10 признаков заражения вашего компьютера вредоносным ПО (часть 1)

Уже почти никого не удивляет буквально ежедневный рост количества и многообразия вредоносного ПО и, как следствие, количества случаев заражения этим ПО компьютеров пользователей по всему миру.
В этом и последующем выпусках мы опишем 10 признаков (или, выражаясь языком врачей, симптомов) того, что ваш компьютер уже не совсем ваш.

1. **Компьютер работает необычно медленно.** Само по себе это не является однозначным признаком заражения (ведь компьютер может быть просто загружен ресурсоёмкими задачами – в таких условиях падение производительности неизбежно), однако, однозначно является поводом внимательно присмотреться к поведению компьютера. Вы стали замечать, что загрузка компьютера идёт слишком медленно, а программы работают необычно долго? И при этом компьютер не выполняет ресурсоёмкие задачи? Сначала необходимо исключить причины, не связанные с заражением вредоносным ПО, а именно уменьшение объёма доступной оперативной памяти, дефрагментацию дисковых массивов, перегрев процессора и ряд других. Если же все эти причины отсутствуют - время готовиться к борьбе за свой компьютер.
2. **Внезапно появляются всплывающие окна с нежелательным содержимым (реклама, порно-сайты и тому подобное).** Такие неизвестно откуда появляющиеся окна не только затрудняют использование интернета, но их ещё часто сложно закрыть, что справедливо раздражает. Это – явный признак наличия вредоносного ПО. Для его удаления необходимы специальные программы, такие как, например, Malwarebytes или Lavasoft Ad-Aware. Однако, и они не гарантируют устранение проблемы и невозможность повторного заражения. Лучший способ (как и при решении многих проблем в области информационной безопасности) – осторожное, внимательное и вдумчивое поведение пользователя. Иными словами, не загружайте и не устанавливайте незнакомое (особенно бесплатное) ПО (плагины, тулбары и т.д.), не открывайте сомнительные сайты и не нажимайте на незнакомые ссылки, не открывайте письма и вложения в них от неизвестных адресатов.
3. **Многократное аварийное завершение работы приложений или всего компьютера (иногда даже с появлением «синего экрана смерти»).** Подобные события могут быть следствием проблемы, связанной с аппаратным или программным обеспечением компьютера (например, несовместимость устройств или неправильная работа драйверов), или, как вы догадались, признаком наличия вредоносного ПО, мешающего нормальной работе компьютера. Как и в пункте 2, для устранения вредоносного ПО не обойтись без специализированных программ. Как правило, в большинстве случаев бывает достаточно хорошего антивируса с актуальной вирусной базой, которым необходимо просканировать весь компьютер, включая системные и почтовые папки и архивы.
4. **Подозрительно активная работа жёсткого диска компьютера.** Если вы не совершаете операции с файлами, не скачиваете на компьютер торренты или ПО, не играете в игры и активно не используете приложения, а компьютер, тем не менее, натужно «шуршит» винчестером – возможно, это результат деятельности вредоносного ПО, которое в этот самый момент или шифрует содержимое вашего жёсткого диска, чтобы потом потребовать с вас деньги за расшифровку, или «размножается» в ветвистой файловой системе компьютера, или рассылает свои копии всем, кого найдёт в вашей почте.
5. **Неожиданно быстро закончилось свободное место на жёстком диске.** Ещё недавно была свободна треть диска – и вот уже вылезает предупреждение операционной системы о том, что места почти нет! Если вы не скачивали больших объёмов данных на свой компьютер, не устанавливали игры, занимающие много места на диске, и не знаете, отчего могло бы так быстро закончиться место – скорее всего, снова придётся «расчехлять» антивирус.

10 признаков заражения вашего компьютера вредоносным ПО (часть 2)

Сегодня мы продолжаем (и заканчиваем) наш небольшой очерк о том, по каким признакам можно предположить заражение компьютера вредоносным ПО.

6. **Необычно высокая сетевая активность компьютера.** Вы ничего не скачиваете из интернета, не выполняется обновление операционной системы или приложений, браузер закрыт, а компьютер, тем не менее, ведёт небывало активную сетевую деятельность? Есть повод присмотреться к нему повнимательнее, и, если сетевая активность продолжается, или, хуже того, компьютер начинает вести себя странно (работает медленнее обычного, появляются всплывающие окна, самостоятельно запускаются приложения и тому подобное) – необходимо понять причину сетевой активности с помощью, например, программ Wireshark, GlassWire или Little Snitch, а также проверить компьютер ПО для удаления вредоносов (мы писали о нём в первой части) и антивирусом.
7. **Смена в браузере страницы, загружаемой по умолчанию, появление в браузере новых панелей инструментов, которые вы не ставили, а в истории посещений браузера - страниц, которые вы не посещали.** Если при открытии нового окна/вкладки в браузере по умолчанию загружается незнакомая вам страница, в браузере появилась новая панель инструментов, а вы не помните, чтобы её устанавливали, или в истории посещений браузера появились страницы, на которых вы никогда не были – это, скорее всего, свидетельство наличия вредоносного ПО, которое скачалось и установилось в результате посещения неблагонадёжного сайта или нажатия на подозрительную ссылку. Снова повод браться за антивредоносное ПО и антивирус…
8. **Появление неизвестных диалоговых окон (в том числе в процессе загрузки компьютера), самопроизвольная загрузка и закрытие приложений, уведомление Windows об отсутствии доступа к какому-либо из локальных дисков.** С одной стороны, всё это может быть следствием проблем с аппаратным и/или программным обеспечением. С другой – признаком заражения компьютера. Если потерян доступ к диску – готовьтесь к худшему: долгим попыткам восстановить доступ к данным с помощью специализированного ПО для работы с разделами жёсткого диска, возможной потере всех данных в затронутом разделе диска или переустановке операционной системы.
9. **Антивирус отключён полностью или отключена функция его обновления.** Понятно, что для любого вредоносного ПО или вируса антивирус – первейший враг. Поэтому очень часто, перед началом своей гнусной деятельности, вредоносное ПО старается снять защиту компьютера, то есть отключить антивирус. А если отключить антивирус полностью не получается, надо попытаться хотя бы отключить его обновление.
10. **Ваши коллеги, знакомые и/или родственники сообщают, что получили от вас сообщения, которых вы не отправляли.** Это могут быть сообщения электронной почты, сообщения, отправленные с ваших аккаунтов в социальных сетях или из мессенджеров. Часто такие сообщения содержат вложения, в которых, как правило, находится копия вируса или ссылка на ресурс, нажав на которую, адресат запустит автоматический процесс скачивания и установки вредоносного ПО уже на свой компьютер. Таким образом, от вредоносного ПО пострадаете не только вы, но и все, с кем вы так или иначе общаетесь.

    Для разрешения проблемы сначала необходимо установить конкретный источник отправки подобных сообщений. Проверьте папки отправленных сообщений и, если в них нет следов несанкционированной отправки сообщений, есть основания предполагать, что сообщения были отправлены от вашего имени сторонним ПО, которое может располагаться либо локально, то есть на вашем компьютере («расчехляем» антивирус), либо удалённо (в этом случае, вполне возможно, что сделать ничего нельзя). Если же сообщения были отправлены с ваших аккаунтов в социальных сетях или мессенджерах и видны в папке отправленных сообщений – вас взломали. В этом случае необходимо срочно менять пароли (и не использовать один и тот же пароль для разных учётных записей) и активировать функцию двухфакторной аутентификации (при наличии таковой).

Надеемся, описанные советы помогут вам избежать многих проблем!