Пользователи компьютеров Windows и Mac, смартфонов и планшетов находятся под постоянно растущей угрозой, исходящей от компьютерных вирусов и вредоносных программ. Принятие мер означает понимание того, с чем вы столкнулись. Рассмотрим основные типы вредоносных программ и их последствия.

Краткий обзор

Термин «вредоносное ПО» используется для описания любой вредоносной программы на компьютере или мобильном устройстве. Эти программы устанавливаются без согласия пользователей и могут вызывать ряд неприятных последствий, таких как снижение производительности компьютера, извлечение из системы персональных данных пользователя, удаление данных или даже воздействие на работу аппаратных средств компьютера. Поскольку киберпреступники придумывают все более сложные способы проникновения в системы пользователей, рынок вредоносных программ существенно расширился. Давайте рассмотрим некоторые из наиболее распространенных типов вредоносных программ, которые можно встретить в интернете.

1. Вирусы

Компьютерные вирусы получили свое название за способность «заражать» множество файлов на компьютере. Они распространяются и на другие машины, когда зараженные файлы отправляются по электронной почте или переносятся пользователями на физических носителях, например, на USB-накопителях или (раньше) на дискетах. По данным Национального института стандартов и технологий (NIST), первый компьютерный вирус под названием «Brain» был написан в 1986 году двумя братьями с целью наказать пиратов, ворующих ПО у компании. Вирус заражал загрузочный сектор дискет и передавался на другие компьютеры через скопированные зараженные дискеты.

2. Черви

В отличие от вирусов, червям для распространения не требуются вмешательства человека: они заражают один компьютер, а затем через компьютерные сети распространяются на другие машины без участия их владельцев. Используя уязвимости сети, например, недостатки в почтовых программах, черви могут отправлять тысячи своих копий и заражать все

новые системы, и затем процесс начинается снова. Помимо того, что многие черви просто «съедают» системные ресурсы, снижая тем самым производительность компьютера, большинство из них теперь содержит вредоносные «составляющие», предназначенные для кражи или удаления файлов.

3. Рекламное ПО

Одним из наиболее распространенных типов вредоносных программ является рекламное ПО. Программы автоматически доставляют рекламные объявления на хост-компьютеры. Среди разновидностей Adware - всплывающие рекламные объявления на веб-страницах и реклама, входящая в состав «бесплатного» ПО. Некоторые рекламные программы относительно безвредны, в других используются инструменты отслеживания для сбора информации о вашем местонахождении или истории посещения сайтов и вывода целевых объявлений на экран вашего компьютера. BetaNews сообщил об обнаружении нового типа рекламного ПО, который может отключить антивирусную защиту. Поскольку Adware устанавливается с согласия пользователя, такие программы нельзя назвать вредоносными: обычно они идентифицируются как «потенциально нежелательные программы».

4. Шпионское ПО

Шпионское ПО делает то, что предполагает его название - следит за вашими действиями на компьютере. Оно собирает информацию (например, регистрирует нажатия клавиш на клавиатуре вашего компьютера, отслеживает, какие сайты вы посещаете и даже перехватывает ваши регистрационные данные), которая затем отправляется третьим лицам, как правило, киберпреступникам. Оно также может изменять определенные параметры защиты на вашем компьютере или препятствовать сетевым соединениям. Как пишет TechEye, новые типы шпионских программ позволяют злоумышленникам отслеживать поведение пользователей (естественно, без их согласия) на разных устройствах.

5. Программы-вымогатели

Программы-вымогатели заражают ваш компьютер, затем шифруют конфиденциальные данные, например, личные документы или фотографии, и требуют выкуп за их расшифровку. Если вы отказываетесь платить, данные удаляются. Некоторые типы программ-вымогателей могут полностью

заблокировать доступ к вашему компьютеру. Они могут выдавать свои действия за работу правоохранительных органов и обвинить вас в каких-либо противоправных поступках. В июне 2015 года в Центр приёма жалоб на мошенничество в Интернете при ФБР обратились пользователи, сообщившие о финансовых потерях на общую сумму 18 000 000 долларов в результате деятельности вируса-вымогателя CryptoWall.

6. Боты

Боты - это программы, предназначенные для автоматического выполнения определенных операций. Они могут использоваться для легитимных целей, но злоумышленники приспособили их для своих вредоносных целей. Проникнув в компьютер, боты могут заставить его выполнять определенные команды без одобрения или вообще без ведома пользователя. Хакеры могут также пытаться заразить несколько компьютеров одним и тем же ботом, чтобы создать бот-сеть, которая затем будет использоваться для удаленного управления взломанными машинами - красть конфиденциальные данные, следить за действиями жертвы, автоматически распространять спам или запускать разрушительные DDoS-атаки в компьютерных сетях.

7. Руткиты

Руткиты позволяют третьей стороне получать удаленный доступ к компьютеру и управлять им. Эти программы используются IT-специалистами для дистанционного устранения сетевых проблем. Но в руках злоумышленников они превращаются в инструмент мошенничества: проникнув в ваш компьютер, руткиты обеспечивают киберпреступникам возможность получить контроль над ним и похитить ваши данные или установить другие вредоносные программы. Руткиты умеют качественно маскировать свое присутствие в системе, чтобы оставаться незамеченными как можно дольше. Обнаружение такого вредоносного кода требует ручного мониторинга необычного поведения, а также регулярного внесения корректировок в программное обеспечение и операционную систему для исключения потенциальных маршрутов заражения.

8. Троянские программы

Более известные как троянцы, эти программы маскируются под легитимные файлы или ПО. После скачивания и установки они вносят изменения в

систему и осуществляют вредоносную деятельность без ведома или согласия жертвы.

9. Баги

Баги - ошибки в фрагментах программного кода - это не тип вредоносного ПО, а именно ошибки, допущенные программистом. Они могут иметь пагубные последствия для вашего компьютера, такие как остановка, сбой или снижение производительности. В то же время баги в системе безопасности - это легкий способ для злоумышленников обойти защиту и заразить вашу машину. Обеспечение более эффективного контроля безопасности на стороне разработчика помогает устранить ошибки, но важно также регулярного проводить программные корректировки, направленные на устранение конкретных багов.

Мифы и факты

Существует ряд распространенных мифов, связанных с компьютерными вирусами:

Любое сообщение об ошибке компьютера указывает на заражение вирусом. Это неверно: сообщения об ошибках также могут быть вызваны ошибками аппаратного или программного обеспечения.

Вирусам и червям всегда требуется взаимодействие с пользователем. Это не так. Для того чтобы вирус заразил компьютер, должен быть исполнен код, но это не требует участия пользователя. Например, сетевой червь может заражать компьютеры пользователей автоматически, если на них имеются определенные уязвимости.

Вложения к электронным письмам от известных отправителей являются безопасными. Это не так, потому что эти вложения могут быть заражены вирусом и использоваться для распространения заражения. Даже если вы знаете отправителя, не открывайте ничего, что в чем вы не уверены.

Антивирусные программы могут предотвратить заражение. Со своей стороны, поставщики антивирусного ПО делают все возможное, чтобы не отставать от разработчиков вредоносных программ, но пользователям обязательно следует установить на своем компьютере комплексное защитное решение класса Internet security, который включает в себя технологии, специально предназначенные для активного блокирования угроз. Даже при

том, что 100-процентной защиты не существует. Нужно просто осознанно подходить к обеспечению собственной онлайн-безопасности, чтобы уменьшить риск подвергнуться атаке.

Вирусы могут нанести физический ущерб вашему компьютеру. Что если вредоносный код приведет к перегреву компьютера или уничтожит критически важные микрочипы? Поставщики защитных решений неоднократно развенчивали этот миф - такие повреждения просто невозможны.

Между тем, рост количества устройств взаимодействующих друг с другом в Интернете Вещей (IoT), открывает дополнительные интересные возможности: что если зараженный автомобиль съедет с дороги, или зараженная «умная» печь продолжит нагреваться, пока не случится превышение нормальной нагрузки? Вредоносного ПО будущего может сделать такой физический ущерб реальностью.

У пользователей есть ряд неправильных представлений о вредоносных программах: например, многие считают, что признаки заражения всегда заметны и поэтому они смогут определить, что их компьютер заражен. Однако, как правило, вредоносное ПО не оставляет следов, и ваша система не будет показывать каких-либо признаков заражения.

Tweet: Как правило, вредоносное ПО не оставляет следов, и ваша система не будет показывать каких-либо признаков заражения. Твитни это!

Так же не стоит верить, что все сайты с хорошей репутацией безопасны. Они также могут быть взломаны киберпреступниками. А посещение зараженного вредоносным кодом легитимного сайта – еще большая вероятность для пользователя расстаться со своей личной информацией. Именно это, как пишет SecurityWeek, произошло с Всемирным банком. Также многие пользователи считают, что их личные данные - фотографии, документы и файлы - не представляют интереса для создателей вредоносных программ. Киберпреступники же используют общедоступные данные для того, чтобы атаковать отдельных пользователей, или собрать информацию, которая поможет им создать фишинговые письма, чтобы проникнуть во внутренние сети организаций.

Стандартные методы заражения

Итак, как же происходит заражение компьютерными вирусами или вредоносными программами? Существует несколько стандартных способов. Это ссылки на вредоносные сайты в электронной почте или сообщениях в социальных сетях, посещение зараженного сайта (известного как drive-by загрузка) и использование зараженного USB-накопителя на вашем компьютере. Уязвимости операционной системы и приложений позволяют злоумышленникам устанавливать вредоносное ПО на компьютеры. Поэтому для снижения риска заражения очень важно устанавливать обновления для систем безопасности, как только они становятся доступными.

Киберпреступники часто используют методы социальной инженерии, чтобы обманом заставить вас делать что-то, что угрожает вашей безопасности или безопасности вашей компании. Фишинговые сообщения являются одним из наиболее распространенных методов. Вы получаете на вид абсолютно легитимное электронное сообщение, в котором вас убеждают загрузить зараженный файл или посетить вредоносный веб-сайт. Цель хакеров - написать сообщение так, чтобы вы нашли его убедительным. Это может быть, например, предупреждение о возможном вирусном заражении или уведомление из вашего банка или сообщение от старого друга.

Конфиденциальные данные, такие как пароли, являются главной целью киберпреступников. Помимо использования вредоносных программ для перехвата паролей в момент их ввода, злоумышленники также могут собирать пароли с веб-сайтов и других компьютеров, которые они взломали. Вот почему так важно использовать уникальный и сложный пароль для каждой учетной записи. Он должен состоять из 15 и более символов, включающих буквы, цифры и специальные символы. Таким образом, если киберпреступникам удастся взломать один аккаунт, они не получат доступ ко всем вашим учетным записям. К сожалению, большинство пользователей имеют очень слабые пароли: вместо того, чтобы придумать труднодоступную комбинацию, они обращаются к standby-паролям типа «123456» или «Password123», которые преступники легко подбирают. Даже контрольные вопросы не всегда могут служить эффективной защитой, потому что многие люди дают один и тот же ответ на вопрос «Ваша любимая еда?», например, если вы находитесь в Соединенных Штатах, то почти наверняка ответ будет - «Пицца».

Признаки заражения

Хотя большинство вредоносных программ не оставляет никаких явных следов, и ваш компьютер работает нормально, иногда все же можно заметить признаки возможного заражения. Самый первый из них - снижение производительности, т.е. процессы происходят медленные, загрузка окон занимает больше времени, в фоновом режиме работают какие-то случайные программы. Еще одним настораживающим признаком может считаться измененных домашних интернет-страниц в вашем браузере или более частое, чем обычно, появление всплывающих объявлений. В некоторых случаях вредоносное ПО даже может влиять на базовые функции компьютера: не открывается Windows, нет подключения к Интернету или доступа к более высокоуровневым функциям управления системой. Если вы подозреваете, что ваш компьютер может быть заражен, немедленно произведите проверку системы. Если заражение не обнаружено, но вы все еще сомневаетесь, получите второе мнение - запустите альтернативный антивирусный сканер.

Users of Windows and Mac computers, smartphones and tablets are under an ever-growing threat from computer viruses and malware. Taking action means understanding what you are facing. Consider the main types of malware and their consequences.

Short review

The term “malware” is used to describe any malware on a computer or mobile device. These programs are installed without the consent of users and can cause a number of unpleasant consequences, such as reduced computer performance, retrieving user personal data from the system, deletion of data, or even an impact on the operation of computer hardware. As cybercriminals come up with increasingly sophisticated ways of penetrating users' systems, the malware market has expanded significantly. Let's look at some of the most common types of malware that can be found on the Internet.

1. Viruses

Computer viruses got their name for the ability to "infect" many files on the computer. They also spread to other machines when infected files are sent via email or transferred by users on physical media, such as USB drives or (earlier) on diskettes. According to the National Institute of Standards and Technology (NIST), the first computer virus called “Brain” was written in 1986 by two brothers to punish pirates who steal software from the company. The virus infects the boot sector of floppy disks and is transmitted to other computers through copied infected floppies.

2. Worms

Unlike viruses, worms do not require human intervention to spread: they infect one computer and then spread through computer networks to other machines without the participation of their owners. Using network vulnerabilities, such as flaws in email programs, worms can send thousands of copies of themselves and infect all new systems, and then the process begins again. In addition to the fact that many worms simply "eat up" system resources, thereby reducing computer performance, most of them now contain malicious "components" designed to steal or delete files.

3. Adware

One of the most common types of malware is adware. Programs automatically deliver advertisements to host computers. Among the varieties of Adware are pop-up advertisements on web pages and ads that are part of “free” software. Some adware programs are relatively harmless, others use tracking tools to gather information about your location or history of visiting sites and display targeted ads on your computer screen. BetaNews announced the discovery of a new type of adware that can disable anti-virus protection. Since Adware is installed with the user's consent, such programs cannot be called malicious: they are usually identified as “potentially unwanted programs”.

4. Spyware

Spyware does what its name implies - monitors your actions on the computer. It collects information (for example, it registers keystrokes on the keyboard of your computer, tracks which sites you visit and even intercepts your registration data), which is then sent to third parties, usually cybercriminals. It can also change certain security settings on your computer or interfere with network connections. According to TechEye, new types of spyware allow attackers to monitor user behavior (of course, without their consent) on different devices.

5. Ransomware programs

Ransomware infects your computer, then encrypts sensitive data, such as personal documents or photos, and requires a ransom for their decryption. If you refuse to pay, the data is deleted. Some types of ransomware programs can completely block access to your computer. They can impersonate their actions for the work of law enforcement agencies and accuse you of any unlawful acts. In June 2015, users who reported a financial loss totaling $ 18,000,000 as a result of the ransomware virus CryptoWall applied to the FBI Internet Reception Center for complaints about fraud on the FBI.

6. Bots

Bots are programs designed to automatically perform certain operations. They can be used for legitimate purposes, but attackers have adapted them for their malicious purposes. Having entered a computer, bots can force it to execute certain commands without approval or without the user's knowledge at all. Hackers can also try to infect several computers with the same bot to create a botnet, which will then be used to remotely control hacked machines — steal confidential data,

monitor victim actions, automatically spread spam, or launch destructive DDoS attacks on computer networks.

7. Rootkits

Rootkits allow a third party to remotely access and control a computer. These programs are used by IT specialists to remotely resolve network problems. But in the hands of intruders, they turn into a fraud tool: penetrating your computer, rootkits provide cybercriminals with the opportunity to gain control over it and steal your data or install other malicious programs. Rootkits are able to qualitatively mask their presence in the system in order to remain unnoticed for as long as possible. Detection of such malicious code requires manual monitoring of unusual behavior, as well as regular adjustments to the software and operating system to eliminate potential infection routes.

8. Trojan programs

Better known as Trojans, these programs are disguised as legitimate files or software. After downloading and installing they make changes to the system and carry out malicious activities without the knowledge or consent of the victim.

9. Bugs

Bugs - errors in fragments of a program code are not a type of malware, but errors made by a programmer. They can be detrimental to your computer, such as stopping, crashing, or slowing performance. At the same time, security bugs are an easy way for intruders to bypass the protection and infect your machine. Providing more effective security controls on the developer’s side helps to eliminate errors, but it is also important to regularly make programmatic adjustments to eliminate specific bugs.

Myths and Facts

There are a number of common computer virus-related myths:

Any computer error message indicates a virus infection. This is incorrect: error messages may also be caused by hardware or software errors.

Viruses and worms always need user interaction. This is not true. In order for a virus to infect a computer, code must be executed, but this does not require user

input. For example, a network worm can infect users' computers automatically if they have certain vulnerabilities.

Email attachments from reputable senders are secure. This is not the case because these attachments can be infected with a virus and used to spread the infection. Even if you know the sender, do not reveal anything that you are not sure about.

Antivirus programs can prevent infection. For their part, anti-virus vendors are doing everything possible to keep up with malware developers, but users must install on their computers a comprehensive Internet security class security solution that includes technologies specifically designed to actively block threats. Even though 100% protection does not exist. You just need to consciously approach to ensuring your own online security to reduce the risk of being attacked.

Viruses can cause physical damage to your computer. What if malicious code overheats the computer or destroys critical microchips? Suppliers of protective solutions have repeatedly debunked this myth - such damage is simply impossible.

Meanwhile, the growth in the number of devices interacting with each other on the Internet of Things (IoT) opens up additional interesting possibilities: what if an infected car drives off the road, or does an infected smart oven continue to heat up until normal load exceeds Future malware can make such physical damage a reality.

Users have a number of misconceptions about malware: for example, *many believe that signs of infection are always noticeable and therefore they can determine that their computer is infected.* However, as a rule, malware does not leave traces, and your system will not show any signs of infection.

Tweet: (можно оформить прям как в твиттере)

As a rule, malware leaves no trace, and your system will not show any signs of infection. Tweet it!

Just *do not believe that all sites with a good reputation are safe*. They can also be hacked by cybercriminals. A visit to a legitimate website infected with a malicious code is an even greater chance for a user to part with his personal information. This, SecurityWeek writes, happened to the World Bank. Also, many users believe that their personal data - photos, documents and files - are of no interest to the creators of malware. Cybercriminals use publicly available data to attack

individual users, or to gather information that will help them create phishing emails in order to penetrate the internal networks of organizations.

Standard infection methods

So, how does a computer virus or malware infection occur? There are several standard methods. These are links to malicious websites in emails or posts on social networks, a visit to an infected site (known as drive-by download) and the use of an infected USB drive on your computer. Vulnerabilities in the operating system and applications allow attackers to install malware on computers. Therefore, to reduce the risk of infection, it is very important to install security updates as they become available.

Cybercriminals often use social engineering techniques to trick you into doing something that threatens your security or the security of your company. Phishing messages are one of the most common methods. You get a seemingly absolutely legitimate email message in which you are persuaded to download an infected file or visit a malicious website. The goal of hackers is to write a message so that you find it convincing. This may be, for example, a warning about a possible virus infection or a notice from your bank or a message from an old friend.

Confidential data, such as passwords, is the main target of cybercriminals. In addition to using malware to intercept passwords when they are entered, attackers can also collect passwords from websites and other computers that they have cracked. That is why it is so important to use a unique and complex password for each account. It must consist of 15 or more characters, including letters, numbers and special characters. Thus, if cybercriminals succeed in hacking one account, they will not get access to all your accounts. Unfortunately, most users have very weak passwords: instead of coming up with a hard-to-use combination, they access standby-type passwords like “123456” or “Password123”, which criminals easily pick up. Even control questions can not always serve as an effective defense, because many people give the same answer to the question “Your favorite food?”, For example, if you are in the United States, then almost certainly the answer will be “Pizza”.

Signs of infection

Although most malware does not leave any obvious traces, and your computer works fine, sometimes you can still notice signs of a possible infection. The very

first of them is a decrease in performance, i.e. processes are slow, loading windows takes longer, some random programs are running in the background. Another warning sign can be considered as modified home pages in your browser or more frequent than usual pop-up ads. In some cases, malware can even affect the basic functions of a computer: Windows does not open, there is no connection to the Internet or access to higher-level system management functions. If you suspect your computer may be infected, immediately check your system. If the infection is not detected, but you are still in doubt, get a second opinion - run an alternative anti-virus scanner.