# *Антивирусная утилита AVZ*


*Антивирусная утилита AVZ предназначена для обнаружения и удаления:*
*SpyWare и AdWare модулей - это основное назначение утилиты*
*Dialer (Trojan.Dialer)*
*Троянских программ*
*BackDoor модулей*
*Сетевых и почтовых червей*
*TrojanSpy, TrojanDownloader, TrojanDropper*
*Утилита является прямым аналогом программ TrojanHunter и LavaSoft Ad-aware 6.*

*Первичной задачей программы является удаление SpyWare и троянских программ.*
*Особенностями утилиты AVZ (помимо типового сигнатурного сканера) является:*
*Микропрограммы эвристической проверки системы. Микропрограммы проводят поиск известных SpyWare и вирусов по косвенным признакам - на основании анализа реестра, файлов на диске и в памяти.*

*Обновляемая база безопасных файлов. В нее входят цифровые подписи десятков тысяч системных файлов и файлов известных безопасных процессов. База подключена ко всем системам AVZ и работает по принципу "свой/чужой" - безопасные файлы не вносятся в карантин, для них заблокировано удаление и вывод предупреждений, база используется антируткитом, системой поиска файлов, различными анализаторами. В частности, встроенный диспетчер процессов выделяет безопасные процессы и сервисы цветом, поиск файлов на диске может исключать из поиска известные файлы (что очень полезно при поиске на диске троянских программ);*

Встроенная система обнаружения Rootkit. Поиск RootKit идет без применения сигнатур на основании исследования базовых системных библиотек на предмет перехвата их функций. AVZ может не только обнаруживать RootKit, но и производить корректную блокировку работы UserMode RootKit для своего процесса и KernelMode RootKit на уровне системы. Противодействие RootKit распространяется на все сервисные функции AVZ, в результате сканер AVZ может обнаруживать маскируемые процессы, система поиска в реестре "видит" маскируемые ключи и т.п. Антируткит снабжен анализатором, который проводит обнаружение процессов и сервисов, маскируемых RootKit. Одной из главных на мой взгляд особенностей системы противодействия RootKit является ее работоспособность в Win9X (распространеннное мнение об отсуствии RootKit, работающих на платформе Win9X глубоко ошибочно - известны сотни троянских программ, перехватывающих API функции для маскировки своего присутствия, для искажения работы API функций или слежения за их использованием). Другой особенностью является универсальная система обнаружения и блокирования KernelMode RootKit, работоспособная под Windows NT, Windows 2000 pro/server, XP, XP SP1, XP SP2, Windows 2003 Server, Windows 2003 Server SP1
Детектор клавиатурных шпионов (Keylogger) и троянских DLL. Поиск Keylogger и троянских DLL ведется на основании анализа системы без применения базы сигнатур, что позволяет достаточно уверенно детектировать заранее неизвестные троянские DLL и Keylogger;

Нейроанализатор. Помино сигнатурного анализатора AVZ содержит нейроэмулятор, который позволяет производить исследование подозрительных файлов при помощи нейросети. В настоящее время нейросеть применяется в детекторе кейлоггеров.
Встроенный анализатор Winsock SPI/LSP настроек. Позволяет проанализировать настройки, диагностировать возможные ошибки в настройке и произвести автоматическое лечение. Возможность автоматической диагностики и лечения полезна для начинающих пользователей (в утилитах типа LSPFix автоматическое лечение отсутствует). Для исследования SPI/LSP вручную в программе имеется специальный менеджер настроек LSP/SPI. На работу анализатора Winsock SPI/LSP распространяется действие антируткита;
Встроенный диспетчер процессов, сервисов и драйверов. Предназначен для изучения запущенных процессов и загруженных библиотек, запущенных сервисов и драйверов. На работу диспетчера процессов распространяется действие антируткита (как следствие - он "видит" маскируемые руткитом процессы). Диспетчер процессов связан с базой безопасных файлов AVZ, опознанные безопасные и системные файлы выделяются цветом;
Встроенная утилита для поиска файлов на диске. Позволяет искать файл по различным критериям, возможности системы поиска превосходят возможности системного поиска. На работу системы поиска распространяется действие антируткита (как следствие - поиск "видит" маскируемые руткитом файлы и может удалить их), фильтр позволяет исключать из результатов поиска файлы, опознанные AVZ как безопасные. Результаты поиска доступны в виде текстового протокола и в виде таблицы, в которой можно пометить группу файлов для последующего удаления или помещения в карантин
Встроенная утилита для поиска данных в реестре. Позволяет искать ключи и параметры по заданному образцу, результаты поиска доступны в виде текстового протокола и в виде таблицы, в которой можно отметить несколько ключей для их экспорта или удаления. На работу системы поиска распространяется действие антируткита (как следствие - поиск "видит" маскируемые руткитом ключи реестра и может удалить их)
Встроенный анализатор открытых портов TCP/UDP. На него распространяется действие антируткита, в Windows XP для каждого порта отображается использующий порт процесс. Анализатор опирается на обновляемую базу портов известных троянских/Backdoor программ и известных системных сервисов. Поиск портов троянских программ включен в основной алгоритм проверки системы - при обнаружении подозрительных портов в протокол выводятся предупреждения с указанием, каким троянских программам свойственно использование данного порта
Встроенный анализатор общих ресурсов, сетевых сеансов и открытых по сети файлов. Работает в Win9X и в Nt/W2K/XP.
Встроенный анализатор Downloaded Program Files (DPF) - отображает элементы DPF, подключен ко всем сситемам AVZ.
Микропрограммы восстановления системы. Микропрограммы проводят восстановления настроек Internet Explorer, параметров запуска программ и иные системные параметры, повреждаемые вредоносными программами. Восстановление запускается вручную, восстанавливаемые параметры указываются пользователем.
Эвристическое удаление файлов. Суть его состоит в том, что если в ходе лечения удалялись вредоносные файлы и включена эта опция, то производится автоматическое исследование системы, охватывающее классы, BHO, расширения IE и Explorer, все

доступные AVZ виды автозапуска, Winlogon, SPI/LSP и т.п. Все найденные ссылки на удаленный файл автоматически вычищаются с занесением в протокол информации о том, что конкретно и где было вычищено. Для этой чистки активно применяется движок микропрограмм лечения системы;
Проверка архивов. Начиная с версии 3.60 AVZ поддерживает проверку архивов и составных файлов. На настоящий момент проверяются архивы формата ZIP, RAR, CAB, GZIP, TAR; письма электронной почты и MHT файлы; CHM архивы
Проверка и лечение потоков NTFS. Проверка NTFS потоков включена в AVZ начиная с версии 3.75
Скрипты управления. Позволяют администратору написать скрипт, выполняющий на ПК пользователя набор заданных операций. Скрипты позволяют применять AVZ в корпоративной сети, включая его запуск в ходе загрузки системы.
Анализатор процессов. Анализатор использует нейросети и микропрограммы анализа, он включается при включении расширенного анализа на максимальном уровне эвристики и предназначен для поиска подозрительных процессов в памяти.
Система AVZGuard. Предназначена для борьбы с трудноудалимыми вредоносными програмами, может кроме AVZ защищать указанные пользователем приложения, например, другие антишпионские и антивирусные программы.
Система прямого доступа к диску для работы с заблокированными файлами. Работает на FAT16/FAT32/NTFS, поддерживается на всех операционных системах линейки NT, позволяет сканеру анализировать заблокированные файлы и помещать их в карантин.
Драйвер мониторинга процессов и драйверов AVZPM. Предназначен для отслеживания запуска и остановки процессов и загрузки/выгрузки драйверов для поиска маскирующихся драйверов и обнаружения искажений в описывающих процессы и драйверы структурах, создаваемых DKOM руткитами.
Драйвер Boot Cleaner. Предназначен для выполнения чистки системы (удаление файлов, драйверов и служб, ключей реестра) из KernelMode. Операция чистки может выполняться как в процессе перезагрузки компьютера, так и в ходе лечения.