Verdict description

|  |  |  |
| --- | --- | --- |
| # | Verdict name | Verdict desctiption |
| 1 | REPORT\_EVENT\_P2P\_SC\_RDL  L"Worm.P2P.generic";  // SC+RDL+ | Черви этого типа распространяют себя используя общие сетевые директории и электронную почту. |
|  |
| 2 | REPORT\_EVENT\_SC\_AR  "Trojan.generic"; //SC+AR+ | Эта категория вредоносных объектов включает в себя троянские программы, созданные для разрушения данных и дестабилизации функционирования компьютеров. |
|  |
| 3 | REPORT\_EVENT\_SC\_ARsrc |  |
| 4 | REPORT\_EVENT\_SCN  "Worm.generic"; // SCN+; | Черви этого типа распространяют себя используя общие сетевые директории и электронную почту. |
|  |
| 5 | REPORT\_EVENT\_P2P\_SCN  "Worm.P2P.generic";  // SCN+(P2P); | №1 |
|  |
| 6 | REPORT\_EVENT\_SC2STARTUP  "Trojan.generic";  // SC2STARTUP+; | №2 |
|  |
| 7 | REPORT\_EVENT\_SC\_MULTIPLE  "Worm.P2P.generic";  // SC+(MULTIPLE); | №1 |
|  |
| 8 | REPORT\_EVENT\_RDR  "RootShell";  // RDR+; | Root shell предоставляет взломщику консольный доступ к атакуемой системе. Root shell перенаправляет стандартные потоки ввода/вывода на специально созданный сокет н аатакуемой машине. Таким образом, удалённый взломщик имеет возможность исполнять команды консольного интерпретатора удалённо |
|  |
| 9 | REPORT\_EVENT\_REGMODIFY  "Registry access" | Процесс пытается получить доступ к одному из контролируемых (критических) разделов системного реестра Windows. Системный реестр Windows — это база данных, в которой хранится информация о настройках системы, установленных приложениях и многое другое. Вредоносные программы модифицируют реестр с целью регистрации себя для автоматического запуска при старте операционной системы, подмены стартовой страницы Internet Explorer и других деструктивных действий. Однако доступ к системному реестру может осуществляться и обычными приложениями. |
|  |
| 10 | REPORT\_EVENT\_HIDDEN\_OBJ  "Hidden object" | Руткит прячет заданный процесс и файлы от других программ. |
|  |
| 11 | REPORT\_EVENT\_INVADER  "Invader" | Эта категория вредоносных объектов встраивает свой код в адресное пространство других програм, таким образом, получая доступ к ресурсам, доступным этим программам. Существует четыре разновидности програм этого класса, каждая из которых распознаётся модулем Проактивная Защита. |
|  |
| 12 | REPORT\_EVENT\_APPG  "Critical application" | Модуль «Контроль целостности приложений» компонента «Проактивная защита» обладает дополнительной возможностью — контролем запуска приложений. По умолчанию этот режим отключен. В этом режиме Kaspersky Anti-Virus 6.0 / Kaspersky Internet Security 6.0 показывает предупреждение всякий раз, когда запускается указанное пользователем приложение. Предупреждение появляется только в том случае, если для контролируемого приложения настроено правило «Запуск: Запросить действие». |
|  |
| 13 | REPORT\_EVENT\_APPG\_CHANGED  "Application changed" | Существуют разновидности вредоносного ПО, которые внедряются в исполняемые файлы, библиотеки или модули расширения известных программ. Таким образом можно, например, организовать утечку данных с компьютера пользователя. Сетевой трафик, инициированный вредоносным кодом, будет свободно пропускаться сетевыми экранами, поскольку, с точки зрения сетевого экрана, этот трафик принадлежит приложению, которому разрешен доступ в интернет.  Для того чтобы противодействовать модификации известных приложений вредоносным ПО применяется модуль «Контроль целостности приложений» компонента «Проактивная защита». Список приложений, контролируемых этим компонентом, автоматически формируется мастером настройки во время установки Kaspersky Anti-Virus 6.0 / Kaspersky Internet Security 6.0.  Событие «Application changed» означает, что исполняемый файл контролируемого приложения изменился с момента предыдущего запуска. Однако изменение исполняемого файла могло произойти как в результате внедрения в приложение вредоносного кода, так и в результате обычного обновления программы. Например, исполняемый файл браузера Microsoft Internet Explorer может измениться в результате обновления Windows. |
|  |
| 14 | REPORT\_EVENT\_IMG\_CHANGED  "Integrity violation" | Существуют разновидности вредоносного ПО, которые внедряются в исполняемые файлы, библиотеки или модули расширения известных программ. Таким образом можно, например, организовать утечку данных с компьютера пользователя. Сетевой трафик, инициированный вредоносным кодом, будет свободно пропускаться сетевыми экранами, поскольку, с точки зрения сетевого экрана, этот трафик принадлежит приложению, которому разрешен доступ в интернет.  Для того чтобы противодействовать модификации известных приложений вредоносным ПО применяется модуль «Контроль целостности приложений» компонента «Проактивная защита». Список приложений, контролируемых этим компонентом, автоматически формируется мастером настройки во время установки Kaspersky Anti-Virus 6.0 / Kaspersky Internet Security 6.0.  Событие «Intergity Violation» означает, что с момента предыдущего запуска изменился один или несколько модулей контролируемого приложения. Однако изменение исполняемого файла могло произойти как в результате внедрения в приложение вредоносного кода, так и в результате обычного обновления программы. Например, библиотеки, используемые браузером Microsoft Internet Explorer, могут меняться в результате обновления Windows. |
|  |
| 15 | REPORT\_EVENT\_APPG\_ASCHILD  "Running as child" | Некоторые вредоносные программы используют обычные программы для организации утечки данных или загрузки вредоносного кода из интернета. Для этого обычная программа, которой правилами сетевого экрана и других средств защиты разрешен доступ в интернет (например, веб-браузер), запускается вредоносной программой как дочерний процесс.  Для того чтобы противодействовать запуску вредоносным ПО известных приложений в качестве дочерних процессов применяется модуль «Контроль целостности приложений» компонента «Проактивная защита». Список приложений, контролируемых этим компонентом, автоматически формируется мастером настройки во время установки Kaspersky Anti-Virus 6.0 / Kaspersky Internet Security 6.0.  Событие «Running as child» означает, что контролируемое приложение запущено другим процессом как дочерний процесс. Предупреждение появляется только в том случае, если для контролируемого приложения настроено правило «Запуск дочернего процесса: Запросить действие». Поскольку запуск одних программ другими в качестве дочерних процессов является достаточно распространенным явлением, по умолчанию показ предупреждений о таких событиях отключен, однако эти события протоколируются в отчетах проактивной защиты. |
|  |
| 16 | REPORT\_EVENT\_APPG\_BROWSER  "Starting Internet Browser" | Launcher получает доступ к ресурсам, расположенным в интернете используя браузер, установленный по умолчанию в системе. Launcher запускает браузер с параметрами, содержащими, к примеру, пользовательские пароли. Существует несколько методов передачи браузеру параметров, включая параметры командной строки, DDE и т.п. |
|  |
| 17 | REPORT\_EVENT\_INVADER\_LOADER  "Invader (loader)" | Существует множество разновидностей вредоносного ПО, которые внедряются в исполняемые файлы, библиотеки или модули расширения известных программ. Таким образом можно, например, организовать утечку данных с компьютера пользователя. Сетевой трафик, инициированный вредоносным кодом, будет свободно пропускаться сетевыми экранами, поскольку, с точки зрения сетевого экрана, этот трафик принадлежит приложению, которому разрешен доступ в Интернет.  Для обнаружения и блокировки попыток внедрения вредоносного кода в процессы в памяти применяется модуль «Анализ активности приложений» компонента «Проактивная защита».  Внедрение в другие процессы широко используется троянскими программами. Однако такая активность характерна также для некоторых безобидных программ, пакетов обновлений и программ установки. Следует разрешать этот вид активности только в том случае, если вы уверены, что внедряемая программа безобидна. |
|  |
| 18 | REPORT\_EVENT\_STRANGEKEY  "Suspicious registry value" | Создатели вредоносных програм часто создают ключи системного реестра, которые не могут быть просмотрены стандартными редакторами реестра. Так называемые «скрытые ключи» позволяют создателям вирусов хранить данные в системном реестре, доступные исключительно им самим. |
|  |
| 19 | REPORT\_EVENT\_SYSCHANGE  "Strange behaviour" | Прямой доступ к памяти.  Модификация точки входа R0-R3. |
|  |
| 20 | REPORT\_EVENT\_HIDDEN\_INSTALL  "Hidden install" | Некоторые программы выполняют установку собственных компонент в системе без пользовательского согласия. Такое поведение характерно для вредоносных программ класса Trojan Downloaders/Droppers |
|  |
| 21 | REPORT\_EVENT\_BUFFEROVERRUN  "Buffer overrun" | Технология переполнения буфера используется злоумышленниками для получения доступа к системе под системной учётной записью. |
|  |
| 22 | REPORT\_EVENT\_DEP  "Data Execution" | Вредоносные программы прячут свой код от анализаторов активности, помещая его в области памяти предназначенной для данных, а не для исполняемого кода. |
|  |
| 23 | REPORT\_EVENT\_HOSTS  "Hosts file modification" | Файл hosts — это один из важных системных файлов операционной системы Windows. Он предназначен для ускорения доступа к интернет-ресурсам за счет преобразования URL в IP-адреса не на DNS-серверах, а непосредственно на локальном компьютере. Это обычный текстовый файл, каждая строка которого определяет соответствие символьного имени (URL) сервера и его IP-адреса.  Вредоносные программы часто используют файл hosts для переопределения адресов серверов обновлений антивирусного ПО, чтобы заблокировать возможность обновления и предотвратить обнаружение вредоносной программы сигнатурным методом, а также для других целей. Для того чтобы противодействовать попыткам модификации файла hosts вредоносным ПО применяется модуль «Анализ активности приложений» компонента «Проактивная защита» Kaspersky Anti-Virus 6.0 / Kaspersky Internet Security 6.0. |
|  |
| 24 | REPORT\_EVENT\_KEYLOGGER  "Keylogger" | Клавиатурный перехватчик. Программа, встраивающаяся в драйвер клавиатуры и перехватывающая нажатия клавиш. Вредоносная программа такого типа может отсылать информацию, набираемую с клавиатуры (логины, пароли, номера кредитных карт) злоумышленнику. Однако перехват нажатий клавиш может использоваться и обычными программами. Часто перехват нажатий клавиш применяется для вызова функций программы из другого приложения с помощью «горячих клавиш» (hotkeys). |
|  |
| 25 | REPORT\_EVENT\_DOWNLOADER  "Trojan Downloader" | Trojan Downloader — это программа, основным назначением которой является скрытая несанкционированная загрузка программного обеспечения из интернета. Наиболее известным источником Trojan Downloader являются хакерские сайты. Сам по себе Trojan Downloader не несет прямой угрозы для компьютера — он опасен именно тем, что производит неконтролируемую загрузку программного обеспечения. Trojan Downloader применяются в основном для загрузки вирусов, троянских и шпионских программ. |
|  |
| 26 | REPORT\_EVENT\_TROJAN\_GEN  "Trojan.generic"  ("Trojan.cryptor") | TrojanCryptor – это программа, модифицирующая документы пользователя (чаще всего MSOffice) таким образом, чтобы с этими документами не возможно было дальше работать. Чаще всего за возврат документов в исходное состояние автор данного криптора требует с пользователя деньги. |
|  |
| 27 | REPORT\_EVENT\_TASKMGR\_PROT  "TaskManager protection" | Некоторые вредоносные программы пытаются спрятать свое присутствие в системе от пользователя путем изменения адресного пространства «менеджера процессов» («Task Manager») |
|  |
| 28 | REPORT\_EVENT\_DRIVER\_INS  "Suspicious driver installation" | Некоторые вредоносные программы патаются установить на систему собственные драйверы чтобы получить доступ к операционной системе на низком уровне тем самым пытаясь скрыть свое присутствие и сделать тяжелым процесс совего удаления из системы. |
|  |
| 29 | REPORT\_EVENT\_HIDDEN\_SEND  "Hidden data sending" | Некоторые вредоносные программы патаются управлять работой других стандартных приложений (без ведома пользователя) в своих корыстных целях. |
|  |
| 31 | REPORT\_EVENT\_MASS\_MAILER  "Mass-mailer software" |  |
|  |
| 32 | REPORT\_EVENT\_BROWSERCONTROL  "Internet Browser Control" | Некоторые вредоносные программы патаются управлять работой интернет браузеров (например для перехода на зараженный сайт без ведома пользователя) |
|  |
| 33 | REPORT\_EVENT\_MAX |  |
| Only in PDM2 | | |
| 34 | “AntiAV” |  |
|  |
| 35 | “AntiAVMultiple” |  |
|  |
| 36 | “IEStartPage” |  |
| 37 | "SecurityViolation" |  |
|  |
| 38 | “KillSystemFiles” |  |
| 39 | “PswAccess” |  |
| 40 | “PswAccessMultiple” |  |
| 41 | “StartSystemFileSuspended” |  |
| 42 | “StartWithSystemName” |  |
| 43 | “OnChangeSystemRegistry” |  |
| 44 | “OnInstallInNTFSStream” |  |
| 45 | “OnDeleteSelf” |  |