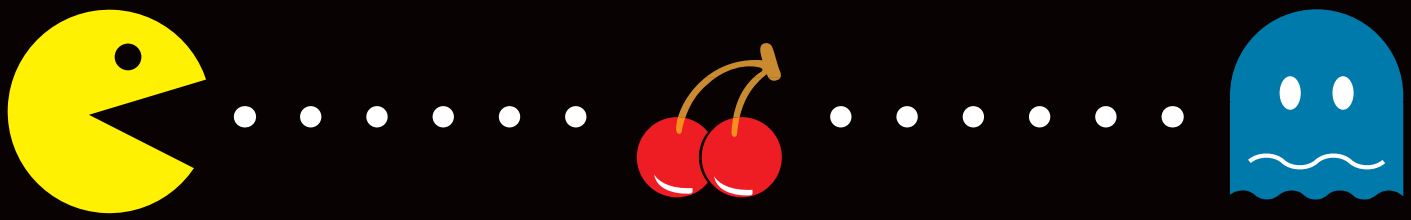
Евгений Дроботун (drobotun@xakep.ru)

НА МАЛВАРЬ БЕЗ АНТИВИРУСА



ЧТО ДЕЛАТЬ, ЕСЛИ ЕГО БАЗЫ ЕЩЕ НЕ УСПЕЛИ ОБНОВИТЬСЯ?

Наверняка к твоему дому уже давно протоптали широкую тропу потерпевшие от разного рода компьютерной нечисти, наслышанные о твоей неимоверной крутости и беспощадности в борьбе с заразой. Поначалу такая популярность тебя смущала и одновременно радовала, чуть позже стала напрягать, ведь у тебя и своих дел полно. Мы решили прийти к тебе на помощь и нарисовали небольшую карту поиска малвари с некоторыми пояснениями. Теперь вместо того, чтобы небрежно отмахиваться от очередной жертвы компьютерного криминала, ты можешь прикрыться своим любимым журналом и сказать: «Сделай сам, тут все написано и нарисовано...»

В общем случае тактика проведения боевой операции по освобождению компьютера от зловредов заключается в следующем порядке действий:

- находим процесс, принадлежащий вредоносному коду, и останавливаем его;
- находим место, где лежит вредоносный файл, и удаляем его;
- ликвидируем последствия.

Основная проблема, как правило, состоит в преодолении первого этапа, ведь подавляющее большинство вредоносных программ тщательно маскируют свое присутствие в системе, да и вредоносный процесс остановить голыми руками получается далеко не всегда.

Удалить файл тоже удается далеко не всегда — малварь крепко цепляется за жизнь и нередко достаточно глубоко вгрызается в жесткий диск.

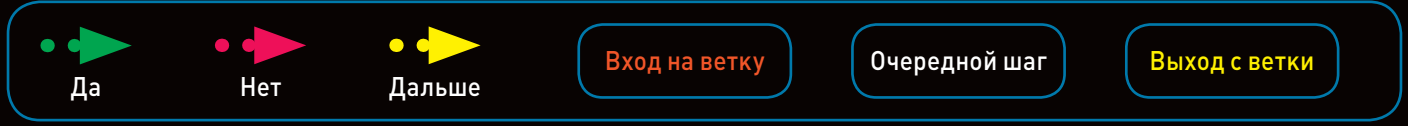
Тем не менее приступим...

ДИСПЕТЧЕР ЗАДАЧ

Первое место, куда стоит заглянуть в поисках следов вредоносов, — это диспетчер процессов. Само собой, способов скрыться от его взора у современной малвари достаточно много, но в жизни всякое бывает.

Итак, вариантов в этом случае у нас будет три:

- в диспетчере задач явно виден какой-то лишний процесс с весьма подозрительным названием, и этот процесс запросто можно завершить;
- также наблюдаем подозрительный процесс, но завершить его обычным способом не получается;
- диспетчер процессов кристально чист, и ничего подозрительного в нем не наблюдается.



В первом случае все просто. Завершаем процесс, ищем файл, смотрим автозагрузку, смотрим внутрь файла, заливаем файл на вирустотал, выносим вердикт и в конце концов смело его удаляем. Надеюсь, что «свои» процессы ты хотя бы частично узнаешь в лицо и трогать системные процессы типа lsas, services, system, winlogon, svchost, csrss в здравом уме не будешь.

При этом следует помнить, что все системные процессы «живут» в папке %windir%\system32\ (исключение — explorer.exe, он, как правило, прописан просто в %windir%\). Если путь к исполняемому файлу процесса ведет в другое место, особенно в какие-нибудь временные папки или на флешку, то это следует расценивать исключительно как вредоносное вмешательство. Также стоит обратить внимание на то, от чьего имени работает процесс. Если системный процесс работает от имени пользователя, то это повод насторожиться. Про то, что вредоносные процессы могут выдавать себя за системные, я думаю, ты знаешь, и процесс с именем вроде "svshost" без своего внимания не оставишь.

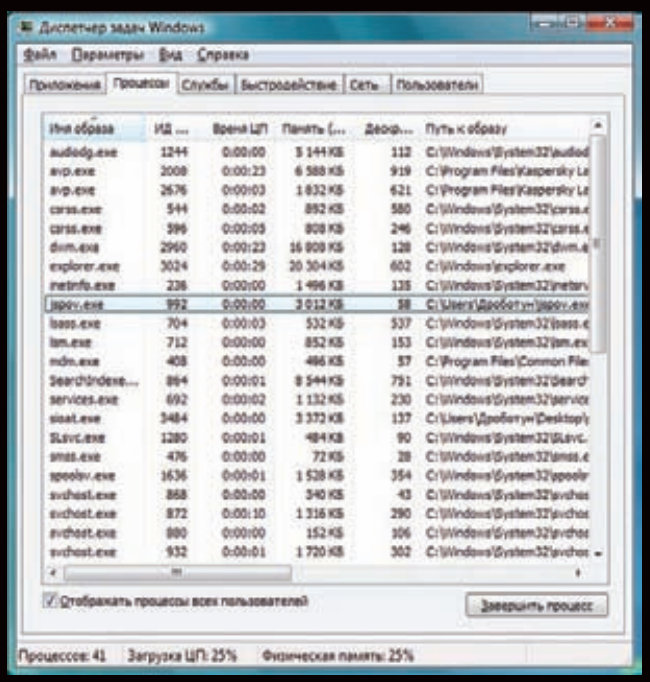
Если мы имеем дело со вторым случаем, то это — серьезный повод задуматься. Обычно нормальные и законопослушные программы без проблем дают себя удалить из списка процессов. В такой ситуации можно попробовать воспользоваться каким-нибудь альтернативным менеджером процессов, например Process Explorer от SysInternals или ProcessHacker, или заюзать утилиту Kernel Detective — последним двум по силам даже справиться с процессами многих антивирусов. Также можно попытаться приаттачиться к этому процессу отладчиком, а потом завершить все это вместе с отладчиком (способ довольно действенный, особенно если использовать для этого WinDbg).

Если случай настолько тяжелый, что все перечисленное не помогает, то, скорее всего, дело не обошлось без перехвата функций в ядре, но об этом несколько позже.

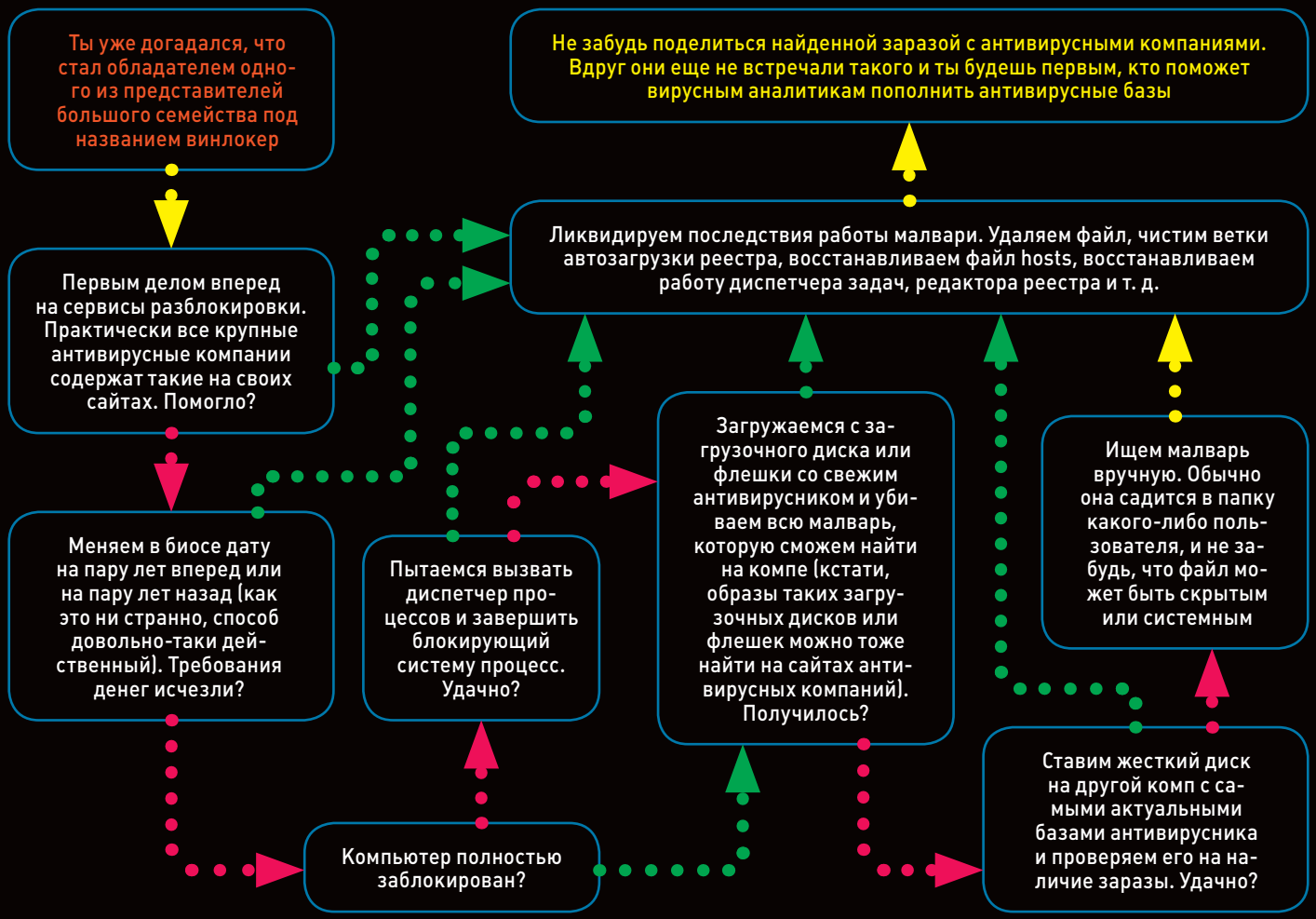
Если в диспетчере задач мы ничего подозрительного не увидели, то либо все чисто (этот вариант мы, как истинные параноики компьютерной безопасности, отметаем), либо вредоносный процесс умело маскирует свое присутствие, либо малварь внедрила свой код в какой-то легальный процесс и под его прикрытием творит свои нехорошие дела.

Скрытые процессы также можно попытаться выявить каким-нибудь альтернативным диспетчером процессов или опять же попробовать использовать Kernel Detective, который умеет выявлять маскировку процесса, реализованную с помощью перехвата API-функции NtQuerySystemInformation.

Вообще бесследно скрыть процесс в системе практически невозможно, какие-нибудь следы присутствия все равно остаются, ведь каждый процесс имеет целую кучу косвенных признаков, по которым



Подозрительный процесс в штатном диспетчере процессов



можно его обнаружить. Это созданные им хендлы, окна, некоторые другие системные объекты (например, многие трояны создают при заражении системы мьютекс, для того чтобы избежать повторного заражения). Все это можно попытаться просмотреть и проанализировать. К примеру, с помощью консольной утилиты Handle от Марка Руссиновича из небезызвестной SysInternals можно увидеть открытые хендлы для всех процессов, в том числе и для скрытых.

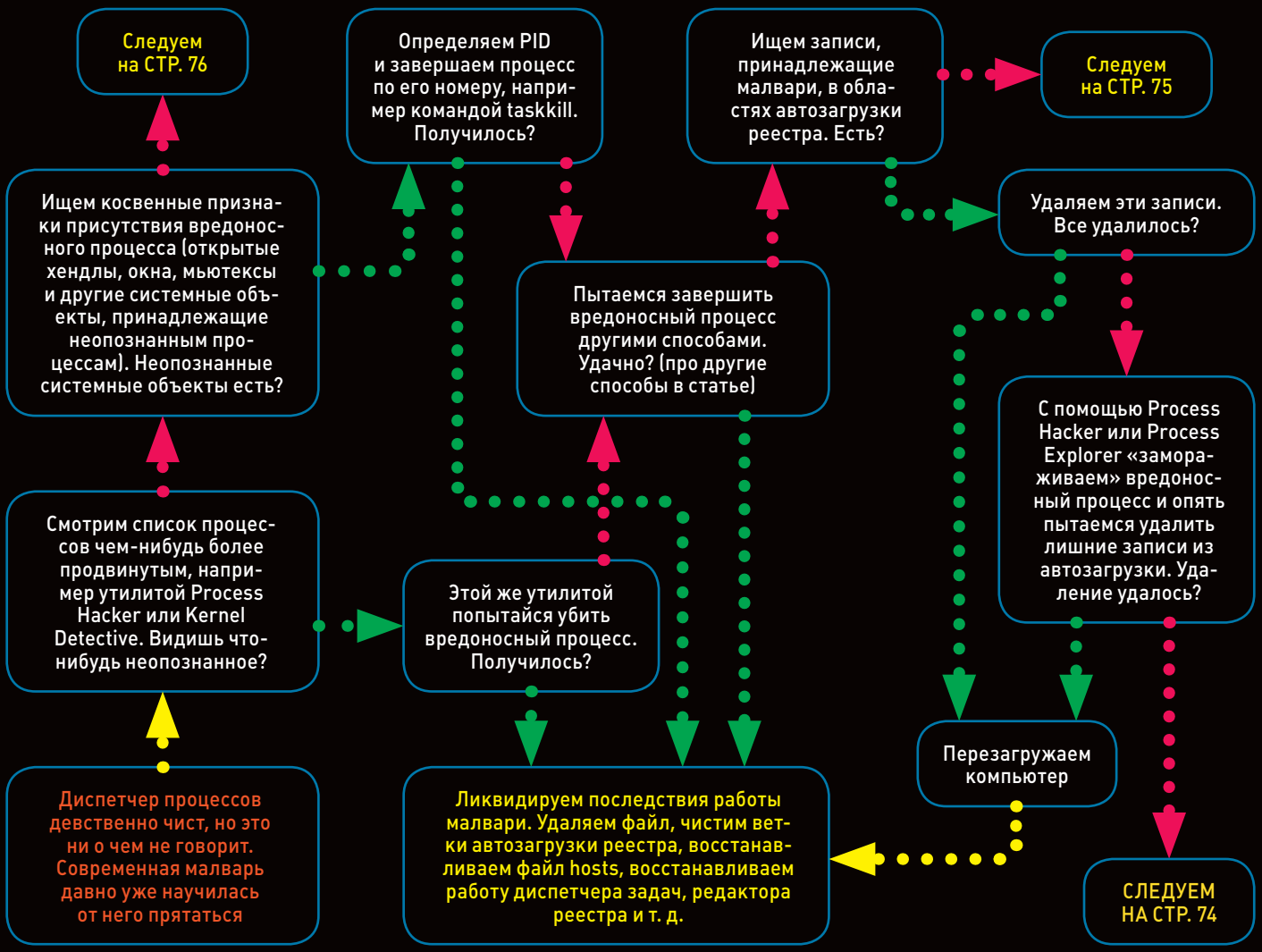
Для исследования объектов, созданных в системе, пригодится тулза под названием WinObj из того же самого набора SysInternals Suit. С ее помощью можно посмотреть все созданные системные объекты и определить, каким процессом он создан.

Если мы столкнулись с внедрением вредоносного кода в процесс, нужно учесть, что, как правило, это делается либо для беспрепятственного доступа в сеть из-под доверенного процесса (для этого неплохо подходят процессы svchost.exe или explorer.exe), либо для организации перехвата некоторых системных функций и внедрения этих перехватов во все запущенные и запускаемые процессы (излюбленным местом для внедрения в этом случае становится процесс explorer.exe, а иногда winlogon.exe).

Обнаружить взаимодействие внедренного кода с сетью можно, используя какие-либо утилиты мониторинга сетевых соединений. К примеру, в «полном собрании сочинений» от SysInternals для этого имеется тулза TcpView, которая производит мониторинг всех подключений и выводит список процессов, использующих TCP- и UDP-соединения. При этом отображаются основные параметры каждого соединения — имя процесса, протокол, идентификатор состояния подключения, локальный и удаленный адреса.

ПЕРЕХВАТЫВАЕМАЯ ФУНКЦИЯ	ФУНКЦИИ, ВЫПОЛНЯЕМЫЕ ПЕРЕХВАТЧИКОМ
ntdll.dll!LdrLoadDll kernel32.dll!LoadLibrary	Отслеживание загрузки библиотек
ntdll.dll!EnumerateValueKey ntdll.dll!EnumerateKey advapi.dll!RegEnumKey advapi.dll!RegEnumKeyEx advapi.dll!RegEnumValue	Маскировка ключей и их значений в реестре, блокировка изменений значений ключей в реестре
ntdll.dll!OpenProcess ntdll.dll!OpenThread	Защита процессов и потоков от анализа и завершения
ntdll.dll!NtQuerySysteminformation ntdll.dll!RtlGetNativeSystemInformation kernel32.dll!Process32Next kernel32.dll! CreateToolhelp32Snapshot	Маскировка процессов
ntdll.dll!NtQueryDirectoryFile ntdll.dll!NtCreateDirectoryObject ntdll.dll!NtOpenDirectoryObject ntdll.dll!QueryInformationFile ntdll.dll!OpenFile ntdll.dll!CreateFile kernel32.dll!FindNextFile kernel32.dll!CopyFile kernel32.dll!MoveFile kernel32.dll!DeleteFile	Маскировка файлов и каталогов, блокировка доступа к файлам, искажение информации о файлах

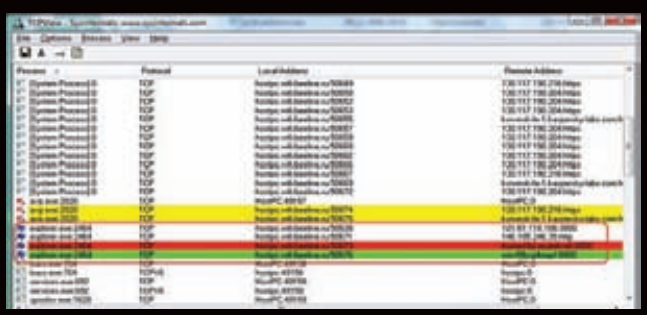
API-функции, которые любят перехватывать вредоносные программы



Если в списке, полученном с помощью этой утилиты, мы увидим, например, explorer.exe, ведущий активный обмен с непонятным адресом, то лучше либо закрыть это соединение, либо вовсе перезапустить процесс.

ОБЛАСТИ АВТОЗАГРУЗКИ

Существует много разных способов сделать так, чтобы вредоносный код запускался вместе с системой. В подавляющем большинстве вредоносов (вновь входящих в моду буткитов это не касается)



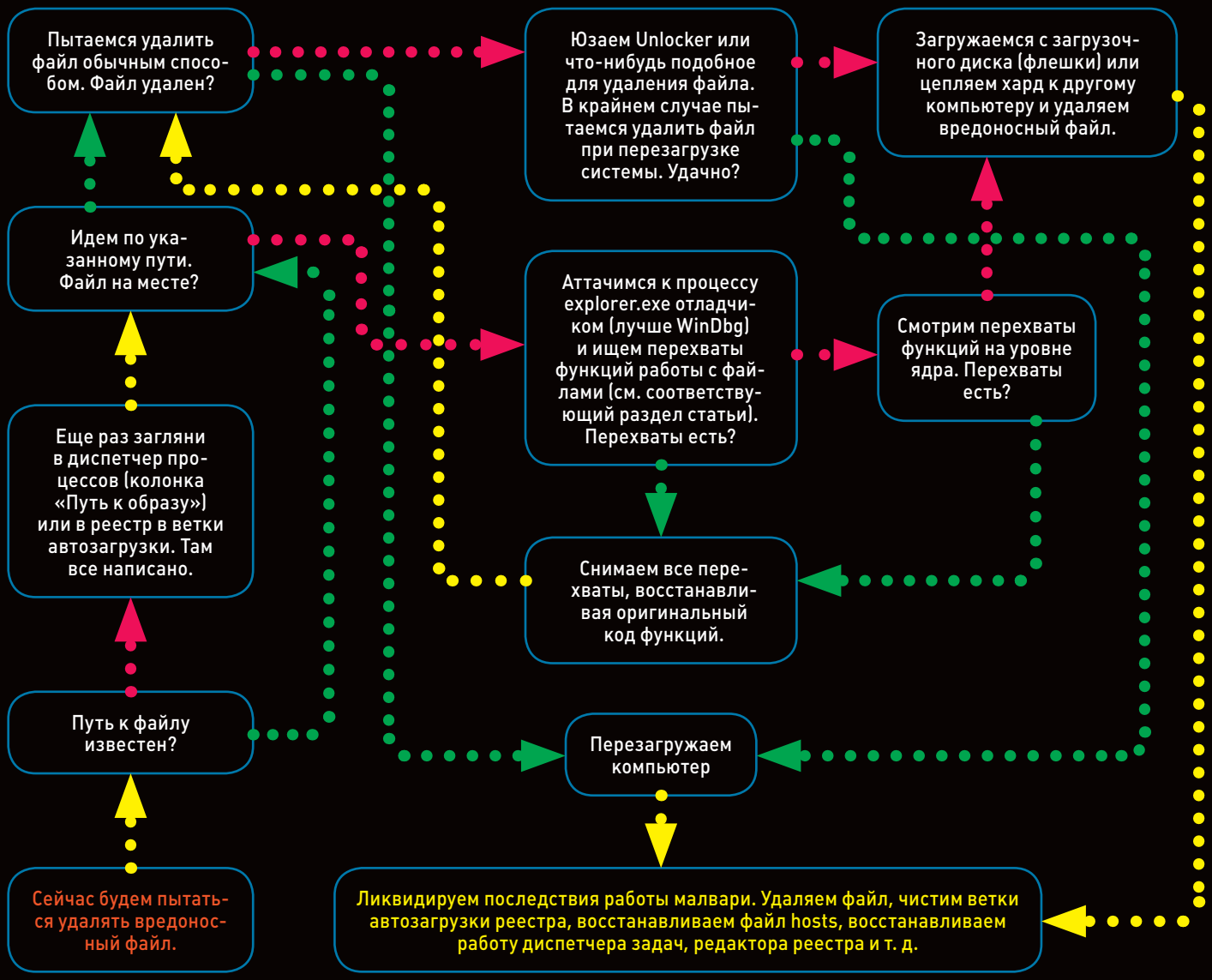
Подозрительная сетевая активность процесса explorer.exe

для этого, тем или иным способом, используется реестр (про папку «Автозагрузка» упоминать не стоит, хотя, говорят, ее тоже иногда задействуют).

Все места в реестре и способы запуска вредоносного кода перечислять мы не будем, их очень много, тем более что просмотреть их вручную — задача не из легких. Гораздо приятнее воспользоваться каким-нибудь менеджером автозагрузки. Самый лучший образец такого рода программ — это Autoruns от SisInternals (более подробно об этой утилите смотри врезку).

К сожалению, многие вредоносные программы защищены от удаления их из областей автозагрузки в реестре. Обычно они периодически проверяют наличие ключей в реестре и, если те удалены, создают их заново. Также может использоваться периодическое удаление текущего ключа и создание нового, с другим именем. Для того чтобы этому противостоять, одного Autoruns'а будет недостаточно. На помощь может прийти Process Explorer или какой-нибудь другой менеджер процессов, который может приостанавливать («замораживать») процесс и все его потоки. Порядок действий прост: приостанавливаем процесс (обычно это пункт меню «Suspend»), затем удаляем все лишнее из автозагрузки, перезагружаемся, и, если повезло, вредоносный код остается не у дел.

Более серьезную защиту областей автозагрузки с вредоносным кодом дает перехват функций работы с реестром. В таком случае



появляется необходимость снимать эти перехваты и восстанавливать оригинальный путь вызова API.

ПЕРЕХВАТЫ ФУНКЦИЙ

Для маскировки своего присутствия в системе более или менее продвинутая малварь может перехватывать некоторые API-функции (про такие перехваты мы уже говорили, когда обсуждали скрытие процессов). Малварь может не только маскировать непосредственно свой процесс, но и скрывать местоположение файла или какие-нибудь записи в реестре. Соответственно в первом случае необходимо перехватывать функции для работы с файлами и директориями, во втором — функции для работы с реестром.

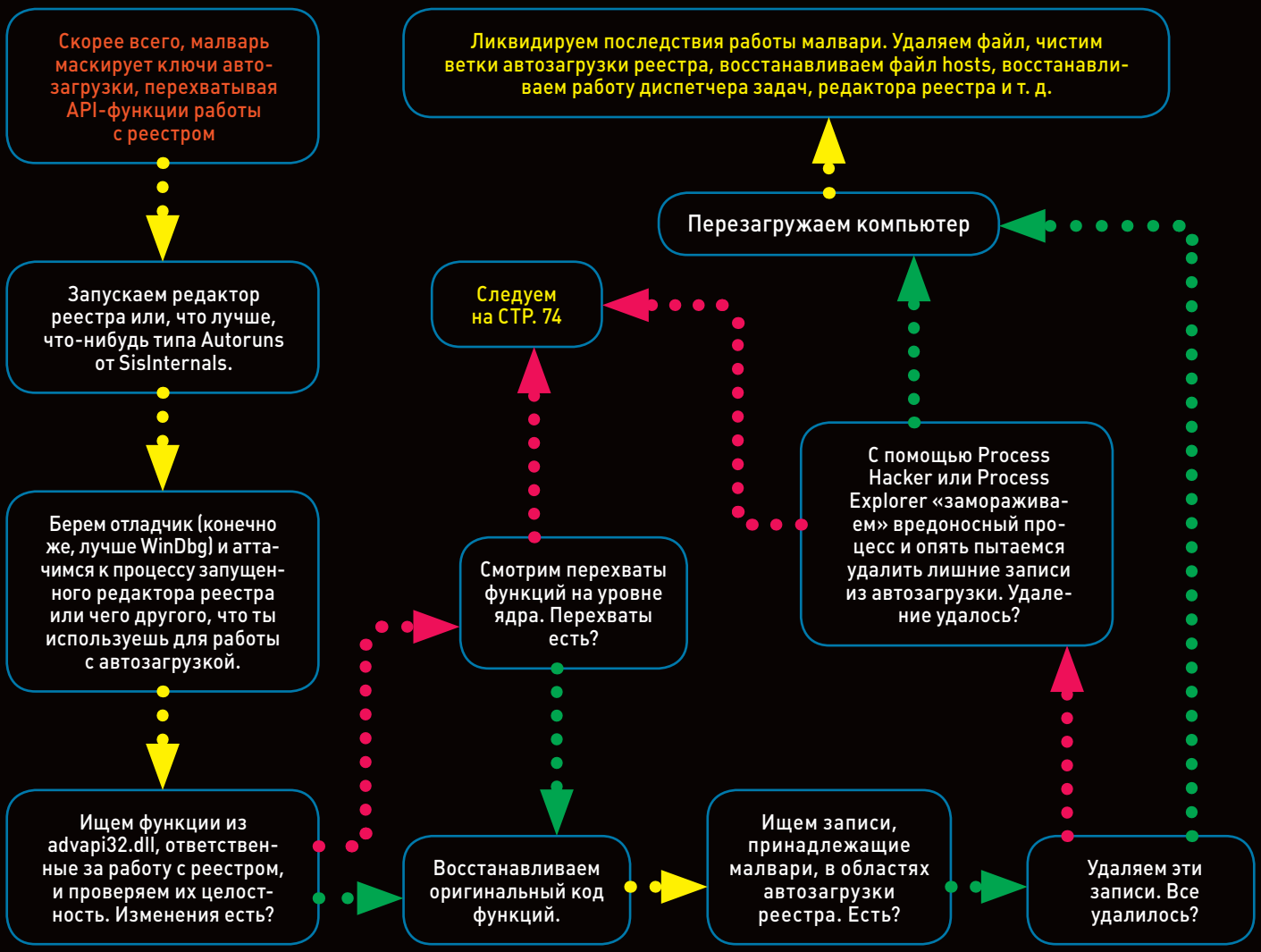
Наиболее популярные во вредоносных кругах для перехвата функции можешь посмотреть в таблице. Думаю, для тебя не секрет, что перехват функций может осуществляться в режиме пользователя или в режиме ядра. Для перехвата в режиме ядра обычно используется драйвер, наличие которого в системе также демаскирует малварь. Для снятия перехватов необходимо либо восстановить оригинальный код функции, если перехват осуществлялся изменением ее кода, либо восстановить таблицу системных вызовов, что умеют делать многие утилиты, в частности, Kernel Detective весьма неплохо справляется с этой задачей. Изменения в самих функциях нетрудно восстановить с помощью отладчика. Как правило, малварь меняет первые пять байт кода функции, вставляя туда безусловный переход. При этом стоит запомнить, что оригинальный код системных функций из ntdll.dll начинается с загрузки в регистр EAX номера функции, а код функций из других библиотек, как правило, начинается с пролога вида:

```
MOV edi, edi
PUSH ebp
MOV ebp, esp.
```

На диске есть видео, которое наглядно демонстрирует процесс восстановления функций для работы с реестром.

ЗАКЛЮЧЕНИЕ

Напоследок стоит сказать: даже если, несмотря на все усилия, потраченные на поиск вредоносного кода на твоем компьютере, его поиски не принесли результатов, не спеши обольщаться. Лучше перезагрузись с линуксового LiveCD, заклей камеру изолентой, заштрихуй окна, надень шапочку из фольги и жди выхода следующего номера журнала «Хакер». К этому моменту антивирусные базы обновятся, и новый вирус наверняка будет ими детектирован :).



МЕНЕДЖЕРЫ ПРОЦЕССОВ

Стандартный диспетчер процессов в Windows выдает минимум информации, да и очень часто становится объектом атак со стороны малвари.

Для анализа компьютера на предмет вредоносного кода нужны другие, более эффективные средства. Средств этих много — начиная от экзотического Task Manager'а, написанного на VBA Excel известным специалистом Дидье Стивенсом (в некоторых случаях Task Manager может быть очень полезным), и заканчивая более продвинутыми утилитами вроде Process Explorer или Process Hacker. Как раз на двух последних стоит остановиться поподробнее.

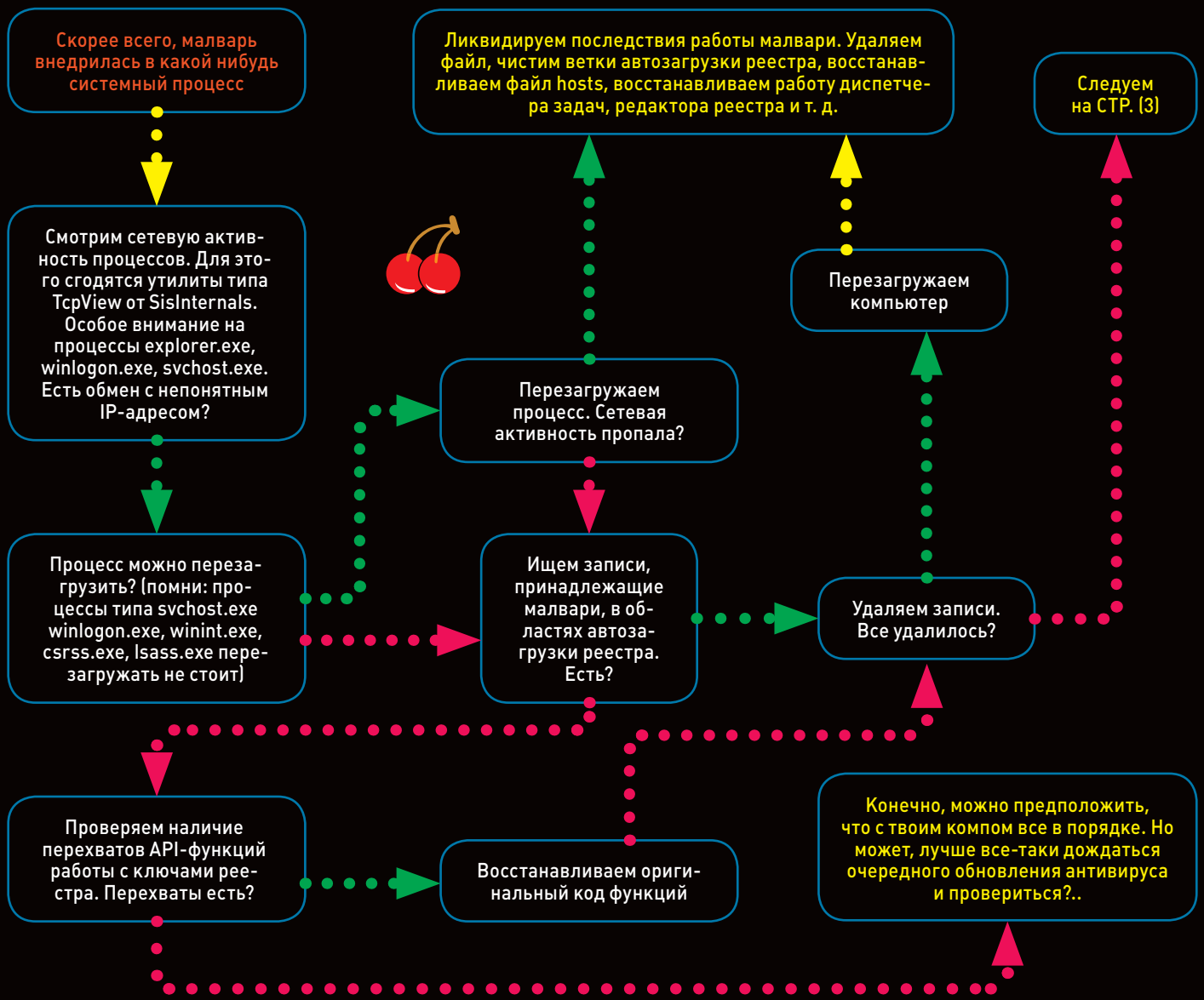
Process Explorer из уже известного нам набора системных утилит от Марка Руссиновича (однозначный мастхэв, между прочим).

Утилита отображает подробную информацию о процессах и, кроме того, позволяет изменять приоритет и привязку процесса к процессорам, приостанавливать («замораживать») выполнение процессов и всех его потоков (соответственно, затем продолжить их выполнение) и выполнять завершение процесса или дерева процессов.

К сожалению, завершение процесса происходит штатным способом, предусмотренным в Windows, поэтому многие труднозавершаемые процессы ей неподвластны. То же самое можно сказать и про скрытые процессы. Утилита использует обычный набор API-функций для формирования списка процессов, поэтому скрытые с помощью перехвата API-процессы она обнаружить не может.

Среди достоинств стоит отметить наличие функций поиска процесса по его окну, поиск библиотеки или хендла по имени и возможность проверки цифровых подписей файлов.

Process Hacker — более продвинутая тулза, которая умеет давать информацию о запущенных службах, показывать сетевую активность приложений и мониторить обращения к диску. Самый главный плюс — это возможность завершить процесс аж семнадцатью различными способами, при этом утилита способна заглушить процесс даже в самых тяжелых случаях (во время экспериментов она запросто расправлялась с процессами некоторых антивирусных продуктов, в том числе и запущенных как службы).



УТИЛИТЫ УПРАВЛЕНИЯ АВТОЗАПУСКОМ

Сначала — стандарт. Достаточно в командной строке набрать msconfig, и на вкладке «Автозагрузка» мы увидим все, что автоматически запускается по содержимому папки «Автозагрузка» и ключей в реестре HKCU\Software\Microsoft\Windows\CurrentVersion\Run и HKLM\Software\Microsoft\Windows\CurrentVersion\Run. К великому сожалению, это далеко не единственные места, откуда может быть дан старт вредоносному коду вместе с загрузкой системы, поэтому единственным достоинством этой утилиты является то, что она по умолчанию входит в состав Windows.

Совсем другое дело — Autoruns из комплекта SisInternals Suit. По мнению многих представителей нашего общества, это лучшее, что было создано из утилит для управления автозапуском. Кроме версии с GUI-интерфейсом, имеется консольная версия анализатора, в лучших традициях спецов старой школы. Утилита показывает множество различных методов автозапуска, начиная от классических способов (ключи Run, RunOnce, папка «Автозагрузка») и заканчивая расширениями Internet Explorer'а (BHO, панели инструментов), причем свежие версии программы периодически дополняются умением распознавать новые способы автозагрузки (на данный момент актуальна версия 11.0).

К сожалению, как иногда бывает, не обходится без ложки дегтя. Основной недостаток утилиты в том, что для анализа реестра в ней используются стандартные API-функции, и в случае их перехвата и последующего искажения содержимого ключей реестра вредоносным кодом Autoruns покажет искаженные данные. Для того чтобы этого избежать, можно, например, запустить Autoruns из-под WinDbg, снять с помощью отладчика перехваты функций и после этого, нажав в отладчике F5, проанализировать реестр с помощью уже исправленных API-функций.

УТИЛИТЫ ДЛЯ ПОИСКА МАСКИРУЕМЫХ ОБЪЕКТОВ (ФАЙЛОВ, КЛЮЧЕЙ РЕЕСТРА, ПРОЦЕССОВ)

RootkitRevealer — утилита из уже известного нам набора от SysInternals. Позволяет выполнять поиск маскируемых файлов и ключей реестра. Ее работа основана на прямом чтении диска (анализируются MFT — Master File Table NTFS-тома и структуры каталогов) и сравнении результатов с данными, полученными с помощью стандартных API-функций. Обнаруженные различия фиксируются.

Аналогичная процедура проводится с реестром — утилита снимает дамп содержимого реестра с помощью операций прямого чтения с диска и сравнивает результат с тем, что получилось при использовании стандартных API-функций для работы с реестром.

Достоинство программы в том, что она распознает скрытые файлы и ключи в реестре независимо от метода перехвата API-функций.

Утилита BlackLight от компании F-Secure позволяет обнаруживать скрытые процессы и файлы путем анализа системы на низком уровне.

Основное достоинство программы в эффективном способе поиска скрытых процессов (так называемый брутфорс PID).

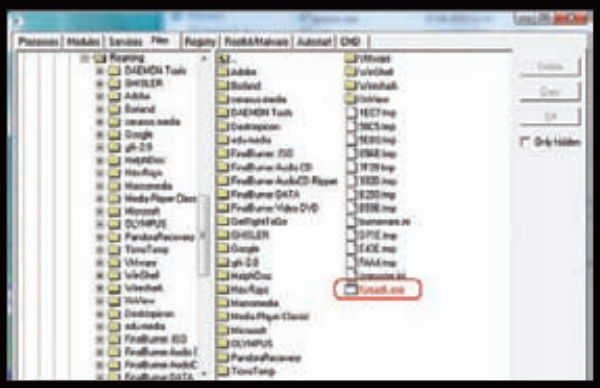
УНИВЕРСАЛЬНЫЕ УТИЛИТЫ

Помимо узконаправленных инструментов, хорошую службу в деле борьбы с вредоносным кодом могут сослужить универсальные утилиты, эдакие швейцарские ножи со множеством лезвий на все случаи жизни.

В первую очередь стоит отметить полезнейший и популярный в определенных кругах инструмент под названием GMER. Он умеет находить и показывать скрытые процессы, завершать их, показывать все загруженные модули и сервисы, искать скрытые файлы и ключи реестра. Помимо этого утилита может вести мониторинг запускаемых приложений, загружаемых драйверов, библиотек, обращений к реестру и работы TCP/IP-соединений. Вся получаемая информация может быть сохранена в лог-файлы для последующего анализа.

Ну и конечно же, здесь не обойтись без упоминания широко известной в определенных кругах программы под названием AVZ. Эта антивирусная утилита снискала себе заслуженную популярность среди борцов с малварью, а ее вердикт в виде лог-файла является своеобразным стандартом обмена информацией о результатах исследования системы между специалистами по антивирусной защите.

Вообще, данный противовирусный инструмент заслуживает отдельной статьи, поэтому мы лишь кратко перечислим его умения.



GMER обнаружил маскирующийся файл

AVZ в работе, найден скрытый процесс

Итак, утилита имеет следующие функции:

- поиск известных вредоносных программ по обновляемой сигнатурной базе;
- обновляемая база безопасных файлов;
- система обнаружения руткитов;
- восстановление системы;
- эвристический анализ системы;
- поиск клавиатурных шпионов;
- анализатор Winsock SPI/LSP-настроек;
- расширенный диспетчер процессов, сервисов и драйверов;
- поиск файлов на диске;
- поиск данных в реестре;
- анализатор открытых TCP/UDP-портов;
- расширенный диспетчер автозапуска;
- анализ NTFS-потоков;
- возможность разработки скриптов для проведения часто повторяемых операций по исследованию и восстановлению системы.

В общем, даже не швейцарский перочинный ножик, а целый антивирусный комбайн.

Итак, имея в кармане загрузочную флешку (о том, как ее сделать, мы уже не раз писали) с какой-нибудь из этих двух утилит (а лучше — с обеими), можно уже выступать на тропу войны с малварью и при этом не чувствовать себя совсем безоружным.

DVD

+ Все программы, упомянутые в статье, ищи на диске.

+ Не забудь посмотреть видео, которое демонстрирует снятие перехватов API-функций работы с реестром при использовании Autoruns.

INFO

Если вдруг ты сам захочешь написать продвинутую тулзу для завершения процессов, то ищи 139-й номер журнала, там Александр Эккерт любезно поделился несколькими интересными способами грохнуть процесс.

WARNING

Помни, что файловые вирусы (паразиты, присоединяющиеся к файлам, а то и шифрующие их содержимое) вовсе не ушли в прошлое. Не забывай слать подозрительные файлы в антивирусные конторы, не навреди себе самолечением!

WWW

• Если ты хочешь получить более подробную информацию о каком-нибудь процессе, иди на www.processlibrary.com.

• На www.nobunkum.ru/ru/rootkits-windbg лежит крайне интересная статья о применении отладчика WinDbg для обнаружения руткитов и борьбы с ними от Дмитрия Олексюка из Esage Lab.

• На www.esetnod32.ru/.support/winlock, sms.kaspersky.ru и на www.drweb.com/xperf/unlocker готовы оказать посильную помощь в разблокировке системы.