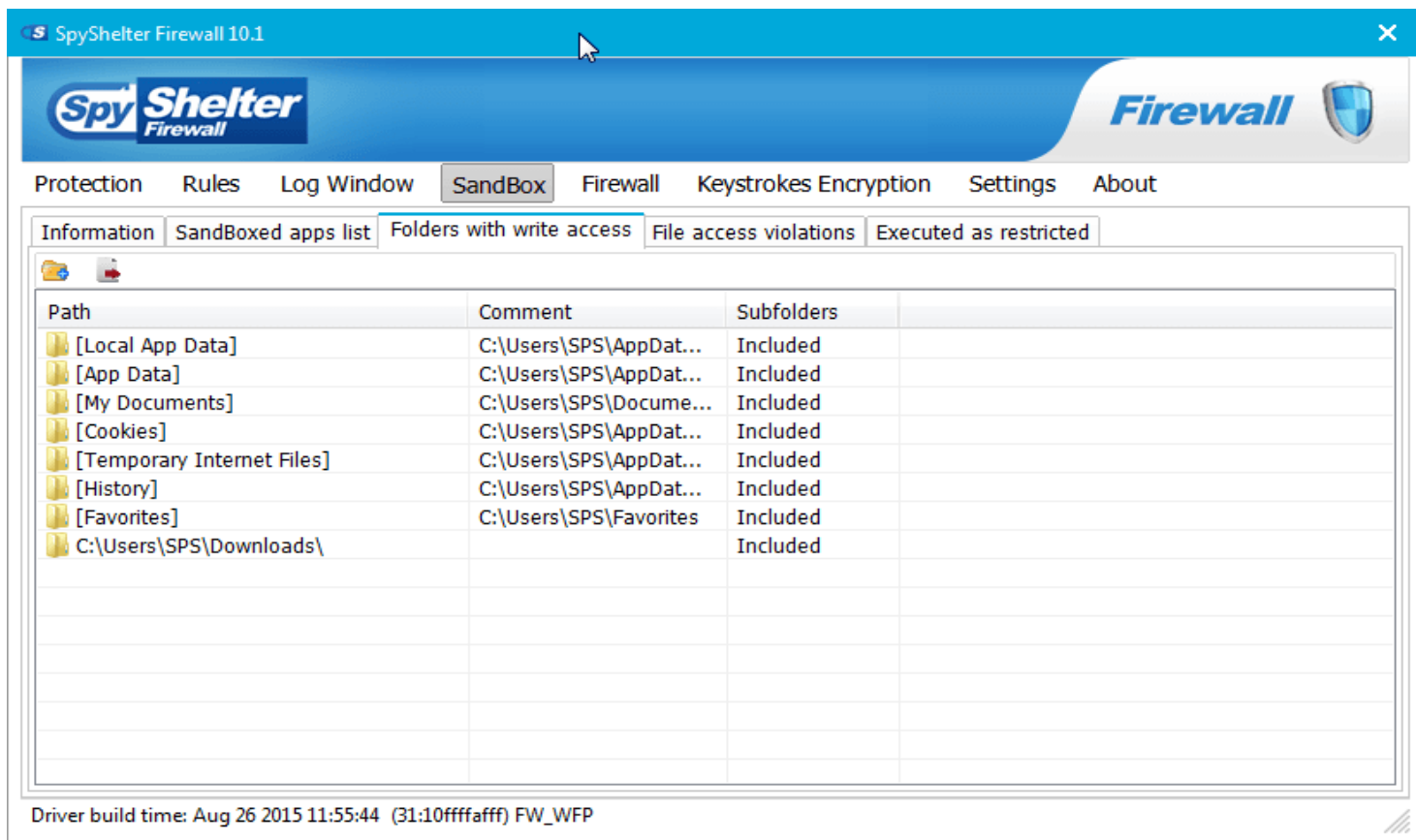
Если вы щелкните правой кнопкой мыши на приложение и выберите этот параметр, приложение перестанет выполняться как ограниченное.

Вы также можете разрешить приложениям в этом списке захват изображения с веб-камеры и запись звука. Обычно эти два варианта автоматически активируются при добавлении приложения в список. Если это не то, что вы хотите, вам просто нужно кликнуть правой кнопкой мыши на элементе и выбрать **Запретить захват вебкамеры и/или Запретить запись звука**.

Вы, также, можете контролировать эти параметры, установив или сняв их в нижней части окна.

Вкладка «Папки с доступом на запись»

В этой вкладке вы можете увидеть папки, к которым вы предоставили доступ на запись.



Щелкнув правой кнопкой мыши на элементе, можно вызвать небольшое меню, из которого можно выполнить следующие действия:

Добавить папку:

Добавление папки в список.

Добавить специальную папку:

Есть некоторые конкретные папки, которые вы можете добавить более быстрым способом, с помощью этой опции. Это папки App Data, Local App Data, My Documents, Cookies, Desktop, Temporary Internet Files и History.

Добавить доступ для съемных дисков:

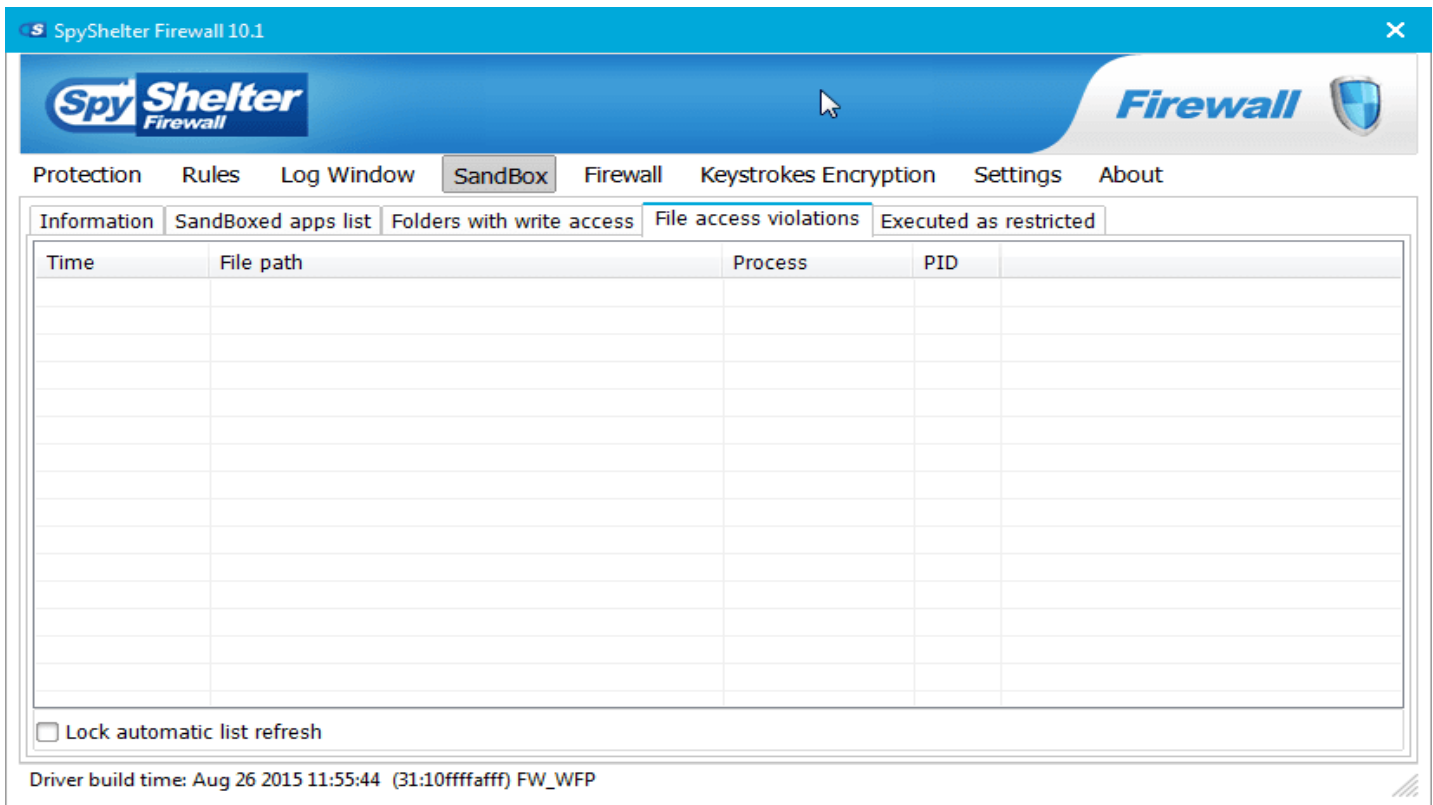
Если вы хотите, можно предоставить высокий доступ на запись к съемным дискам (Флэш-картам и USB-накопителям).

Удалить элемент:

Удаление папки из списка.

Владка «Нарушение доступа к файлам»

В этой вкладке появляется запись всякий раз, когда блокируется доступ к файлам.



Вы можете просмотреть информацию о времени, когда доступ к файлу был заблокирован, путь к файлу, имя процесса, который попытался получить доступ и PID процесса. Если вы щелкните правой кнопкой мыши на пункте, появится меню, содержащее следующие параметры:

Добавить доступ на запись в папку Имя_этой_папки:

Данный параметр позволяет изменить разрешения для выбранного файла.

Обновить список:

Проверьте, есть ли новые действия, которые были заблокированы.

Очистить список:

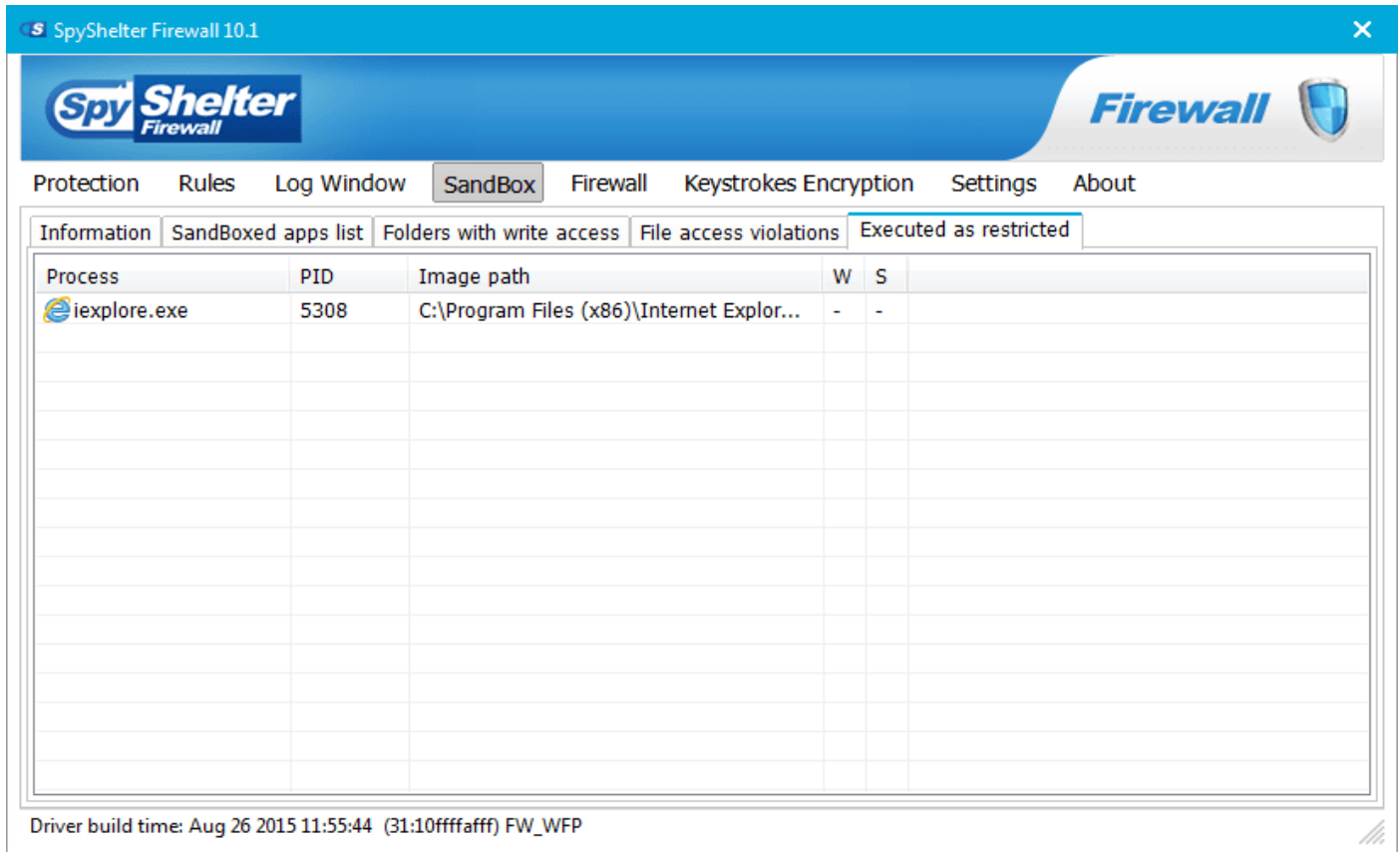
Этот параметр удаляет все предупреждения.

Если вы не хотите автоматического обновления списка предупреждений, вы можете выбрать опцию «**Блокировать автоматическое обновление списка**» в нижней части окна.

Поскольку приложениям, которые выполняются в ограниченном режиме, не разрешен доступ ко всем папкам на запись, вы можете увидеть здесь сообщение, если некоторые из этих приложений попытались получить доступ на запись к папке и были заблокированы. Таким образом, вы можете дать им разрешение на запись, чтобы быть уверенным, что они продолжают функционировать должным образом, даже если они выполняются как ограниченные.

Вкладка «Выполняются как ограниченные»

В этой вкладке вы можете увидеть все приложения, выполняющиеся в ограниченном режиме.



Можно удалить приложение из списка, щелкнув правой кнопкой мыши его имя и выбрав **Завершить процесс**, или вы можете просто выделить приложение, которое вы хотите удалить, и нажать клавишу "Del".

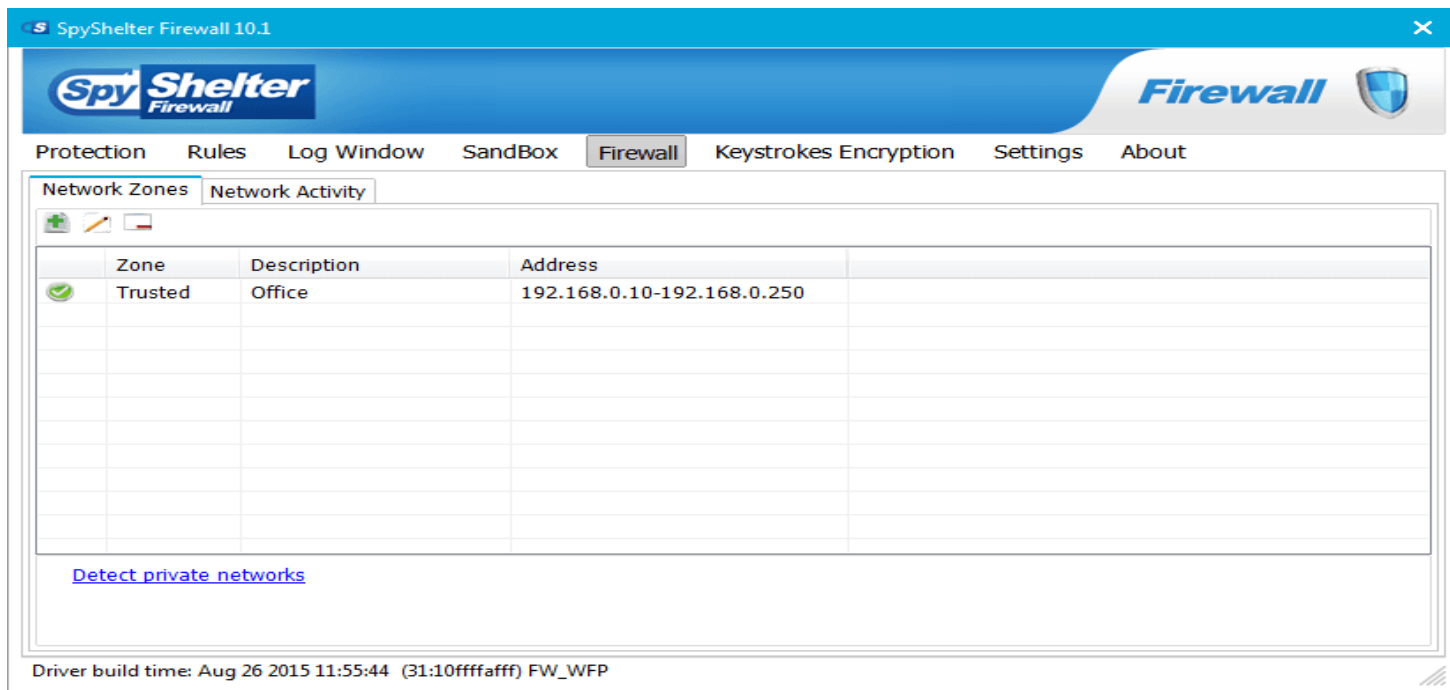
Вкладка Firewall

Закладка Сетевые Зоны

Эта вкладка содержит зоны сети (например, ip-диапазоны) где доступ разрешен (тип **Доверенная Зона**), блокирован (тип **Заблокированная Зона**) или неопределенная (тип **Неопределенная Зона**)

Пользователь может задать зоны надежных локальных сетей и Spyshelter авто позволит запросы, когда приложение пытается получить доступ к этой локальной сети (например, когда происходит обмен файлами)

Пользователь может нажать на лейбл **«Обнаружение частных сетей»** и Spyshelter попытается автоматически определить локальные сети



Добавление/Редактирование зоны

Вы можете добавить новую зону, нажав кнопку +, или редактировать существующие зоны, нажав кнопку **изменить** или дважды щелкнув существующую зону

Описание: Имя/описание зоны сети.

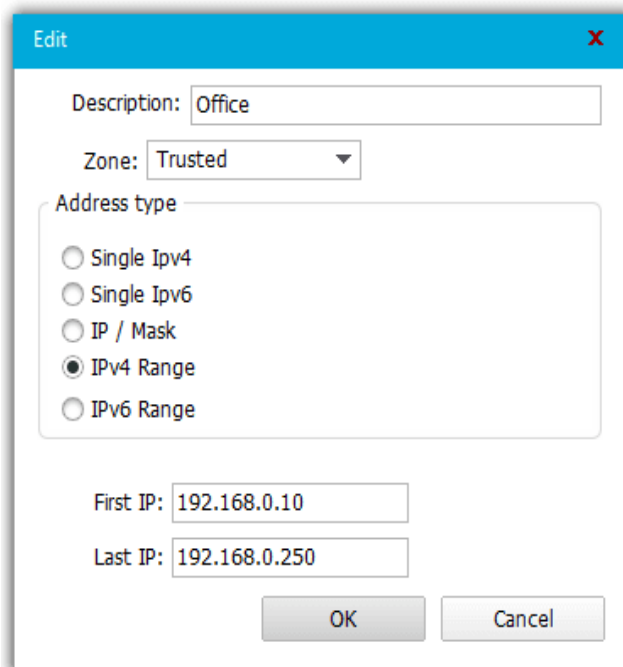
Зона: Надежная, - все запросы для доступа к этой сети будут авто разрешены.

Заблокированная, - все запросы для доступа к этой сети будут автоматически заблокированы.

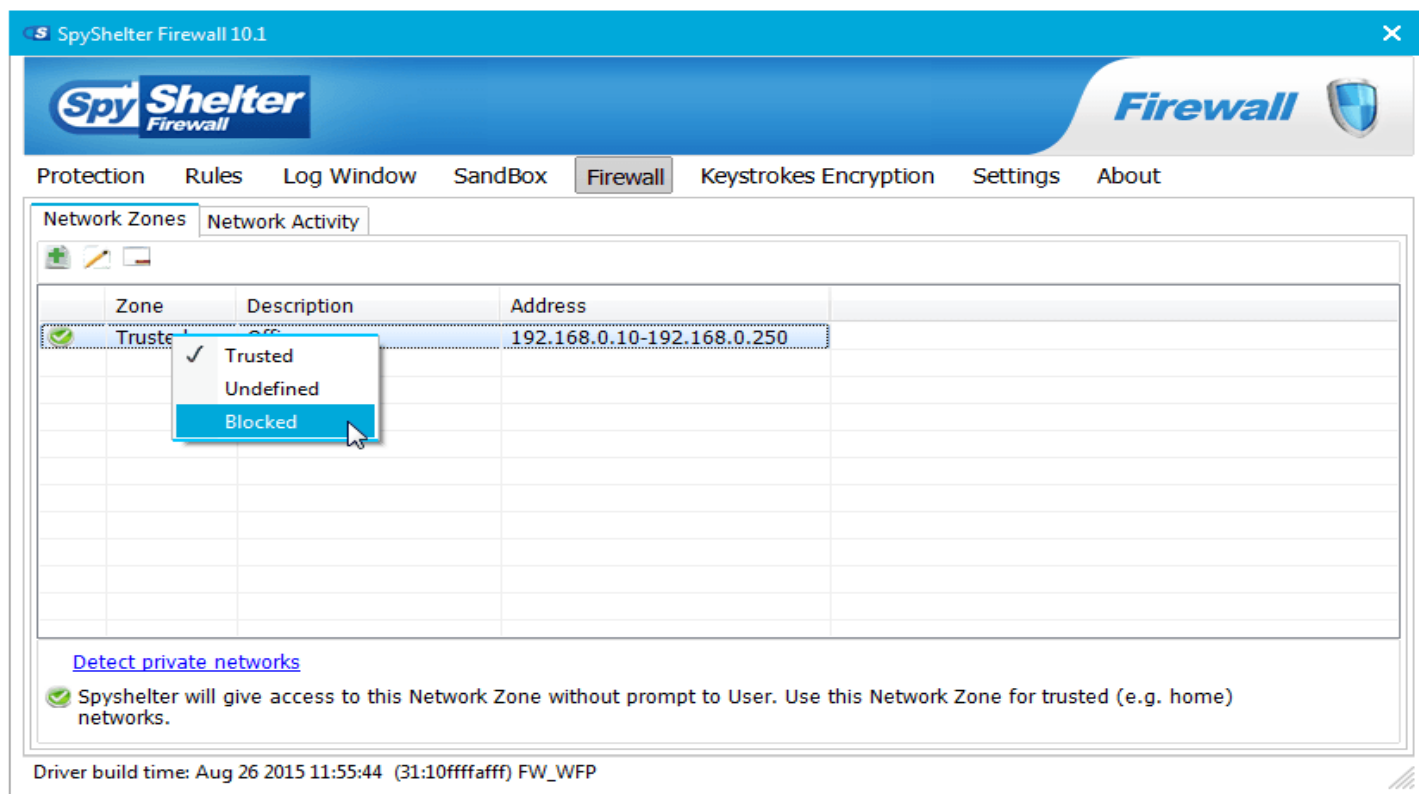
Неопределенная - означает, что все попытки доступа к этой сети будут запрашивать авторизацию.

Тип адреса: Определяет, задана ли зона IP-адресом / маской, диапазоном IPv4-адресов или диапазоном адресов IPv6.

Первый/последний IP-адрес или IP/маска: диапазон IP-адресов или маска указаны для зоны сети.

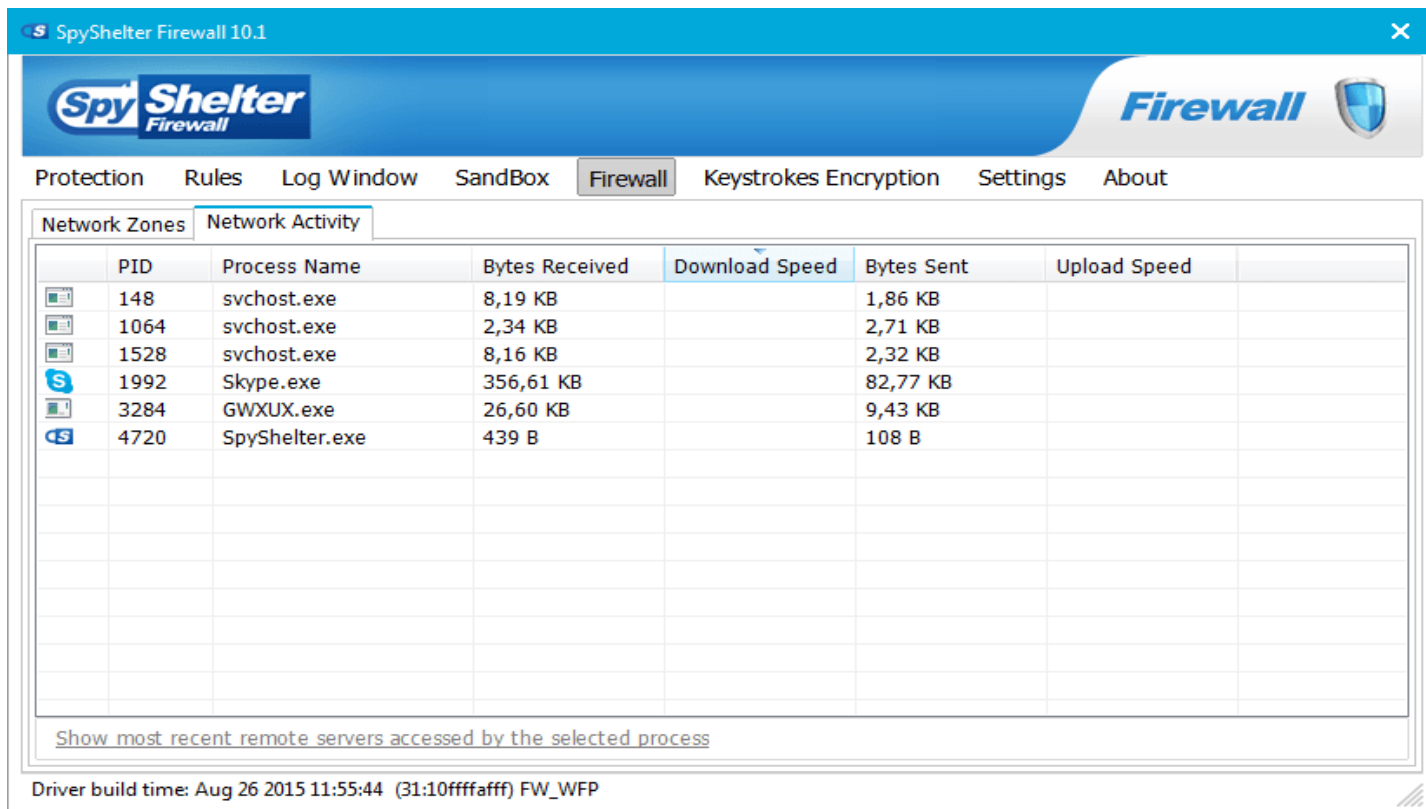


Вы можете также щелкнуть левой кнопкой мыши на запись в столбце **Зона**, чтобы изменить **тип Зоны**:

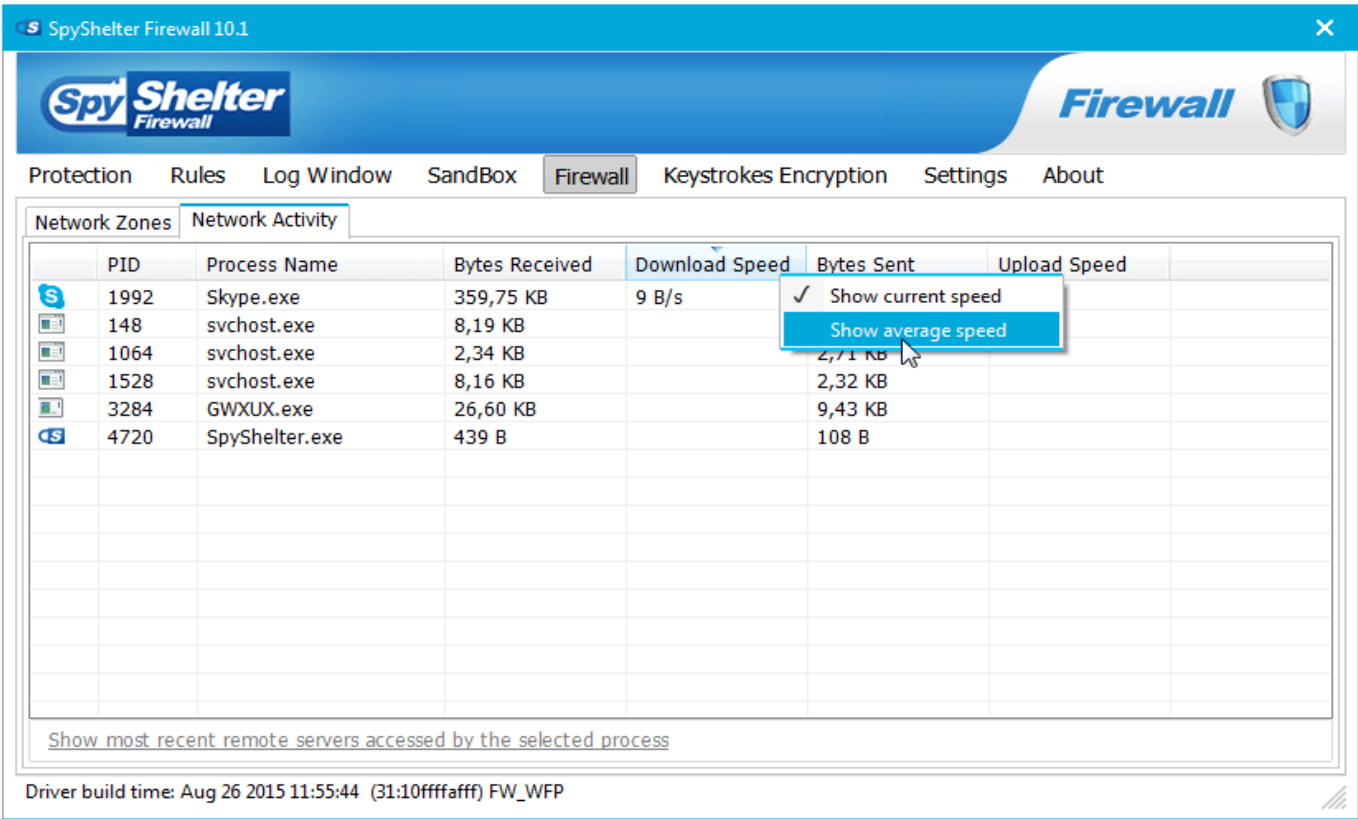


Сетевая активность

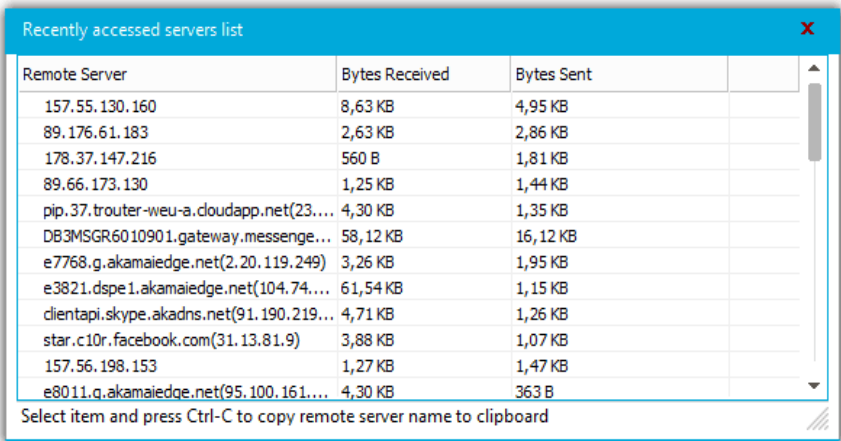
Эта вкладка позволяет вам смотреть, какие приложения, в настоящее время, подключены к Интернету и сколько данных они отправили и получили.



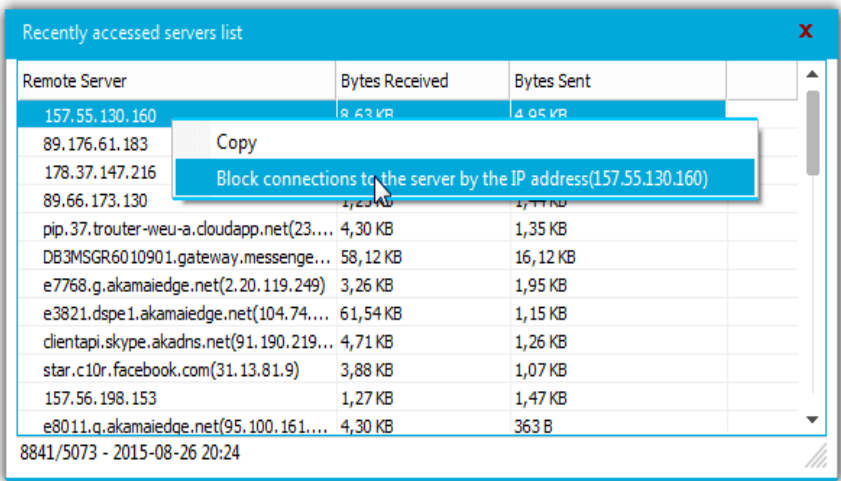
Нажав правой кнопкой мыши на **Скорость Загрузки** или **Скорость Выгрузки**, можно изменить отображение **текущей** скорости на **среднюю** скорость.



Вы, также, можете дважды щелкнув на процессе, раскрыть список серверов, с которыми приложение взаимодействует.



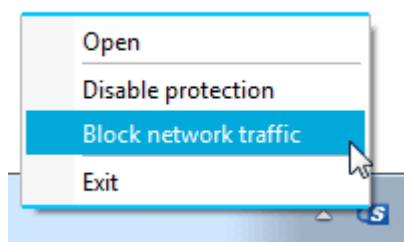
Если вы хотите блокировать подключение к определенному удаленному серверу, щелкните правой кнопкой мыши и выберите **Заблокировать**.



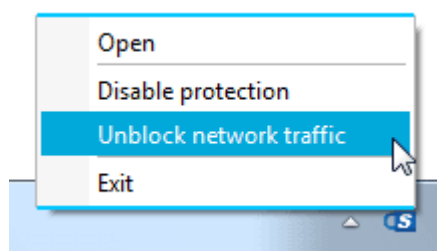


Сетевой трафик

Вы можете заблокировать все сетевые подключения, кликнув правой кнопкой мыши на иконку в меню трея SpyShelter.



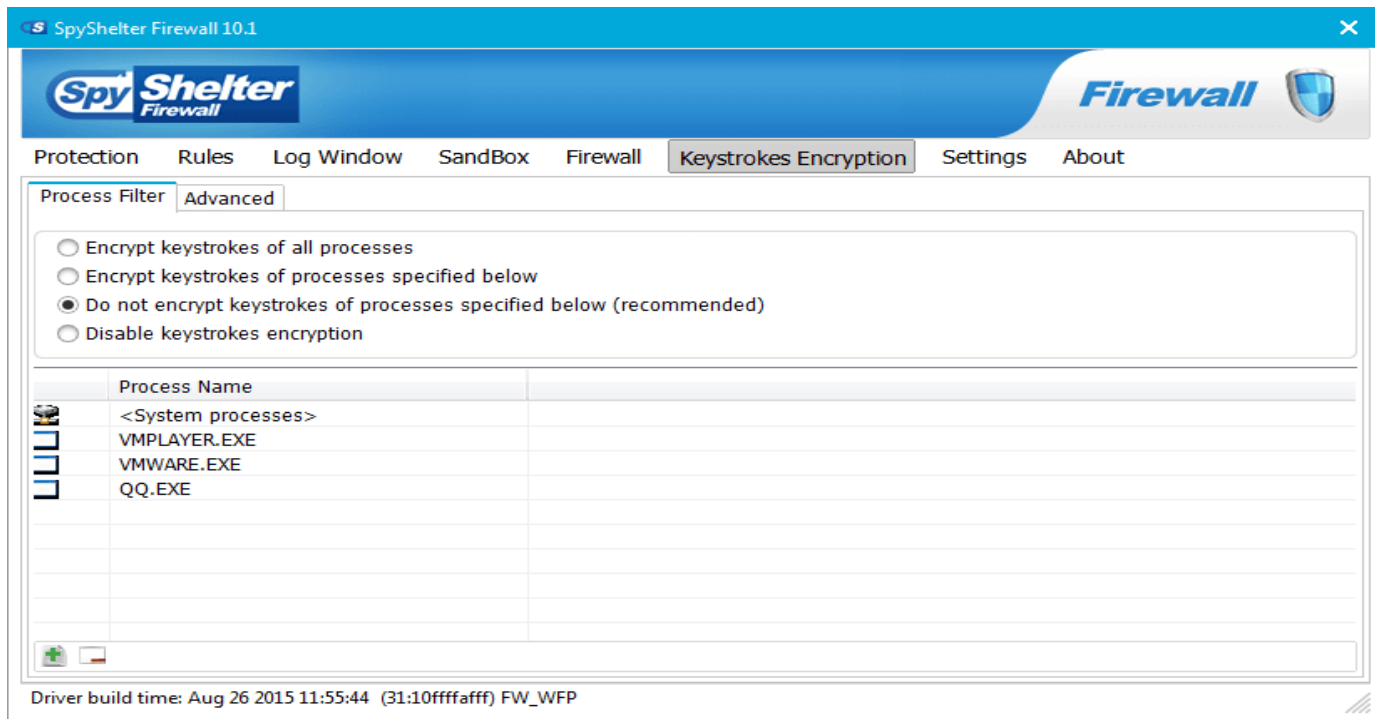
После того, как вы блокировали соединение, вы можете легко разблокировать его, таким же образом.



Шифрование Нажатий Клавиш

Драйвер шифрования клавиатуры шифрует каждое нажатие клавиши вами. Кроме того эта функция блокирует другие приложения даже от получения этих зашифрованных нажатий клавиш. Напечатанные нажатия клавиш отправляются через безопасный туннель только к тому приложению, которое находится в фокусе клавиатуры. Шифрование нажатий клавиш начинается перед входом в учетную запись Windows - это независимое решение. Все ваши важные личные данные будут надежно зашифрованы, с момента запуска компьютера, и практически бесполезны для различных клавиатурных шпионов и опасных приложений.

Модуль, в настоящее время, поддерживает 32 и 64 битные операционные системы и доступен в SpyShelter Premium и SpyShelter Firewall.



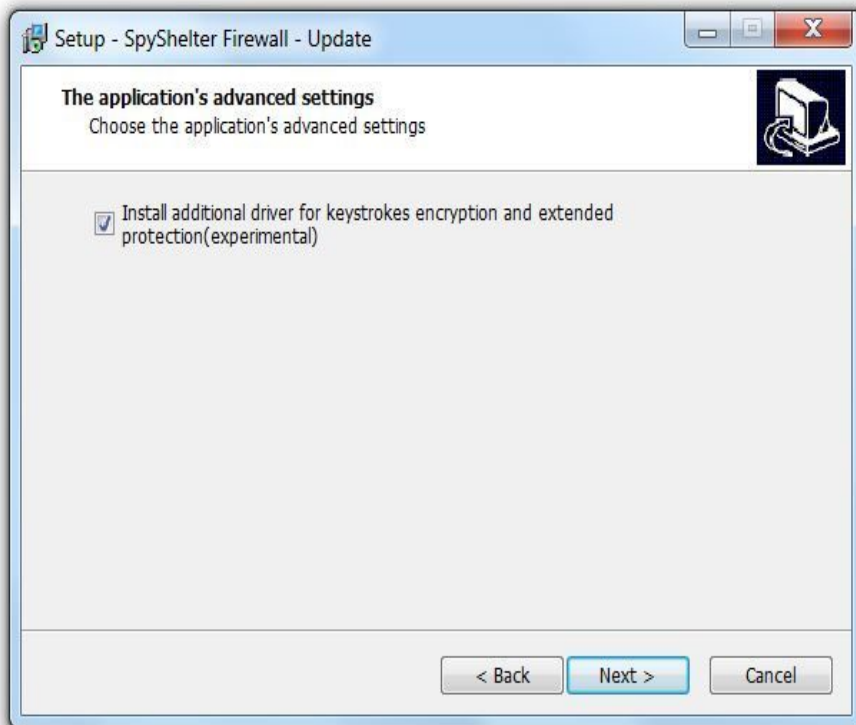
Включение Шифрования Клавиш

Шифрование Нажатий Клавиш может быть включено, только, при установке SpyShelter. Так что, если вы не видите вкладку **Шифрование Клавиш**, необходимо скачать установщик продукта, которым вы владеете.

1) Если вы установили SpyShelter и хотите добавить функцию шифрования нажатия клавиш:

Запустите программу установки и установите флажок «**Установка дополнительных драйверов для шифрования нажатия клавиш и расширенной защиты**».

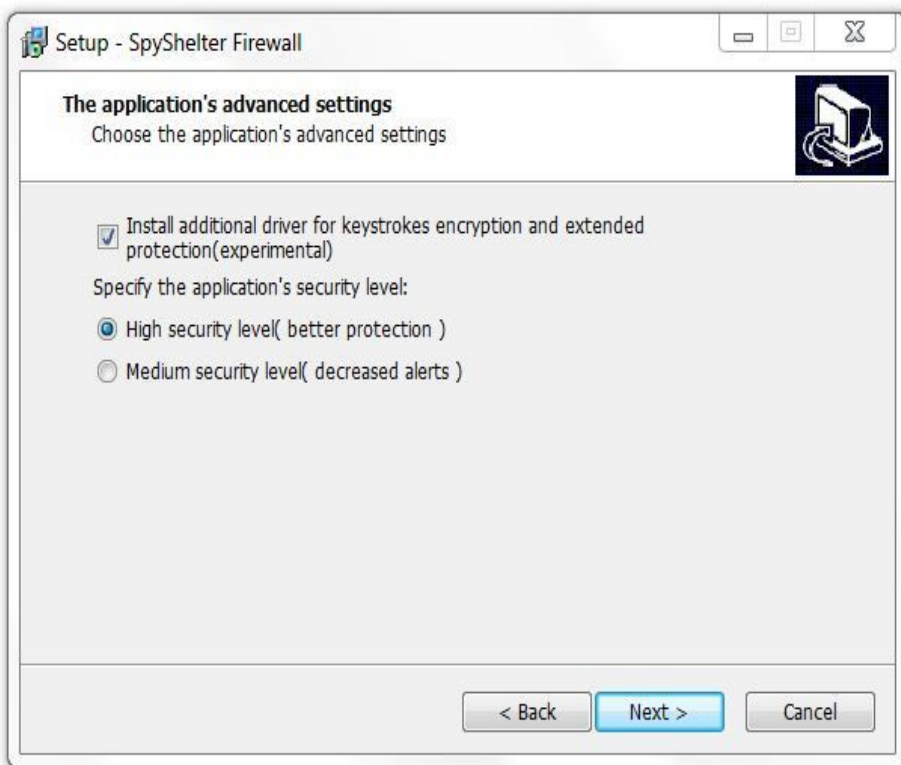
И продолжите установку. После чего перезагрузите компьютер.





2) Если вы устанавливаете SpyShelter впервые и хотите включить шифрование нажатий клавиш:

Установите флажок «**Установка дополнительных драйверов для шифрования нажатия клавиш и расширенной защиты**» на экране, где вы выбираете уровень защиты.

И продолжите установку. >



Вкладка Фильтр процессов

Вкладка Фильтр процессов позволяет управлять процессами, для которых нажатия клавиш будет зашифровано драйвером шифрования. Вы можете добавить или удалить их с помощью  и  кнопок.

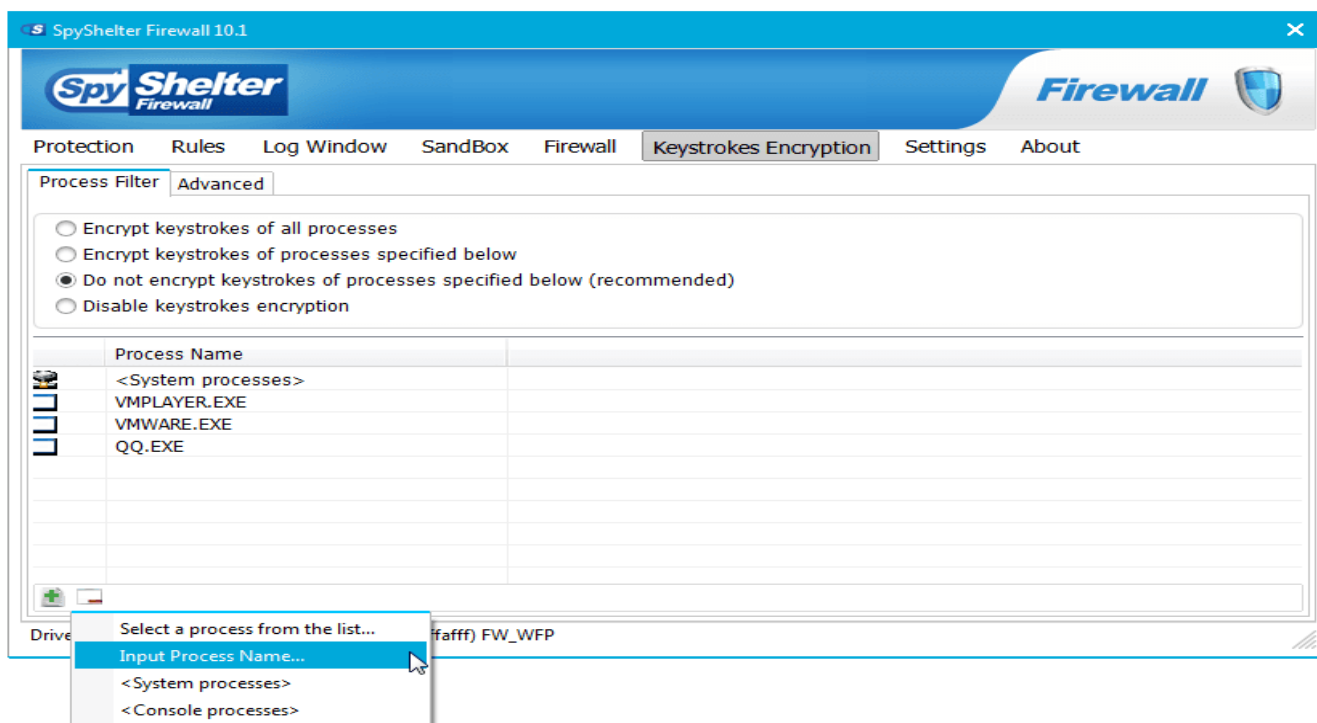
Шифровать нажатия клавиш для всех процессов — При выборе этого параметра будут шифроваться нажатия для каждого процесса.

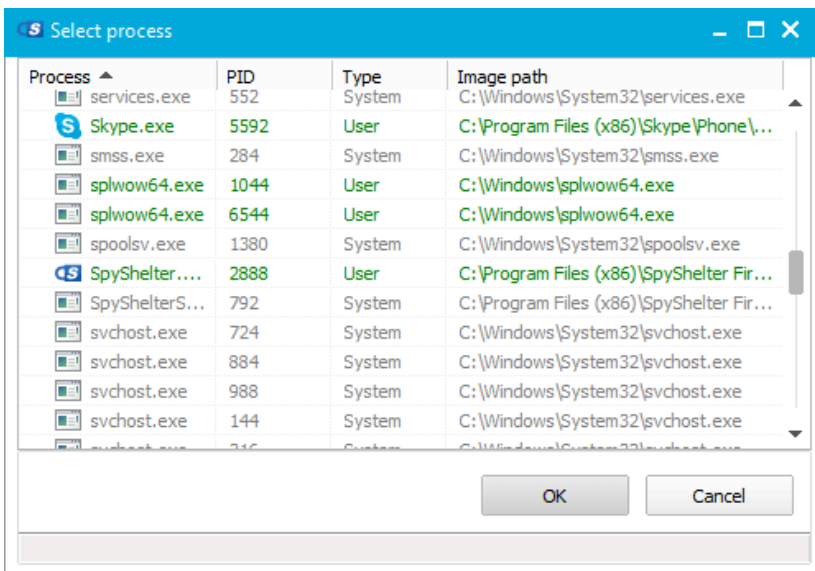
Шифровать нажатия клавиш процессов, указанных ниже - Будут зашифрованы только процессы из списка. С помощью кнопок ниже списка, можно добавить процессы и удалить их.

Не шифровать нажатия клавиш процессов, указанных ниже - Процессы из списка не будут зашифрованы.

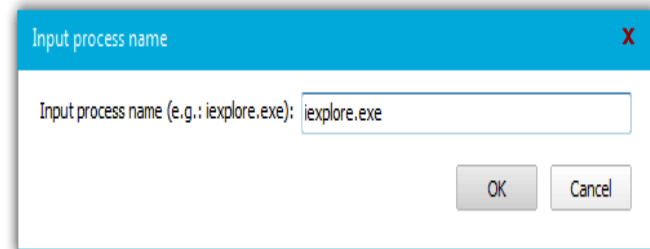
Отключить шифрование нажатий клавиш - Полностью отключает шифрование нажатий клавиш.

Шифрование процессов системы отключено по умолчанию для того, чтобы избежать проблем во время входа в свою учетную запись Windows.





Выбрать процесс из списка... - Позволяет выбрать выполняемый процесс и добавить < его в список.



Ввести имя процесса - Позволяет добавить имя определенного процесса в список.

<**Системные процессы**> - Добавляет все системные процессы.

<**Консольные процессы**> - Добавляет все консольные процессы.

Вкладка Дополнительно

Вкладка Дополнительно предназначена только для продвинутых пользователей. Это было сделано для случаев проблем совместимости.

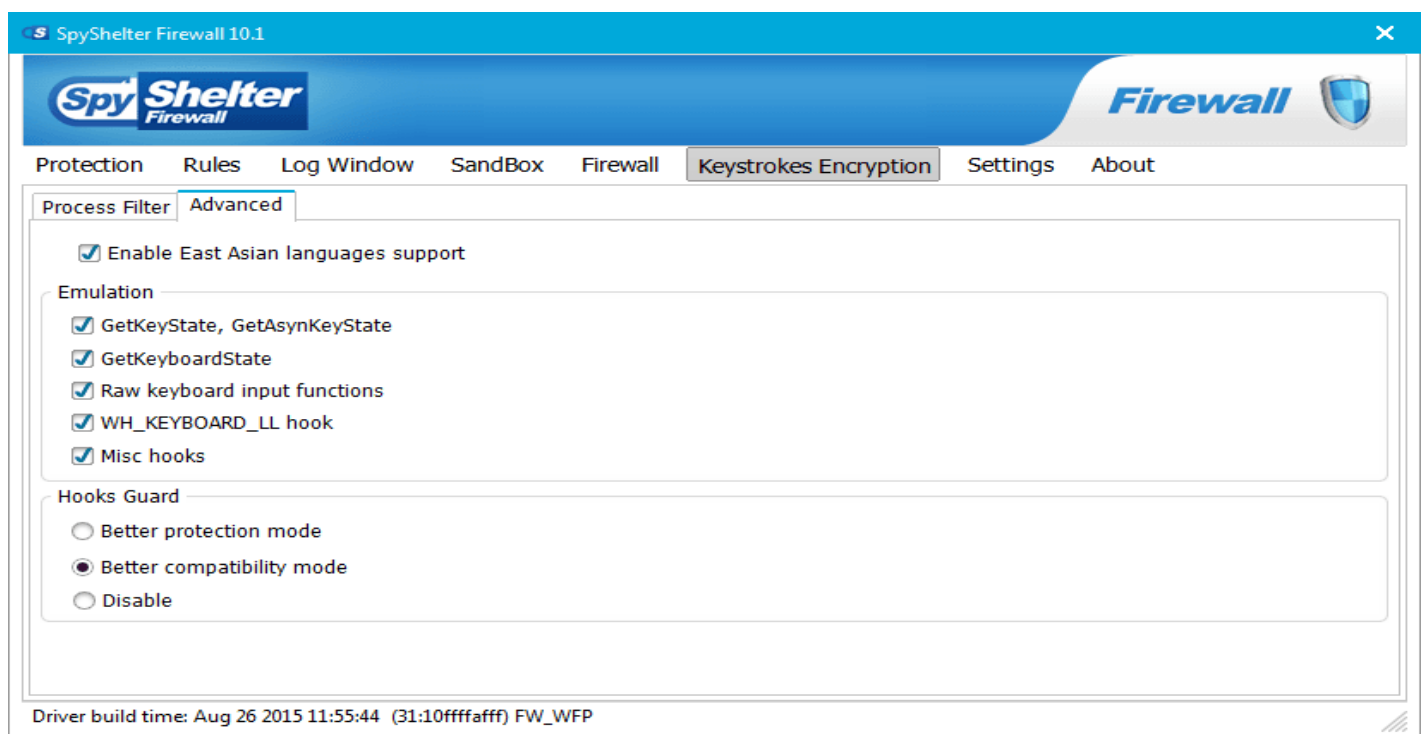
Эмуляция

Эти параметры следует изменять только опытным пользователям или тем, кто испытывает проблемы с драйвером ключа шифрования.

Сняв флажок с параметра группы **Эмуляции** можно сделать анти-кейлоггер защиту немного лучше, но менее совместимой.

Приложение (находящееся в фокусе клавиатуры) имеет возможность прочитать зашифрованные коды клавиш с помощью различных функций.

Устанавливая/снимая флажок опции в окне эмуляции, вы выбираете, какие функции системы будут иметь возможность читать зашифрованные нажатия клавиш.





Hooks Guard

Hooks Guard это функция самообороны, которая помогает защитить от различных кейлоггеров.

Лучший режим защиты - рекомендуется использовать этот параметр, так как он обеспечивает лучшую защиту. Если нет проблем совместимости, он не должен быть изменен.

Лучший режим совместимости - выбирать только, если возникают проблемы с шифрованием нажатий клавиш.

Использование SpyShelter's Шифрование Нажатий Клавиш с другим программным обеспечением шифрования клавиш

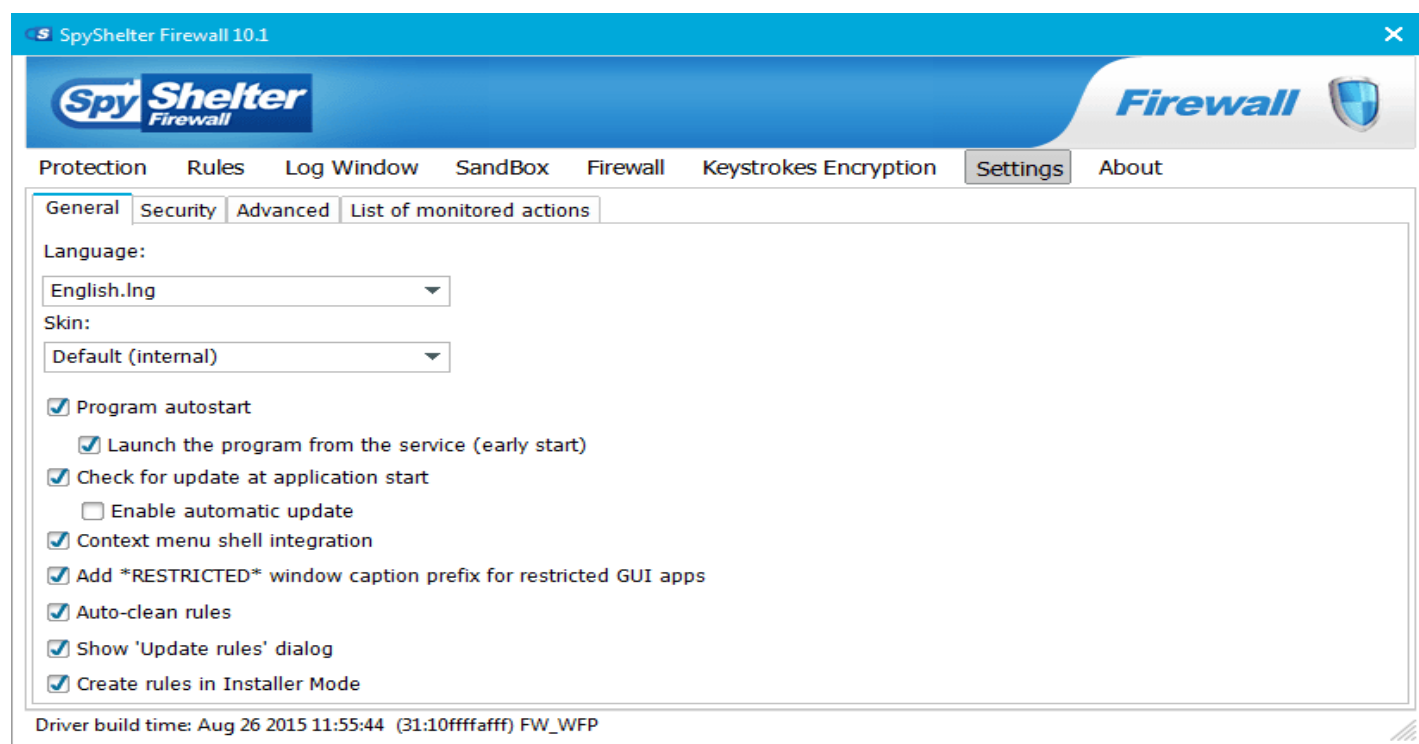
Если есть любые проблемы, используйте функцию Фильтр Процессов и добавьте iexplore.exe в список исключений.

ПРИМЕЧАНИЕ: В системе с Windows XP шифрование нажатий клавиш устанавливается в режим лучшей совместимости по умолчанию для того, чтобы устранить возможные проблема совместимости с IE.

Вкладка "Параметры"

В этом разделе вы можете настроить множество параметров программы.

Вкладка «Общие»



Язык:

Здесь вы можете выбрать язык программы. Доступны следующие значения:

- Brazilian -Portuguese
- Chinese
- Traditional -Chinese
- Croatian
- Czech
- English
- French
- German
- Italian
- Japanese
- Macedonian
- Polish
- Serbian
- Spanish
- Turkish
- Danish

Автозапуск Программы:

Установите этот флажок, чтобы запускать программу каждый раз, когда загружается Windows.

Запуск программы как сервис (ранний старт):

Включение этого параметра даст возможность SpyShelter установить службу в вашей системе, которая позволит SpyShelter запускаться раньше.

Проверить наличие обновлений при запуске приложения:

Проверяет наличие обновлений каждый раз, когда вы запустите SpyShelter.

Включить автоматическое обновление

Этот параметр позволяет включить функцию автоматического обновления. После выпуска новой версии, SpyShelter будет автоматически обновляться в фоновом режиме. После обновления SpyShelter предложит вам перезагрузить компьютер.

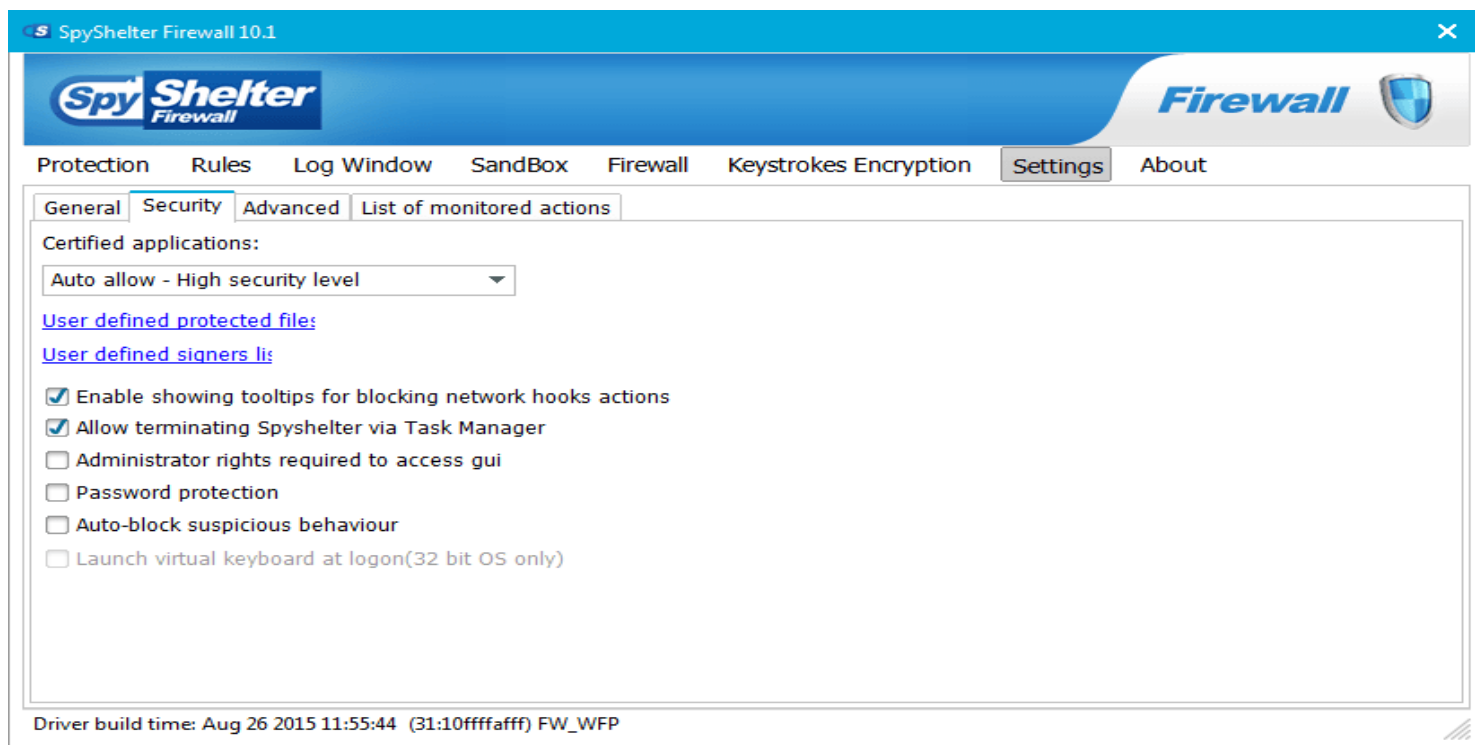
Добавление префикса *ограниченное* в заголовке окна для ограниченного GUI приложения:

Установите этот флажок, если вы хотите увидеть слово * ограниченное * перед именем приложения в его окне и когда приложение сворачивается в трей.

Интеграция в контекстное меню оболочки:

Если этот параметр включен, в стандартное контекстное меню файлов и папок, которое появляются при нажатии правой кнопкой мыши на значке файла в проводнике или на рабочем столе, добавятся несколько дополнительных элементов с функциями SpyShelter.

Вкладка «Безопасность»



Сертифицированные приложения:

Здесь вы можете определить, как SpyShelter брандмауэр будет взаимодействовать с подписанными приложениями.

Доступны следующие значения:

Авто-Разрешить - высокий уровень безопасности:

Основываясь на наших внутренних правилах, будет автоматически разрешать некоторые не подписанные программы без запроса. Это происходит, когда SpyShelter брандмауэр уже определил и классифицировал эти приложения как безопасные.

Разрешить Microsoft:

С этой опцией автоматически разрешены только приложения, подписанные Майкрософт. Если приложение не подписано корпорацией Майкрософт, SpyShelter брандмауэр будет спрашивать вас, хотите ли вы разрешить или запретить его.

Авто -Разрешить - уровень средней безопасности:

Основываясь на наших внутренних правилах, это сбалансированный вариант между высоким уровнем безопасности и меньшим количеством ложных срабатываний. Это рекомендуемый вариант для не опытных пользователей.

Спросить пользователя:

Когда пользователь активизирует этот параметр, программа предложит ему задавать желаемое действие [разрешить или запретить] для каждой программы, которые могут демонстрировать подозрительное поведение

Список подписей, определенных пользователем:

Эта функция позволяет вам вручную добавлять в список и удалять надежные и ненадежные цифровые подписи. Приложения с надежными подписями будут выполняться по умолчанию, в то время как ненадежные из них не будут.

Используйте эту функцию с осторожностью, поскольку некоторые обнаруженные программы могут иметь цифровую подпись, если они являются коммерческими продуктами.

Включить показ подсказки для блокирования сетевых hooks действий:

Этот параметр предлагает включить подсказки в трее, которые, например, сообщают о dll инъекции или ssl loggers или других hooks.

Административные права для доступа к GUI:

Только администраторам будет разрешен доступ к пользовательскому интерфейсу. Когда пользователь работает под гостевой учетной записью, доступ к GUI будет невозможен.

Защита с помощью пароля:

Пользователь может задать пароль для доступа к пользовательскому интерфейсу.

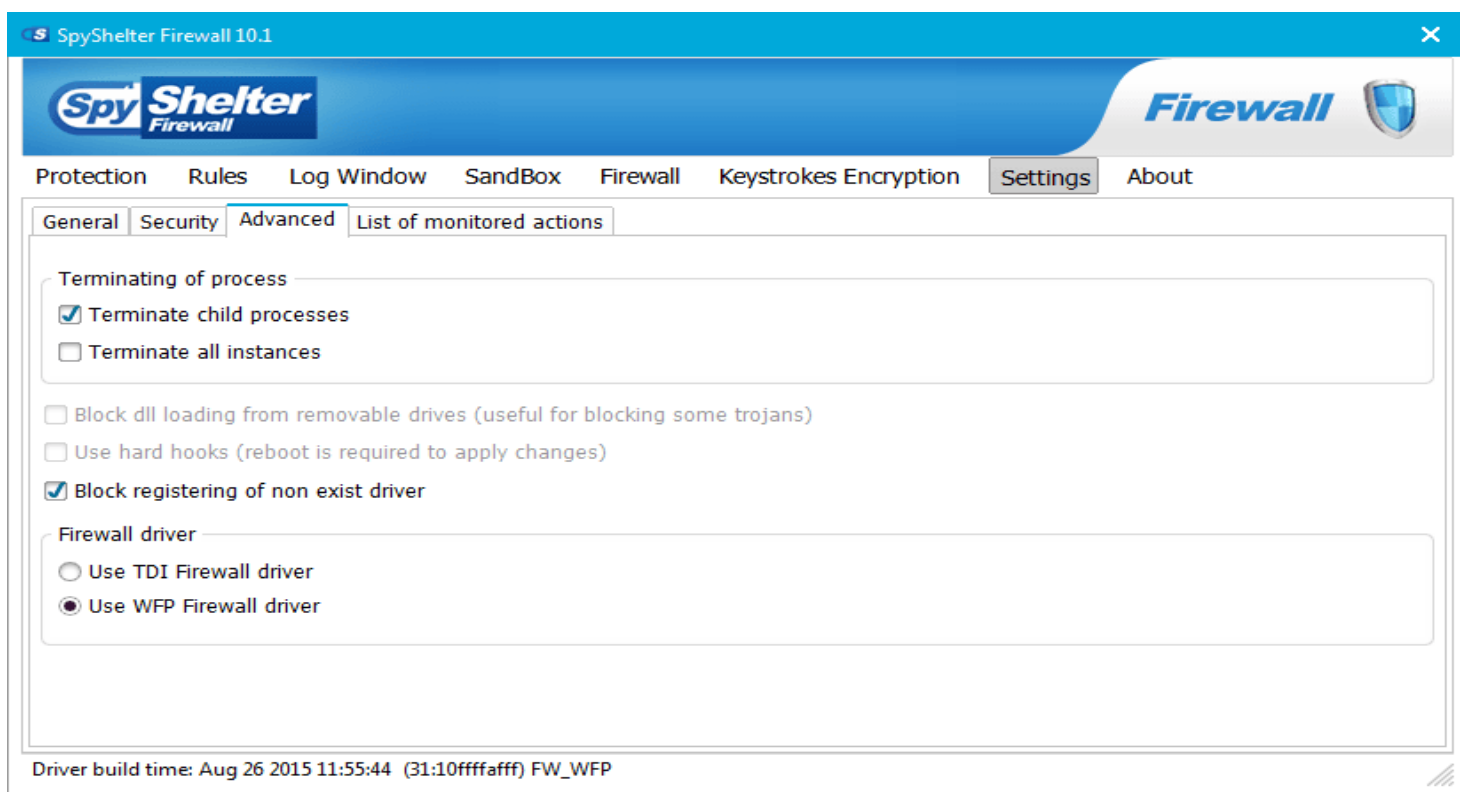
Автоматическое блокирование подозрительного поведения:

Если этот параметр выбран, приложения с подозрительным поведением будут автоматически включены в черный список.

Запуск виртуальной клавиатуры при входе в систему:

Эта функция доступна только для 32-разрядной ОС. Когда она включена, кнопка запуска виртуальной клавиатуры будет отображаться при входе пользователя в систему. Это очень полезно, когда пользователь хочет безопасно войти в учетную запись, но не уверен, что его клавиатура не имеет встроенный аппаратный кейлоггер.

Вкладка Дополнительно



Завершать дочерний процесс - завершить процесс, созданный подозрительным модулем, который вызвал оповещение

Завершать все экземпляры - убить все процессы с тем же путем, как и подозрительный процесс.

Блокировка загрузки библиотек dll со съемных дисков:

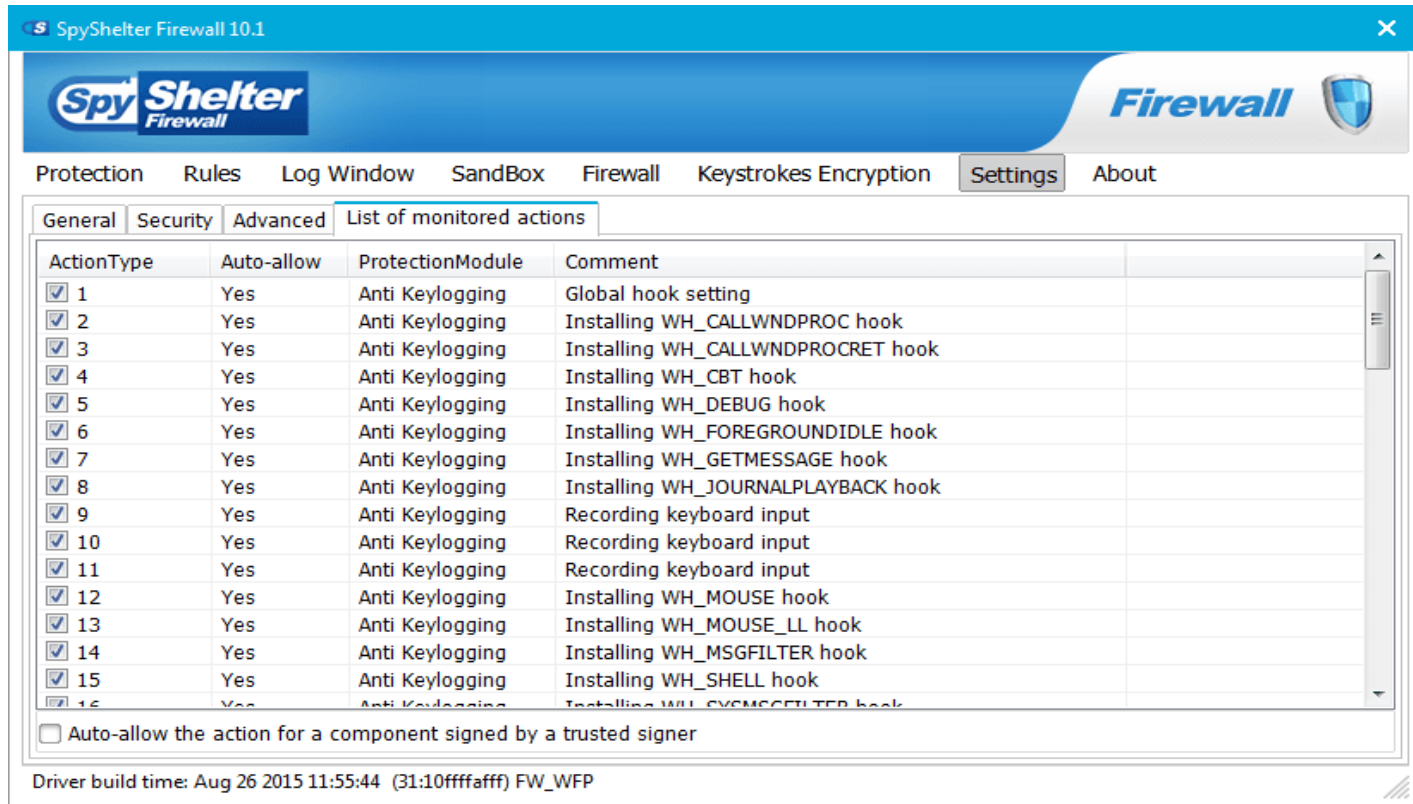
Установите этот флажок, если вы не хотите загружать dll файлы со съемных дисков (внешние жесткие диски, флеш-память, USB накопители). Некоторые трояны используют эту технику, поэтому вам может быть полезен выбор этой опции.

Использование жестких hooks - Использование жестких hooks (с помощью принудительной установки hook, когда есть проблемы с совместимостью при установке других приложений безопасности.)

Блок регистрации не существующего драйвера - с помощью этого параметра можно отключить отображение ложных оповещений о несуществующем драйвере, которые появляются при установке некоторыми программами обновлений и так далее..

Вкладка «Список отслеживаемых действий»

В этой вкладке вы можете увидеть список всех действий, которые контролируются в вашей системе.



По умолчанию отслеживаются все действия. Однако, если вы предпочитаете прекратить наблюдение за одним из них, вам просто нужно снять его выделение.

Авто-разрешение действий для компонента, подписанного доверенной цифровой подписью - По умолчанию SpyShelter авто-позволяет выполнять все действия, выполняемые доверенным компонентом. Вы можете выбрать любой тип действия из списка и снять флажок в этом поле, чтобы запретить.

Вкладка О Программе

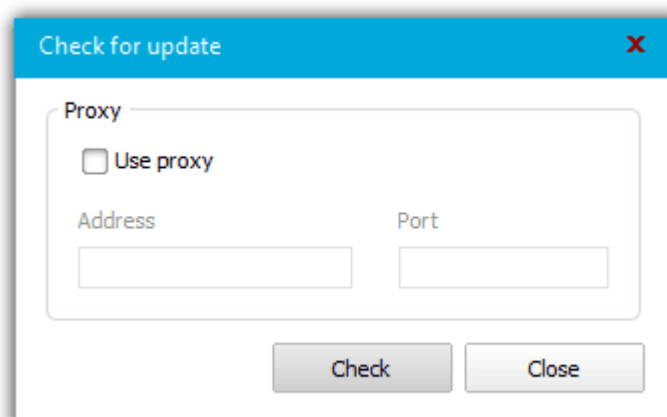


Справка:

Запускает этот файл справки.

Проверить обновления:

Выберите этот параметр, если вы хотите проверить, доступна ли новая версия программы (требуется подключение к Интернету). Если вы хотите использовать прокси-сервер, просто выберите «использовать прокси» и введите адрес и номер порта (см. скриншот ниже):



Сообщить об ошибке:

Используйте этот инструмент, если вы хотите отправлять сообщения об ошибках, которые вы заметили

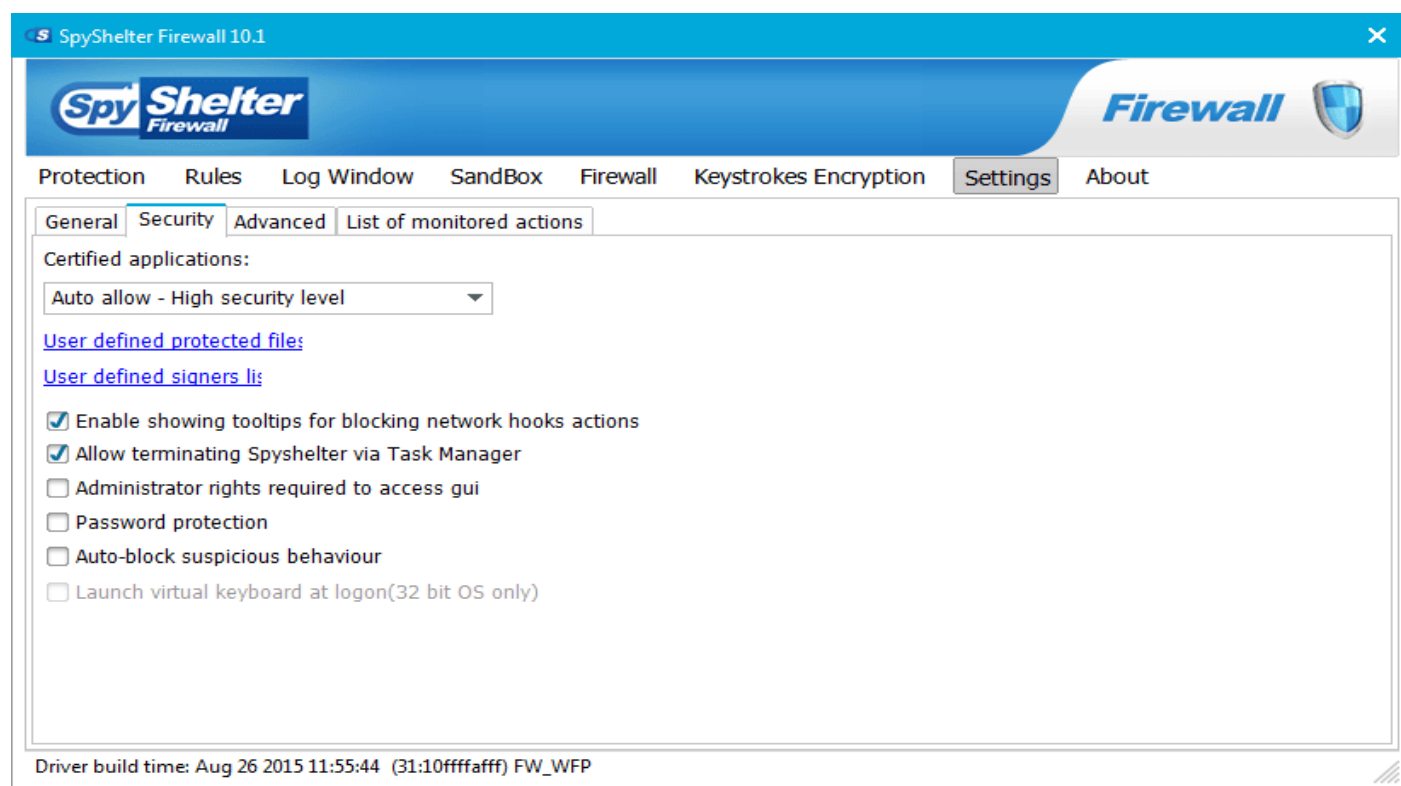
Определяемые пользователем защищенные файлы

Эта функция предназначена только для продвинутых пользователей.

По умолчанию SpyShelter защищает критические системные файлы. С помощью этой функции можно определить свой собственный список файлов и папок и защитить ваши конфиденциальные данные от несанкционированного доступа, например, вымогателей.

SpyShelter покажет окно предупреждения, если один из перечисленных файлов будет вовлечен в процесс. Каждый новый процесс, который будет пытаться получить доступ к файлу, будет вызывать новое окно оповещения. Оповещение может показать попытки **Чтения** или попытки **Записи&Чтения**, и две существующие категории защищенных файлов – **Общие** и **Личные**.

Эта функция может быть доступна в «**Настройка**» > вкладка «**Безопасность**».

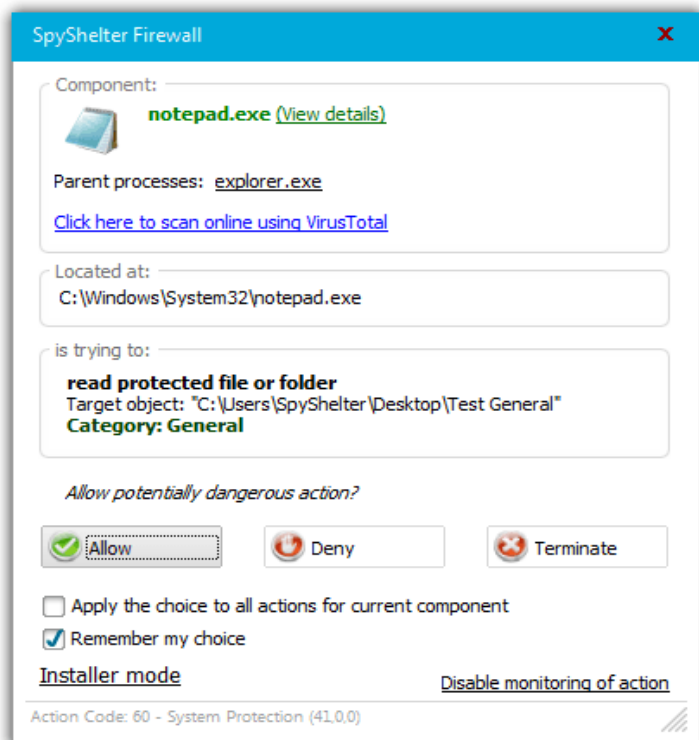
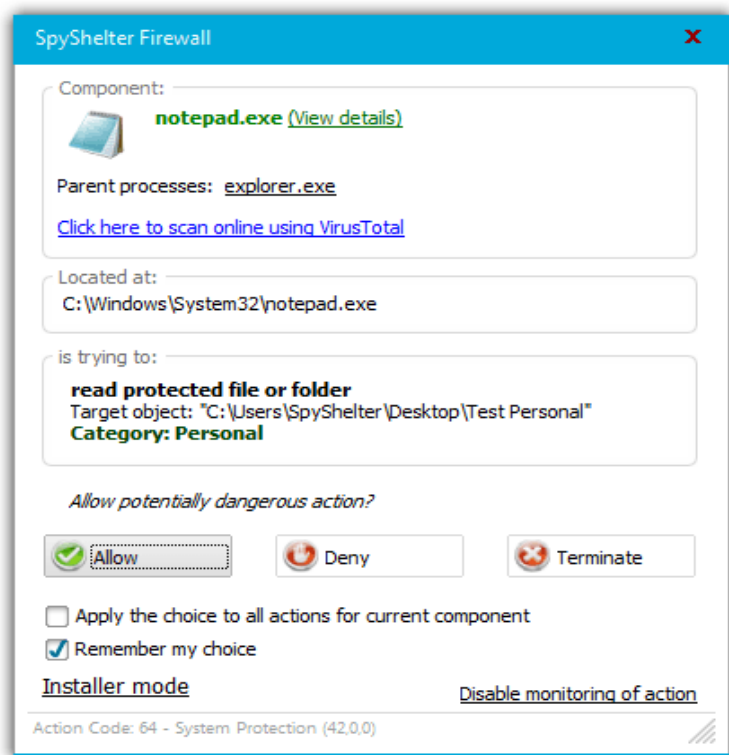


User defined protected files			
Path	Access	Category	
C:\Users\SpyShelter\Desktop\2nd Test General	Read & Write	General	
C:\Users\SpyShelter\Desktop\2nd Test Personal	Read & Write	Personal	
C:\Users\SpyShelter\Desktop\Test General	Read & Write	General	
C:\Users\SpyShelter\Desktop\Test Personal	Read & Write	Personal	

Объясняем, как использовать эту функцию, на примере. У нас есть четыре папки. Для двух из них устанавливается параметр «**Общие**», для двух других «**Личные**».

<

Если пользователь пытается открыть файл .txt из **Общей** папки, появится окно оповещения с сообщением, что Notepad.exe (или любое другое приложение, назначенное для открытия файлов с расширением .txt) пытается получить доступ для чтения этого файла. Если пользователь разрешает это действие, приложение Блокнот немедленно получит доступ ко всем файлам, которые находятся внутри папки **Общей** категории в списке **Защищенных файлов**. >



Если пользователь пытается запустить тот же файл, например, с Open Office, оповещение, показанное выше, появится снова потому, что требуется решение на основе сведений о процессе.

После создания правила для Notepad.exe, которое позволяет выполнение файлов из категории «**Общие**», попытка выполнить txt-файл из папки «**Личной**» категории приведет к появлению другого окна оповещения.

<

User defined protected files		
Path	Access	Category
C:\Users\SPS\Desktop\Test Folder	Read & Write	General
C:\Users\SPS\Desktop\Test Folder\File 1 Personal.txt	Read & Write	Personal

Можно, также, создать папку с доступом на **Чтение&Запись** с **Общей** категорией и затем указать файлы в этой папке с **Личной** категорией.

<

Доступ к файлам из «**Личной**» категории вызовет другое оповещение, с просьбой представить дополнительные разрешения, даже если пользователь выбрал параметр «**Запомнить мой выбор**» для **чтения и записи** для любого файла в папке с категорией «**Общая**».

Советы

Вот список полезных советов для усиления защиты:

- Не позволяйте программам запускаться, если их поведение подозрительное. Когда вы не уверены в программе, рекомендуется сначала заблокировать ее. Если она работает и ваша система остается стабильной, можно удалить это приложение из черного/белого списка и позволить ему работать в вашей системе.

- Не останавливайте программу SpyShelter, когда она блокирует подозрительное поведение.
После того, как общая защита отключена, вредоносное программное обеспечение может установить hooks, которые не могут быть заблокированы, даже, если вы включите защиту позже (для того, чтобы восстановить полную защиту, может потребоваться перезагрузка системы)

- Не доверяйте всем подписанным модулям и проверьте имя подписавшего, чтобы увидеть, какой тип программного обеспечения эта компания производит.



Модули

Модуль AntiKeyLogging

Модуль анти-клавиатурный предназначен для обеспечения защиты от всех клавиатурных шпионов. Информационная безопасность проверяется активно, без необходимости использования базы данных подписей.

Клавиатурный шпионаж может выполняться несколькими различными способами. SpyShelter останавливает все KeyLoggers, независимо от их методов считывания. В дополнение к этому, благодаря его методам проактивной защиты, модуль анти-клавиатурный защитит ваш компьютер от новых (и пока еще неизвестных) угроз.

Реальная защита от кейлоггеров

Кейлоггер - это вредоносное приложение, которое заражает ваш компьютер и регистрирует все действия клавиатуры (клавиш). Каждое нажатие клавиш (информация) сохраняется. Эти записи могут храниться локально внутри вашего компьютера, или даже в отдаленных местах.

Клавиатурные шпионы предназначены для кражи информации высокой стоимости, которую пользователь может разглашать при использовании Интернета (например когда пользователь использует этот вид услуг: интернет магазины, электронную коммерцию, интернет банкинг, рассылки и т.д.) Для устранения этих угроз, особенно для банковских операций в интернете, используется виртуальная клавиатура. Однако, традиционные методы для защиты пользователя от клавиатурных шпионов и их угроз, не достаточны по сравнению с защитой, что может предложить SpyShelter.



Модуль AntiKernelModeLogger

Это уникальный защитный модуль, который защищает вашу систему от кейлоггеров режима ядра.

Клавиатурные шпионы режима ядра работают на уровне драйверов или сервисов и их очень трудно обнаружить с помощью обычного программного обеспечения защиты. SpyShelter был разработан метод защиты против этих серьезных угроз.



Модуль Анти-GetText

Хакеры могут использовать функцию GetText для получения важной информации с вашего компьютера. Этот модуль позволяет предотвратить использование этого метода для захвата конфиденциальных данных с вашего компьютера.



Модуль Анти-Захвата Экрана

Этот модуль защищает вашу систему от захватчиков экрана: это программы, предназначенные для использования функции захвата экрана для кражи ваших данных. Они работают путем регулярного снятия скриншотов рабочего стола для того, чтобы захватить информацию, отображаемую на экране.



Модуль Анти-Захвата Веб-камеры

Захватчики Веб-камеры тайно подключаются к вашей веб-камере. Они делают фотографии и отправляют информацию через Интернет. Многие из этих программ могут работать, даже когда веб-камера активируется незаметно. Эта угроза стала более актуальной в настоящее время, учитывая, что веб-камеры уже встроены в почти каждый современный ноутбук. Подумайте о всей возможной информации, которая может быть собрана через веб-камеры! Информация обо всем, что вы делаете, когда работаете на вашем компьютере, потенциально может быть злонамеренно использована.

Модуль Анти-захвата веб-камеры обеспечивает уникальную проактивную защиту от этой угрозы. Благодаря этой проактивной защите, SpyShelter, также, может защитить вас от неизвестных угроз такого рода.



Модуль Анти-захвата буфера обмена

Буфер обмена — это место, где хранятся данные, когда данные изменяются во время процесса вырезания, копирования и вставки. Программа захвата Буфера Обмена обеспечивает отслеживание информации, содержащейся в буфере обмена. Путем проверки изменений внутри него и контролируя, что хранится в нем, этот тип программного обеспечения имеет возможность захвата данных и отправки его третьим лицам.

Модуль Анти-захвата буфера обмена работает в режиме реального времени: он защищает вас от этих угроз, прежде чем они появятся и в момент появления.

Модуль Анти-захвата буфера обмена, благодаря его мощным методам борьбы с угрозой, повысит уровень информационной безопасности и защитит жизненно важные данные способами, которые никогда не использовались в более традиционном защитном программном обеспечении.

Модуль защиты системы

Ваш компьютер имеет важные системные области, повреждение которых может привести к общей нестабильности системы. Эти области включают реестр операционной системы Windows и физическую память.

Модуль защиты системы SpyShelter — это активный компонент, который защищает важные системные области от любого вредоносного программного обеспечения, которое может нанести вред вашей системе. Когда он защищает вашу систему, он также предотвращает внедрение вредоносных кодов [DLL инъекции] любых вредоносных приложений в надежные компоненты.

Модуль защиты системы SpyShelter оснащен действенным методом, чтобы предотвратить эти случаи. Кроме того, он блокирует вредоносные приложения, которые используют загрузку драйвера ядра: это заражает систему путем установки кода в операционную систему вашего компьютера.

Этот модуль, также, защищает вас от вредоносных приложений, которые могут изменять значения в реестре Windows.

Модуль системной обороны может защитить наиболее важные области вашей системы. Он, также, может предотвратить попытки вредоносных приложений вывести любой модуль SpyShelter из эксплуатации. Это активный метод защиты. Модуль системной обороны не только защитит вас от известных угроз, но, также, защитит вас от неизвестных угроз.

Уникальная Защита Системы от вредоносных программ

Системные Вредоносные Программы атакуют непосредственно вашу операционную систему. Основными методами атаки являются:

- Установка Глобального Hook
- Установка руткита
- Изменение контекстного потока
- Прямой доступ к физической памяти
- Создание удаленного потока
- Инъекция кода в DLL
- Загрузка драйвера ядра
- Изменение состояния программы и памяти
- Изменение критических мест системы и реестра

Если вредонос проникает в вашу систему, это может нанести вред системе. Ваша операционная система может стать нестабильной. Возможно изменение уровня использования системы, что вызовет много нежелательных эффектов в аппаратном обеспечении системы. В итоге, когда операционная система и ее оборудование повреждены, можно потерять ваши ценные данные и вы, также, понесете финансовый ущерб.

Модуль защиты системы SpyShelter предназначен для защиты от вредоносных программ, благодаря его методу проактивной защиты.



Модуль Анти-звукозапись

Это уникальный защитный модуль, который защищает вашу систему от троянов записи звука VOIP. Это может быть полезно при использовании мгновенных сообщений, для голосовых звонков. Троянские рекордеры Веб-камеры могут попытаться сохранить голосовые данные из вашего встроенного или внешнего микрофона. Этот модуль даст вам лучшую защиту против такого рода угрозы.



Модуль Сетевой Анти-шпион

SpyShelter Сетевой Анти-шпион проактивный модуль предотвращает кражи вашей личной информации во время важных SSL Интернет-транзакций. Он блокирует протоколирования HTTP/HTTPS и также POP, SMTP, FTP и другие средства записи опасных троянов.



Модуль брандмауэра

Модуль брандмауэра SpyShelter предназначен для управления (разрешить или запретить) сетевыми передачами на основе набора правил.

Обычно он используется для защиты системы компьютера от несанкционированного доступа из/к сети, разрешая надежные пакеты для передачи.

SpyShelter брандмауэр поддерживает протокол IPv6.

SPYSHELTER ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ КОНЕЧНОГО ПОЛЬЗОВАТЕЛЯ

УВЕДОМЛЕНИЯ:

ПРАВОВАЯ ИНФОРМАЦИЯ: ВНИМАТЕЛЬНО ПРОЧИТАЙТЕ СЛЕДУЮЩЕЕ ЮРИДИЧЕСКОЕ СОГЛАШЕНИЕ ПЕРЕД УСТАНОВКОЙ И НАЧАЛОМ ИСПОЛЬЗОВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ.

ЭТО ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ КОНЕЧНОГО ПОЛЬЗОВАТЕЛЯ (EULA)-ЭТО ЮРИДИЧЕСКОЕ СОГЛАШЕНИЕ МЕЖДУ ВАМИ (КОНЕЧНЫМ ПОЛЬЗОВАТЕЛЕМ) И АВТОРОМ SPYSHELTER. ВЫ СОГЛАШАЕТЕСЬ БЫТЬ АВТОМАТИЧЕСКИ СВЯЗАННЫМИ, ТАКИМ ОБРАЗОМ, С УСЛОВИЯМИ НАСТОЯЩЕГО ЛИЦЕНЗИОННОГО ДОГОВОРА, КАК ТОЛЬКО ВЫ УСТАНОВИТЕ ЭТУ ПРОГРАММУ.

ЕСЛИ ВЫ НЕ СОГЛАСНЫ С ЛЮБЫМ ИЗ ПОЛОЖЕНИЙ, СОДЕРЖАЩИХСЯ В НАСТОЯЩЕМ ДОКУМЕНТЕ, ПОЖАЛУЙСТА, НЕ УСТАНАВЛИВАЙТЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И НЕ НАЖИМАЙТЕ НА КНОПКУ, КОТОРАЯ ПОКАЗЫВАЕТ ВАШЕ ЖЕЛАНИЕ СОБЛЮДАТЬ УСЛОВИЯ НАСТОЯЩЕГО КОНТРАКТА.

1. DEFINITIONS

- 1.1. "SOFTWARE", "PROGRAM", "PRODUCT", "SPYSHELTER" REFERS TO SPYSHELTER PREMIUM AND SPYSHELTER FIREWALL SOFTWARE.
- 1.2. "USER", "END-USER", "YOU", MEANS A PERSON/ORGANIZATION WHO INSTALLS AND/OR USES OUR SOFTWARE.
- 1.3. "COMPUTER", "PC" MEANS A DEVICE LIKE PERSONAL COMPUTER, LAPTOP OR A WORKSTATION WHICH CAN BE USED TO RUN OUR SOFTWARE.
- 1.4. "OWNER", "PRODUCER", "DEVELOPER" MEANS DATPOL, JANUSZ SIEMIENOWICZ - A COMPANY LOCATED IN POLAND, DEVELOPER OF SPYSHELTER.

2. TRIAL VERSION AND ACTIVATING SOFTWARE

SPYSHELTER FIREWALL AND SPYSHELTER PREMIUM PROGRAMS ARE DISTRIBUTED AS TRIAL VERSIONS. THE PROGRAMS HAVE ALL FEATURES UNLOCKED FOR 14 DAYS FROM THE MOMENT YOU INSTALL IT. TO USE SPYSHELTER BEYOND TRIAL PERIOD, YOU MUST ENTER A VALID LICENSE KEY WHICH WILL TURN YOUR TRIAL VERSION INTO A FULL VERSION.

SPYSHELTER FREE ANTI-KEYLOGGER IS A FREE VERSION OF THE PROGRAM. DEVELOPER GRANTS YOU A NON-EXCLUSIVE LICENSE TO USE THE SPYSHELTER FREE ANTI-KEYLOGGER FOR 1 YEAR SINCE THE DATE OF RELEASE. THIS SOFTWARE CAN BE USED ON BOTH HOME COMPUTERS AS WELL AS BUSINESS OR INSTITUTIONAL DEVICES.

3. LICENSING

LICENSES CAN BE ACQUIRED AT <https://www.spyshelter.com/purchase> OR FROM AUTHORIZED SPYSHELTER RESELLER.

IF YOU HAVE PURCHASED A ONE-YEAR LICENSE FOR THE PRODUCT, THE PRODUCT SHALL FUNCTION WITHIN THE SAME PERIOD AND SHALL AUTOMATICALLY STOP FUNCTIONING AFTER THIS TIME (EXACTLY ONE YEAR AFTER PURCHASING). AN LICENSE THAT IS VALID FOR AN INDEFINITE PERIOD OF TIME MAY ALSO BE PURCHASED.

SPYSHELTER DEVELOPER GRANTS YOU THE FOLLOWING RIGHTS PROVIDED THAT YOU COMPLY WITH ALL TERMS AND CONDITIONS OF THIS EULA. YOU ARE ALLOWED TO:

A. USE ONE COPY OF THE SPECIFIC VERSION OF THE SOFTWARE AND ITS ACCOMPANYING DOCUMENTS THAT YOU PURCHASED AND ENJOY THIS RIGHT AS A NONTRANSFERABLE AND EXCLUSIVE RIGHT. IF YOU PURCHASED THIS PRODUCT AS PART OF A SET OF SOFTWARE, YOU ARE ALSO BOUND BY THE TERMS OF THE LICENSES FOR THOSE OTHER PRODUCTS IN THE SET, IF SO INDICATED IN THEIR RESPECTIVE EULA. THIS SOFTWARE, UNLESS YOUR LICENSE INDICATES OTHERWISE, MAY NOT BE USED ON MORE THAN ONE DEVICE.

B. INSTALL THIS SOFTWARE TO YOUR COMPUTER OR TO ANY OTHER COMPATIBLE DEVICE FOR WHICH THIS PRODUCT HAS BEEN CREATED.

C. COPY YOUR LICENSE CODE ONCE BUT ONLY FOR THE PERSONAL AND LEGAL PURPOSE OF CREATING A BACK-UP. YOU ARE RESPONSIBLE FOR ENSURING THAT YOUR LICENSE CODE WILL NOT BE COPIED OR REPRODUCED FOR ANY OTHER PURPOSE AND BY ANY OTHER PERSON.

D. ASK FOR A FULL REFUND UP TO 14 DAYS AFTER PLACING INITIAL ORDER. AFTER THIS PERIOD, MONEY WILL NOT BE REFUNDED.

PURSUANT TO YOUR LICENSE, YOU HAVE THE FOLLOWING ADDITIONAL DUTIES:

A. UNINSTALL THE SOFTWARE SHOULD YOU DECIDE TO DISPOSE OF THE DEVICE THAT CONTAINS THE SOFTWARE IN ORDER TO PREVENT UNAUTHORIZED COPYING, DISTRIBUTION, REPRODUCTION, AND OTHER RELATED ACTS.

B. YOU MUST NOT TRANSFORM OR ALTER ANY PART OF THIS SOFTWARE [E.G. TRANSFORM FROM SOURCE TO CODE, REVERSE ENGINEERING, PULLING UP, MAKING IT READABLE IN DIFFERENT FORMS].

C. YOUR LICENSE TO THIS SOFTWARE DOES NOT, IN ANY WAY, ALLOW YOU TO CREATE DERIVATIVE WORKS FROM THIS SOFTWARE. NEITHER ARE YOU AUTHORIZED TO ALLOW A THIRD PARTY TO MAKE COPIES OF THE PRODUCT. ACTIVITIES RELATED TO THIS PURPOSE SUCH AS CORRECTION OF MISTAKES, OTHER TYPES OF MODIFICATION, ADAPTATION AND TRANSLATION ARE ALSO NOT ALLOWED UNDER THIS AGREEMENT

D. THIS LICENSE PROHIBITS YOU FROM LEASING, LENDING, OR TRANSFERRING YOUR LICENSE RIGHTS TO ANY THIRD PARTY OR THE GRANTING OF A LICENSE TO SUCH THIRD PARTY. IF YOUR LICENSE CODE LEAKS INTO THE INTERNET, OR WILL BE USED ON MORE PC'S THAN IT IS ALLOWED, WE MIGHT BLOCK YOUR LICENSE CODE WITHOUT WARNING.

E. SPYSHELTER REQUIRES ITS USERS TO INSTALL THE SOFTWARE'S LATEST VERSION AND THE CORRESPONDING LATEST MAINTENANCE PACK THEREOF.

YOU, HOWEVER, MUST NOTE THAT IF YOU PURCHASED THE PRODUCT FROM A VENDOR OTHER THAN SPYSHELTER, THE LATTER IS AND SHALL NOT BE LIABLE FOR WARRANTIES AND GUARANTEES MADE BY THAT VENDOR IN RELATION TO THE PRODUCT, UNLESS A SPECIFIC AGREEMENT ON THESE MATTERS HAVE BEEN MADE BETWEEN THIS VENDOR AND SPYSHELTER.

4. SUPPORT

SPYSHELTER AGREES TO PROVIDE TECHNICAL SUPPORT AND FREE UPDATES FOR AS LONG AS IT REMAINS IN LEGAL EXISTENCE AND WITHIN THE DURATION OF THE LICENSES THAT YOU PURCHASED.

USE SUPPORT TICKET SYSTEM LOCATED AT <https://www.spysshelter.com/helpdesk> IN ORDER TO GET PRODUCT SUPPORT.

SUPPORT SERVICES INCLUDE SUPPORT VIA SUPPORT TICKET SYSTEM OF THE DEVELOPER. IN ORDER TO GET TECHNICAL SUPPORT, YOU ARE REQUIRED TO HAVE THE LATEST VERSION OF THE SOFTWARE (INCLUDING ITS MAINTENANCE PACK).

SPYSHELTER SUPPORT WILL REPLY TO MESSAGE IN 72 HOURS FROM THE MOMENT OF CREATING A SUPPORT TICKET. SPYSHELTERS RESERVES THE RIGHT TO EXTEND THE TIME TO REPLY IN SPECIAL CASES. PRODUCER HOLDS NO RESPONSIBILITY FOR A TICKET ANSWER THAT IS NOT DELIVERED TO THE USER VIA E-MAIL.

PRODUCER WILL NOT REPLY TO MESSAGES THAT DO NOT CONCERN SPYSHELTER PRODUCTS.

PRODUCER CAN DENY PROVIDING INFORMATIONS IN ORDER TO PRESERVE THE CONFIDENTIALITY OF COMMERCIAL SENSITIVE DATA AND INFORMATION.

PRODUCER DOES NOT GUARANTEE TECH SUPPORT FOR SPYSHELTER FREE USERS.

5. PRIVACY

DEVELOPER COLLECTS PERSONAL INFORMATION OF LICENSED USERS IN ORDER TO KEEP TRACK OF SALES RECORDS, AND PROVIDE NECESSARY SERVICES LIKE RESENDING LOST LICENSE KEY. those informations are gathered from share-it(digital river gmbh), developer's payment processor who records and stores your payment informations. you can view digital river gmbh privacy policy at <http://www.mycommerce.com/privacy-policy>

spysshelter privacy policy is available here: <https://www.spysshelter.com/privacy>

6. PROPERTY RIGHTS

THIS SOFTWARE IS PROTECTED BY INTELLECTUAL PROPERTY LAWS. SPYSHELTER CREATOR THUS OWNS ALL RIGHTS, PROPERTIES, AND OTHER INTERESTS OVER THIS SOFTWARE. ACCORDING TO LAW, SPYSHELTER OWNS THE COPYRIGHTS, PATENTS, TRADEMARKS, AND OTHER RELATED INTELLECTUAL PROPERTY RIGHTS OF THIS PRODUCT AND THE USER'S UTILIZATION AND INSTALLATION OF THIS PRODUCT DOES NOT, IN ANY WAY, TRANSFER THE RIGHTS JUST MENTIONED TO THE USER. ONLY THOSE RIGHTS EXTENDED IN THIS EULA ARE TRANSFERRED TO THE USER.

-YOU MAY NOT USE THIS PROGRAM IN ACTIONS, WHICH INFRINGE ANY LAW OF YOUR COUNTRY OR INTERNATIONAL LAWS.

-YOU MAY NOT USE THIS PROGRAM IN ACTIONS, WHICH INFRINGE THE RIGHTS OF ANY PERSON OR ENTITY.

-YOU MAY NOT DISASSEMBLE AND REVERSE ENGINEER ANY PART OF THIS PROGRAM

-YOU MAY NOT RENT, LEASE OR SELL THIS PROGRAM.

7. CONFIDENTIALITY

THIS SOFTWARE, ITS MAINTENANCE PACKS, THE SPECIAL DESIGN AND STRUCTURE OF THE INDIVIDUAL PROGRAMS, THE LICENSE KEY, AND THE RELATED DOCUMENTS ARE COVERED BY THIS CONFIDENTIALITY CLAUSE. WITHOUT THE PRIOR CONSENT OF SPYSHELTER, YOU ARE UNAUTHORIZED TO DISCLOSE OR DISPOSE ANY CONFIDENTIAL INFORMATION TO A THIRD PARTY. YOU ARE REQUIRED TO USE REASONABLE SECURITY MEASURES TO PROTECT CONFIDENTIAL INFORMATION RECEIVED BY VIRTUE OF YOUR PURCHASE OF THIS PRODUCT.

8. WARRANTY

NO WARRANTY, AND LIMITED REPLACEMENT: THE SOFTWARE IS PROVIDED "AS IS" WITH NO WARRANTIES, EXPRESS OR IMPLIED. SPECIFICALLY DISCLAIMS ANY AND ALL WARRANTIES, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION, OR SAMPLE. IF THE MEDIA ON WHICH THE SOFTWARE IS DISTRIBUTED ARE FOUND TO BE DEFECTIVE IN MATERIAL OR WORKMANSHIP UNDER NORMAL USE FOR A PERIOD OF NINETY (90) DAYS FROM THE DATE OF RECEIPT, DEVELOPER'S ENTIRE LIABILITY AND YOUR EXCLUSIVE REMEDY SHALL BE THE REPLACEMENT OF THE MEDIA BY AUTHORIZED RESELLER FROM WHOM YOU BOUGHT THE PRODUCT. THIS OFFER IS VOID IF THE MEDIA DEFECT RESULTS FROM ACCIDENT, ABUSE, OR MISAPPLICATION



9. LIMITATION OF LIABILITY.

IN NO EVENT SHALL SPYSHELTER DEVELOPER AND DISTRIBUTORS/PARTNERS BE RESPONSIBLE FOR ANY INDIRECT, CONSEQUENTIAL OR SPECIAL DAMAGES OR LOST PROFITS EVEN IF SPYSHELTER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND/OR FOR ANY CLAIM FOR COMPENSATION OR DAMAGE BY ANY THIRD PARTY TO USER. . LIABILITY ON THE PART OF SPYSHELTER AND ITS AUTHORIZED REPRESENTATIONS/DEALERS SHALL ALSO NOT EXSIT IN CASE THERE IS: LOSS OF INCOME OR PROFITS, LOSS OF SAVINGS, LOSS OF OPPORTUNITY, LOSS OF HONOR, LOSS, DAMAGE OR HARM OF SENSITIVE DATA.

DISPUTES ARISING FROM THIS AGREEMENT SHALL BE RESOLVED IN THE PROPER COURTS OF POLAND.THIS AGREEMENT IS VALID AND BINDING BETWEEN SPYSHELTER AND THE USER. NO TERMS AND PROVISIONS OUTSIDE OF THIS AGREEMENT SHALL BE VALID AND BINDING BETWEEN THESE PARTIES.

IF YOU DO NOT WISH TO BE BOUND BY THIS EULA AND FALL UNDER THE CONDITIONS/CLASSIFICATIONS FOUND BELOW, PLEASE NOTE:

FOR USERS WHO PURCHASED THE SOFTWARE FROM VENDORS OTHER THAN SPYSHELTER: PLEASE RETURN THE PRODUCT TO YOUR VENDOR, WITH ITS CD COVER INTACT AND UNALTERED IN ANY MANNER. FAILURE TO PRESERVE THE PRODUCT AND ITS COVER IN ITS ORIGINAL STATE WILL RESULT TO YOU BEING CONTINUOUSLY BOUND BY THE TERMS OF THIS EULA.

DATPOL

K.K. WIELKIEGO 29

OLKUSZ, POLAND

REGON: 120012823

TAX VAT ID PL637-192-90-41

Contact: <https://www.spyshelter.com/about-us>

(Kumga - <http://forum.ru-board.com/>)