AVZ и uVS – братья, но не близнецы.

(сравнительный анализ, update от 2021_12_31)

AVZ, **uVS**, прежде всего – две замечательные антивирусные утилиты российских программистов **Зайцева Олега (http://z-oleg.com)**, **Кузнецова Дмитрия (http://dsrt.dyndns.org/)** обладают уникальным функционалом, который позволяет в большинстве случаев оперативно излечивать зараженные системы.

AVZ развивается достаточно давно (собственно, на наших глазах), с 2004 г. За это время эволюционировал от быстро сканирующей утилиты, к комплексной программе с менеджерами процессов, служб и драйверов, автозапуска и др., с подсистемами ограничения активности приложений, расширенного мониторинга процессов, антируткитом, ревизором, подсистемами исследования, восстановления, мастером поиска и устранения проблем. Широко применяется специалистами по ИТ-безопасности, и просто опытными пользователями.

uVS - менее известная программа, разрабатывается с 2009г, с оригинальной и неповторимой методикой, предназначена для ИТ специалистов, и возможно, будет более сложна для пользователей без достаточных знаний о Windows. *Функции поддержки (создания и импорта) пользовательских списков безопасных, известных файлов, сигнатур, белых ЭЦП, критериев поиска вредоносных программ (простых и составных условий с логикой И, ИЛИ, НЕ) позволяют исследователю создать свой мини - вирлаб, интегрировать личные списки и базы в общие в интересах ИТ-сообщества. Механизм авто_скрипта, развиваемый в uVS, сокращает время, затрачиваемое на анализ зараженной системы и написание рабочего скрипта до разумного минимума.*

интерфейс		
графический интерфейс	да	да
вызов командной строки	да	да
Управление удаленным рабочим столом в локальной сети	нет	да
Автоматическое создание загрузочного диска Winpe с добавлением списка необходимых программ / создание Live.CD на базе Winpe51 с поддержкой проверки внешних ЭЦП (по CatRoot)	нет	да
поддержка запуска внешних утилит	да	да
поддержка списков безопасных, известных файлов, сигнатур файлов, нежелательных файлов, критериев поиска вредоносных программ		
поддержка списка безопасных файлов	да	да
поддержка списка известных файлов	нет	да
поддержка списка белых цифровых подписей (ЭЦП)	нет	да
поддержка списка нежелательных файлов	нет	да
проверка цифровых подписей файлов	да	да
поддержка сигнатур вирусных файлов	да	да
автообновление списков, сигнатур	да	да
Импорт списков, сигнатур из внешних файлов	нет	да
поддержка списков, сигнатур, создаваемых пользователем	нет	да
поддержка списка критериев поиска вредоносных программ (простых и составных с логикой И, ИЛИ, НЕ)	нет	да
Авто_извлечение сигнатур файлов, в том числе из загрузчиков в MBR/VBR/IPL	нет	да
поддержка вычисления md5	Да	да
поддержка вычисления sha1	Да	да
Обзор списка установленных программ/оборудования/	нет	да
поддержка деинсталляции программ	нет	да
поддержка расширенного инфо о подозрительных файлах	нет	да
режимы запуска утилиты		
исследование активной системы	да	да
исследование пассивной системы	нет	да
исследование удаленной системы (в локальной сети)	нет	да
Выбор учетной записи для исследования системы	нет	да
запуск в безопасном режиме	да	да
запуск с live.cd	нет	да

uVS прост и удобен в работе. Практически все режимы работы программы унифицированы, с минимумом окон. Ядро **uVS** запускается через стартовое меню (start.exe или startf.exe) из которого можно выбрать режим работы: с активной, пассивной, удаленной (в локальной сети) системами, запуск ядра утилиты (с автоматически произвольным именем) с различными правами (админ, LocalSystem, текущий пользователь), с выбором учетной записи в системе, с возможностью_попыткой выгрузки потенциально нежелательных программ, с проверкой ограниченного или полного списка автозапуска по цифровым подписям. После загрузки основного модуля программы список автозапуска уже создан и проанализирован по списку безопасных sha1, по пользовательской базе сигнатур, по списку критериев поиска. Дополнительный анализ отдельного файла/группы файлов (например, категории – «подозрительные») по **глобальной базе** Virustotal, Virusscan.jotti на порядок увеличивает достоверность принятия решения хелпером по тому или иному файлу.

AVZ (нормальная и полиморфная версии**)** состоит из монолитного модуля + драйвера**,** с расширенной системой баз, работает лишь с активной системой, с правами текущего пользователя, автоматически после загрузки avz.exe до сканирования не выполняет еще никаких действий.

создание образа автозапуска		
создание образа автозапуска для последующего анализа	да	да
Автоархивация образа автозапуска, независимо от установленного архиватора.	нет	да
анализ и фильтрация автозапуска системы		
анализ активной зараженной системы	да	да
анализ активной удаленной в локальной сети системы	нет	да
анализ пассивной зараженной системы (по образу автозапуска)	нет	да
анализ пассивной зараженной системы с Live.CD	нет	да
механизм сравнения автозапуска активной и пассивной системы	нет	да
механизм сравнения различных образов автозапуска (отдельная утилита)	нет	да
Механизм сравнения текущего образа автозапуска по файлу сверки	нет	да
поиск и сортировки в списке объектов автозапуска	нет	да
анализ группы_категории файлов по глобальной базе Virustotal.com, Virusscan.jotti.org	нет	да
Поддержка поиска файлов на SystemExplorer.net, runscanner.net	нет	да
Поддержка сервиса whois для поиска dns-серверов по ip-адресу	нет	да
Автоматический анализ системы с помощью списка сложных критериев, создаваемых пользователем, поддержка логики И, ИЛИ, НЕ	нет	да
поддержка фильтров анализа автозапуска	нет	да

образ автозапуска в **uVS** (автоматически архивируется в файл (независимо от установленного архиватора) с уникальным именем), как правило, содержит всю необходимую инфо для анализа, в том числе и для извлечения сигнатур подозрительных и вредоносных файлов, для создания набора критериев поиска вирусов и для поиска инфо на сервисах VirusTotal, Virusscan.

Для чтения логов **AVZ** (virusinfo_syscure.zip, virusinfo_syscheck.zip) и формирования скрипта используется браузер с поддержкой javascript. Дополнительно, для принятия решения хелперу и необходим карантин файлов с последующей проверкой на антивирусных сервисах. Разработчику необходим карантин для изготовления сигнатур. Для извлечения сигнатур, очевидно, используются третьи средства.

По структуре образ автозапуска в **uVS,** удачнее и полнее чем html-лог **AVZ**, поскольку файл образа открывается самой утилиткой **uVS**, и для его анализа и фильтрации используется вся мощь интерфейса – фильтры (процессы, сервисы, драйвера, модули, подозрительные файлы и др.), (фильтрующий) поиск, проверка по спискам безопасных, по каталогу безопасности Windows, по базе сигнатур, поиск инфо по sha1, информация о проверке цифровых подписей, фильтры по дате создания файла и др.

В **AVZ** интерфейс программы для анализа системы можно использовать на активной системе, при просмотре же лога исследуемой системы (html-лог) для анализа хелпер использует лишь возможности браузера по отображению инфо о подозрительных файлах. (или дополнительные парсеры) Т.е. это (html-лог) действительно, более лог автозапуска, нежели его образ.

режим ограничения работы нежелательных приложений		
режим ограничения активности вредоносных приложений	да	нет
антируткит	да	нет
антисплайсинг, выгрузка нежелательных приложений	нет	да
запрет на повторный запуск небезопасных приложений	нет	да
виртуализация реестра	нет	да
изменить статус приложения в автозапуске	нет	да

Для активного противодействия вредоносным программам в uVS используется анти-сплайсинг, выгрузка нежелательных программ в процессе запуска **uVS (startf)**, блокирование повторного запуска зловредов, виртуализация реестра, изменение статуса исполняемого модуля. Согласно документации, "*дополнительный стартер - StartF.exe обладает иммунитетом к некоторым видам троянов, блокирующих запуск любых процессов и соотв. способен запуститься, когда запуск других приложений невозможен. При запуске он блокирует: внедрение библиотек с помощью реестра в запускаемый процесс; запуск и перезапуск служб; выгружает все неизвестные процессы, разрешает запуск редактора реестра и диспетчера задач, после чего запускает start.exe с ключом /d на (чистом рабочем столе), что практически полностью исключает внедрение в uvs посторонних DLL".(с), Кузнецов Д.*

Для удаления из активной системы вредоносных программ с элементами самозащиты можно применить режим (безопасной) виртуализации реестра + актуализация.

Еще более эффективен для борьбы трудноудаляемыми файлами, с руткитами режим исследования пассивной зараженной системы (например, с использованием запуска с Live.CD) и сверки с автозапуском активной системы.

В **AVZ** режим антируткита, avzguard (ограничения активности приложений), boot cleaner ("*технология Boot Cleaner основана на KernelMode Boot драйвере, который выполняет заданную последовательность операций в момент загрузки системы. После выполнения заданных операций драйвер автоматически самоуничтожается. Основное назначение - борьба с трудноудаляемыми вредоносными программами, пересоздающими свои ключи реестра и файлы, или блокирующие доступ к ним….Boot Cleaner размещен в AV базе и обновляется в ходе автоматического обновления", © Зайцев О.*) позволяет эффективно удалять вредоносные программы **лишь из активной системы**.

Сканер		
Использование сигнатур вредоносных программ	да	да
поддержка поиска альтернативных потоков	да	да
проверка файлов автозапуска по спискам, сигнатурам	да	да
Сканер (cleaner), с возможностью удаления обнаруженных вредоносных программ	да	да
режим отложенного удаления		
отложенное удаление файлов	да	да
режим поддержки скриптов		
поддержка скриптового языка	да	да
внешний редактор скриптов	да	нет
автогенерация команд скрипта при работе с образом	да	да
Автогенерация скрипта при работе с активной системой	нет	да
Режим тестирования скрипта	нет	да

автоскрипт	нет	да
ведение карантина		
добавить в карантин	да	да
автоархивировать карантин	да	да

Режим сканирования в **uVS** гибче: мы можем проверить по базе сигнатур файлы из образа автозапуска, а так же выбранный каталог (системы) пользователя из диалога (т.е. провести альтернативное сканирование), **AVZ** при сканировании дополнительно выполняет расширенный набор операций: поиск руткитов и перехватчиков функций API в в UserMode, KernelMode, проверяет процессы, Winsock, включает поиск маскировки процессов и драйверов, поиск перехватчиков событий, открытых портов, уязвимостей и мастер обнаружения неисправностей и проблем, что опять же применимо только на активной системе.

Базу сигнатур в **uVS** хелпер может самостоятельно пополнять как из образа автозапуска, так и из ранее обнаруженных вредоносных исполняемых программ. «*uVS имеет уникальную способность самостоятельно извлекать сигнатуры из исполняемых модулей и затем находить все их копии и моды. Пользователь (хелпер) может внести сигнатуру в базу и последовательно, а главное быстро залечить набор компьютеров пораженных одинаковым набором вирусов. Единственное, что задает пользователь - это длина сигнатуры и ее имя. Длина фактически есть чувствительность поискового движка - чем больше длина, тем меньше вероятность случайного совпадения сигнатур и соотв. меньше вероятность ошибки.» (с), Кузнецов Д.*

в **AVZ** добавить сигнатуры в базы может лишь разработчик, для чего пользователям необходимо карантинить подозрительные и вредоносные файлы.

В версии 3.76 uVS улучшен механизм анализа автозапуска с помощью списка критериев, создаваемых пользователем. **Поддерживаются сложные критерии**, составляемые из нескольких простых условий. Условия могут быть объединены с помощью логических операндов «И», «ИЛИ», «НЕ».

Набор скриптовых команд в **uVS** минимален и достаточен. Скрипт создается в активном режиме и при работе с образом автозапуска. На сегодня список скриптовых команд позволяет качественно выполнить лечение зараженной системы. Необходимость внешнего редактора скриптов отсутствует поскольку написание скрипта тесно связано с анализом текущего образа автозапуска. Следует обратить внимание на команду EXEC, которая через cmd /c выполняет внутренние команды системы, в том числе с использованием сокращенных путей к файлам (%SYSTEMDRIVE%, %SYSTEMROOT%, %SYS32%), деинсталляцию нежелательных программ из списка программ. В uVS развивается механизм автоскрипта, который позволяет автоматически (после загрузки образа автозапуска) создавать отдельные команды для рабочего скрипта на основе пользовательской базы сигнатур, списка нежелательных программ, а так же предварительно созданных шаблонов.

Скриптовые возможности AVZ имеют более продолжительное развитие. Команды скрипта создаются из браузера в интерактивном режиме при просмотре логов virusinfo***.***, или во внешнем редакторе с использованием шаблонов. Скрипты AVZ помимо работы с файлами, правки реестра управляют активностью антируткита, boot cleaner-a, avzguard.

резервное копирование, восстановление системы (реестра, системных файлов)		
твики исправления настроек системы	да	да
мастер восстановления системы	да	нет

восстановление ключей реестра из сохраненных копий	да	да
оптимизация реестра системы	нет	да
режим сохранения и восстановления критических файлов (и областей) системы		
создание копий файлов реестра системы	нет	да
создание копий веток реестра системы	да	нет
Восстановление стандартного загрузчика в MBR	нет	да
Восстановление стандартных загрузчиков в VBR+IPL	нет	да
Удаление стартовых страниц из из настроек браузеров	нет	да
Восстановление известных системных файлов из внешнего архива STORE	нет	да
New! Восстановление известных системных файлов по известному id_file	нет	да
Восстановление файлов реестра системы из сохраненных копий	нет	да

В обеих утилитах реализован режим сохранения_восстановления важнейших параметров и областей системы.

AVZ сохраняет параметры веток реестра в reg- файлы, восстановить настройки через интерфейс программы возможно будет лишь в активной системе.

uVS создает копии файлов реестра System, Software (или использует найденные копии, созданные программой ERUNT), соответственно, не проблема будет восстановить настройки при любом режиме запуска: на активной системе, на пассивной системе, или при запуске с Live.Cd. В некоторых случаях возможно восстановление нормального запуска системы путем оптимизации реестра системы. Режим восстановления отсутствующих известных системных файлов из под WinPE позволяет эффективно излечивать различные виды win-локеров, подменяющих системные файлы (например, userinit.exe, taskmgr.exe), а восстановление загрузчика в MBR позволяет снять блокирование загрузки системы, создаваемое троянами MBRLock. Судя по последним тестам (для 32битных систем) uVS успешно восстанавливает загрузчики в VBR+IPL для XP, Vista, Seven, заражение которых характерно для нового бутового трояна Boot.Cidox.a.В v3.69 добавлен режим извлечения сигнатур из загрузчиков, возможность проверки дампов загрузчиков на VT, jotti. Проверка загрузчиков в VBR, IPL по списку безопасных, проверка дампов загрузчиков на VT, jotti позволяет детектировать бутовый вариант Carberp. В v.3.72-73 добавлены актуальный режим: создание загрузочного образа WinPE&uVS.iso на базе WAIK3 или Windows7 SP1 AIK Supplement Update, запись Live.CD или Live.USB. Добавлен новый режим запуска uVS: выполнить скрипт из буфера обмена, упрощающий выполнение скриптов для пользователя, добавлен режим просмотра загрузчиков MBR,VBR, IPL. В v.3.74-3.76 добавлены новые ключи автозапуска, добавлены дефолтные значения некоторых ключей реестра, благодаря чему стало возможным выполнить корректное лечение модификаций Corkow, Crevx.
В v 3.77 добавлена поддержка проверки внешних ЭЦП (по CatRoot) для Windows 8.
В v 3.78-80 реализован механизм автоматического обновления базы безопасных MAIN с участием пользователей программы + реализовано автоматическое обновление модулей и списков программы для подписчиков uVS. Улучшен механизм автоматического формирования скрипта. Автоматически, согласно добавленным критериям по списку установленных программ формируются команды деинсталляции нежелательного софта. Модифицирован режим создания Winpe&uVS. Теперь загрузочный образ формируется на базе WINPE4 и установленного пакета Windows 8 ADK.
В v3.81 улучшен механизм автоскрипта. Автоматически добавляются твики разблокировки редактора реестра, диспетчера задач, свойств папки и др., автоматически добавляются команды очистки hosts согласно добавленным критериям, автоматически обрабатывается список объектов со статусом ?ВИРУС? согласно выбранному в settings.ini методу удаления объекта. Добавлен 64битный модуль, который активируется при анализе 64битных систем, т.о. теперь адресное пространство 64-х разрядных процессов анализируется в полном объеме, добавлена информация об активной IP Sec policy, а так же функции деактивации и удаления указанной политики.

В v3.82 реализован твик (27) очистки групповой политики для браузеров, которая используется вирусописателями в целях принудительного включения в список нежелательных расширений для браузеров.

В v3.83:
добавлено кэширование проверок для VT, модифицирован поиск объектов в списке: теперь поиск возможен по любому из столбцов, по которому установлена сортировка. Добавлен инвертированный поиск. Улучшен механизм автоскрипта с добавлением новых твиков 28, 29 для автоматической очистки модифицированных ярлыков рабочего стола, быстрого запуска.
Добавлена поддержка создания образов дисков и загрузочных флешек на базе WinPE 5.1, ссылка на скачивание ADK 8.1 обновлена: http://www.microsoft.com/en-us/download/details.aspx?id=39982
Добавлен белый список ЭЦП. При включении его поддержки, статус проверенного файла получает лишь тот файл, который подписан подписчиком из данного списка. В случае работы с образом автозапуска статусы файлов приводятся в соответствие с белым списком при открытии образа. Таким образом, автоматически будут отсеяны из ПРОВЕРЕННЫХ файлы с левой цифровой подписью.

В v3.84:
- добавлен модуль report_crash. В случае аварийного завершения uVS модуль report_crash.exe запускается автоматически и отправляет минидамп процесса uVS разработчику на анализ.
- добавлен метод Autohide для автоматического скрытия чистых объектов с цифровой подписью (из белого списка), попавших под ложный детект.
В v3.85:
- модифицирована (и оптимизирована) функция проверки на VT через public API.
В v3.86:
- Добавлен детект и удаление групповых политик Chrome, которые используются зловредами для добавления нежелательных расширений, или поисковых движков.
- добавлена очистка кэша Sun Java;
- добавлены в список автозапуска расширения и поисковые движки для Firefox, Chrome, Opera;
- улучшен механизм автоскрипта:
добавлены настраиваемые действия для критериев snms: auto – вариант действий, установленный в settings.ini, del, delref, delall, deldir, deldirex, skip (пропуск действия).
- добавлены возможность установить приоритеты в критериях, т.о., что в автоскрипт автоматически будет добавлено действие с максимальным приоритетом.
- добавлена возможность создания загрузочного диска WINPE на базе Windows 10 ADK;

В v 4.0 изменился подход к выполнению команд.
Теперь функции, а так же все соответствующие им скриптовые команды:
- Удаление ссылки на объект (delref)
- Удаление объекта вместе со всеми ссылками на него (delall)
- Выгрузка из памяти (unload)
- Удаление ссылок на отсутствующие файлы (delnfr)

НЕ исполняются немедленно, а помещаются в очередь команд, очередь не имеет ограничений на количество элементов.

Для исполнения команд в очереди и применения изменений необходимо нажать новую кнопку "Принять изменения". Удалить отдельные команды вы можете в новом разделе "Очередь команд".

Все команды в очереди будут исполнены за один проход.
запуск автоскрипта автоматически добавляет в скрипт все команды из очереди и очищает очередь команд.

Добавлена новая категория "WMI: обработчики событий".

В v 4.0.14
---
o Добавлена экспериментальная функция обнаружения внедренных потоков в известные системные процессы (пока только для 32-х битных процессов).
В случае обнаружения в лог выводится строка:
Injected thread detected in process полный_путь [PID], tid=TID
Функция дополняет старый функционал по обнаружению потоков на базе внедренных DLL.

В v 4.0.15
---
o Обновлена и исправлена функция обнаружения внедренных потоков.
Добавлена поддержка 64-х битных потоков, функция теперь доступна для Windows Vista и старше

в v 4.0.21
---
o Добавлена возможность удалять события WMI и задачи без удаления всех ссылок на файл/объект. Скриптовые команды: delwmi и deltsk

в v 4.11.2
---
o Добавлена поддержка VT API v3.

В v 4.11.5
---
o Добавлена поддержка отслеживания процессов.
Отслеживание процессов позволяет определять родителя любого процесса, даже если родительский процесс уже завершен, а также достоверно определять все файлы, которые запускались с момента старта системы.
Если отслеживание включено то в категорию "Запускался неявно или вручную" попадают только те файлы, что запускались с момента запуска системы.

В v 4.11.6
---
o Добавлена поддержка отслеживания задач.
В окно информации исполняемого файла, который создавал, модифицировал или изменял задачи добавлены следующие разделы:
"Создание задачи", "Удаление задачи", "Обновление задачи" в которых указано время операции, pid процесса,
pid и имя запустившего процесс, а так же XML описание задачи при его наличии.

4.11.7

В uVS добавлен раздел "DNS лог", в нем находятся адреса, которые запрашивали процессы с момента загрузки системы,

в окне информации для каждого адреса указан процесс, его pid, дата обращения к DNS и результат, если он был, промежуточные адреса в список не включены.

4.11.9
---
o Твик #39 теперь дополнительно включает отслеживание командных строк завершенных процессов, командные строки отображаются в окне информации.
Только для Windows 8.1/Windows Server 2012 R2 и старше.

4.11.10
---
o Улучшена функция определения внедренного кода.
Теперь при обнаружении модифицированного кода в процессе (hollowing/dopelganging и т.п.) выдается предупреждение в лог.

4.11.11
---
o Добавлена поддержка Windows 11.

4.12
---
o Добавлена поддержка STORE для Windows 11.
o В STORE добавлены файлы для Windows 11.

uVS – основной инструмент помощи пользователям при лечении активного заражения на техническом форуме ESET RUSSIA (**forum.esetnod32.ru**).
uVS успешно стартовал на форуме Компьютерной помощи **pcHelpForum.ru**, активно используется хелперами **adminplanet.ru, kompasnet.org, tehnari.ru, cyberforum.ru**

документирование системы		
документирование системы	да	да
Дополнительная языковая редакция программы (английская)	да	да

AVZ, **uVS** хорошо документированы. Разработчик AVZ поддерживает файл справки avz.hlp, документация по **uVS** содержится в актуальном архиве программы в текстовых файлах. Следует добавить, что оба автора поддерживают английскую редакцию утилит.

Собственно, **AVZ**, **uVS** не единственные пули в нагане хелпера, но обе - отменного калибра.

(c), santy. 2010_11_15---2021_12_31.