История возникновения компьютерных вирусов

Идея компьютерных вирусов впервые обсуждалась в серии лекций математика Джона фон Неймана в конце 1940-х годов;

В 1966 году вышла его монография «Теория самовоспроизводящихся автоматов» – по сути, это мысленный эксперимент, рассматривающий возможность существования «механического» организма – например, компьютерного кода – который бы повреждал машины, создавал собственные копии и заражал новые машины аналогично тому, как это делает биологический вирус.

История компьютерных вирусов делится на несколько этапов:

- **Доисторический.** Вирусы-легенды и документально подтверждённые инциденты на «мейнфреймах» 1950-80-х годов.
- **«До-интернетовский».** В основном ему присущи «классические вирусы» для MS-DOS.
- **Интернет-этап.** Многочисленные черви, эпидемии, приводящие к колоссальным убыткам.
- **Современный, криминальный этап.** Использование интернета в преступных целях.

Появление первых компьютерных вирусов, способных дописывать себя к файлам, связывают с инцидентом, который произошел в первой половине 70-х годов на системе Univax 1108. Вирус, получивший название «Pervading Animal», дописывал себя к выполняемым файлам – делал практически то же самое, что тысячи современных компьютерных вирусов.

Можно отметить, что в те времена значимые события, связанные с компьютерными вирусами, происходили один раз в несколько лет. С началом 80-х компьютеры становятся все более и более популярными. Появляется все больше и больше программ, начинают развиваться глобальные сети. Результатом этого является появление большого числа разнообразных «троянских коней» – программ, которые при их запуске наносят системе какой-либо вред. В 1986 г. произошла первая эпидемия IBM-PC вируса «Brain». Вирус, заражающий 360Кб дискеты, практически мгновенно разошелся по всему миру. Причиной такого «успеха» являлась, скорее всего, неготовность компьютерного общества к встрече с таким явлением, как компьютерный вирус.

В 1987 г. произошло событие, которое популяризировало «компьютерные вирусы». Код вируса «Vienna» впервые публикуется в книге Ральфа Бюргера «Computer Viruses: A High Tech Desease». Сразу же в 1987 г. появляются несколько вирусов для IBM-PC.

В пятницу 13-го мая 1988-го года сразу несколько фирм и университетов нескольких стран мира «познакомились» с вирусом «Jerusalem» – в этот день вирус уничтожал файлы при их запуске. Вместе с несколькими другими вирусами, вирус «Jerusalem» распространился по тысячам компьютеров, оставаясь незамеченным – антивирусные программы еще не были распространены в то время так же широко как сегодня, а многие пользователи и даже профессионалы еще не верили в существование компьютерных вирусов. Не прошло и полгода, как в ноябре повальная эпидемия сетевого вируса Морриса (другое название – Internet Worm) заразила более 6000 компьютерных систем в США и практически парализовала их работу. По причине ошибки в коде вируса он неограниченно рассылал свои копии по другим компьютерам сети и, таким образом, полностью забрал под себя ее ресурсы. Общие убытки от вируса Морриса были оценены в 96 миллионов долларов.

В 1992 году появились первые конструкторы вирусов VCL и PS-MPC, которые увеличили и без того немаленький поток новых вирусов. В конце этого года первый вирус для Windows, заражающий выполняемые файлы этой операционной системы, открыл новую страницу компьютерных вирусов.

В дальнейшем развитие компьютерных вирусов напоминает сводку с полей сражений. Создатели вирусов становятся все более изощренными, количество антивирусных программ растет, но ни одна из них не защищает в полной мере. В компьютерном обществе появляется синдром «компьютерного вируса».

К борьбе с вирусами подключаются правоохранительные органы: летом 1994 года автор вируса SMEG был арестован. Примерно в то же самое время в той же Великобритании арестована целая группа вирусописателей, называвшая себя ARCV (Assotiation for Really Cruel Viruses). Некоторое время спустя еще один автор вирусов был арестован в Норвегии.

Август 1995 г. один из поворотных моментов в истории вирусов и антивирусов: обнаружен первый вирус для Microsoft Word («Concept»). Так начиналось время макровирусов.

В 1998 году появились первые полиморфные Windows32-вирусы-»Win95. HPS» и «Win95. Marburg». Разработчикам антивирусных программ пришлось спешно адаптировать к новым условиям методики детектирования полиморфных вирусов, рассчитанных до того только на DOS-вирусы.

Наиболее заметной в 1998 г. была эпидемия вируса «Win95. CIH», ставшая сначала массовой, затем глобальной, а затем повальной – сообщения о заражении

компьютерных сетей и домашних персональных компьютеров исчислялись сотнями, если не тысячами. Начало эпидемии зарегистрировано на Тайване, где неизвестный заслал зараженные файлы в местные Интернет-конференции.

С середины 90-х годов основным источником вирусов становится глобальная сеть Интернет.

26 марта 1999 г. происходит эпидемия вируса Melissa. Тогда это был вирус нового типа. Он распространялся по электронной почте в присоединенном файле, и после того как пользователь открывал этот файл, вирус рассылал себя по первым 50 адресам в адресной книги почтовой программы Microsoft Outlook. Он не наносил никакого ущерба самому компьютеру, но порождал лавину новых писем, и из-за перегрузки выходили из строя корпоративные серверы.

С 1999 года макровирусы начинают постепенно терять свое господство. Это связано со многими факторами. Во-первых, пользователи осознали опасность, таящуюся в простых doc- и xls-файлах. Люди стали более внимательными, научились пользоваться стандартными механизмами защиты от макровирусов, встроенными в MS Office.

В 2000 году происходят очень важные изменения на мировой «вирусной арене». На свет появляется новый тип вредных кодов – сетевые черви. В это же время появляется супервирус – «Чернобыль». «Чернобыль» исполняемый вирус под Windows, имеющий следующие особенности.

Во-первых, зараженный файл не меняет своего размера по сравнению с первоначальным вариантом. Такой эффект достигается благодаря структуре исполняемых файлов Windows: каждый exe-файл разбит на секции, выровненные по строго определенным границам. В результате между секциями почти всегда образуется небольшой зазор. Хотя такая структура приводит к увеличению места, занимаемого файлом на диске, она же позволяет существенно повысить скорость работы операционной системы с таким файлом. «Чернобыль» либо записывает свое тело в один такой зазор, либо дробит свой код на кусочки и копирует каждый из них в пустое место между границами. В результате антивирусу сложнее определить, заражен ли файл или нет, и еще сложнее вылечить инфицированный объект.

Во-вторых, «Чернобыль» стал первопроходцем среди программ, умеющих портить аппаратные средства. Некоторые микросхемы позволяют перезаписывать данные, хранящиеся в их мини ПЗУ. Этим и занимается этот вирус.

2000 год еще можно назвать годом «Любовных Писем». Вирус «LoveLetter», обнаруженный 5 мая, мгновенно разлетелся по всему миру, поразив десятки миллионов компьютеров практически во всех уголках планеты. Причины этой глобальной эпидемии кроются в чрезвычайно высокой скорости распространения. Вирус рассылал свои копии немедленно после заражения системы по всем адресам

электронной почты, найденным в адресной книге почтовой программы Microsoft Outlook. Подобно обнаруженному весной 1999 года вирусу Melissa, LoveLetter это делал, якобы, от имени владельца зараженного компьютера, о чем тот, естественно, даже не догадывался. Немаловажную роль при распространении вируса сыграл и психологический аспект: мало кто сможет удержаться, чтобы не прочитать любовное письмо от своего знакомого. Именно на это была сделана основная ставка в процессе разработки вируса. О масштабах заражения вирусами в начале 21 века свидетельствует тот факт, что только в мае атаке вируса LoveLetter подверглись более 40 миллионов компьютеров. Уже за первые 5 дней эпидемии вирус нанес мировой экономике убытки в размере 6,7 миллиардов долларов.

С 2000 года сетевые черви начинают полностью преобладать на вирусной арене мира. По данным Лаборатории Касперского, на их долю приходится 89,1 % всех заражений. В структуре распространенности сетевых червей традиционно преобладают почтовые, использующие e-mail в качестве основного транспорта для доставки на целевые компьютеры.

В 2001 году был обнаружен новый тип вредоносных кодов, способных активно распространяться и работать на зараженных компьютерах без использования файлов – «бестелесные черви». В процессе работы такие вирусы существуют исключительно в системной памяти, а при передаче на другие компьютеры - в виде специальных пакетов данных.

Такой поворот событий поставил сложные задачи перед разработчиками антивирусных пакетов. Традиционные технологии (антивирусный сканер и монитор) проявили неспособность эффективно противостоять новой угрозе, поскольку их алгоритм борьбы с вредоносными программами основан именно на перехвате файловых операций. Решением проблемы стал специальный антивирусный фильтр, который в фоновом режиме проверяет все поступающие на компьютер пакеты данных и удаляет «бестелесных» червей. Глобальная эпидемия сетевого червя CodeRed, начавшаяся 20 июля 2001 года, подтвердила действенность технологии «бестелесности». Но еще серьезнее оказалась эпидемия вируса Helkern' 25 января 2003 года.

В сентябре 2010 года вирус Stuxnet поразил компьютеры сотрудников АЭС в Бушере (Иран) и создал проблемы в функционировании центрифуг комплекса по обогащению урана в Натанзе. По мнению экспертов, Stuxnet стал первым вирусом, который был использован как кибероружие.

В 2014 г. появилась и сразу поставила под угрозу множество интернет-серверов угроза Heartbleed.

12 мая 2017 года значительное число компьютеров с операционной системой Windows подверглось атаке вируса-вымогателя WannaCry (англ. "хочу плакать").

27 июня 2017 года от атаки компьютерного вируса - шифровальщика Petya.A пострадали десятки компаний в РФ и на Украине. По сообщению Group-IB, которая занимается предотвращением и расследованием киберпреступлений, в России атаке подверглись компьютерные системы "Роснефти", "Башнефти", "Евраза", российских офисов компаний Mars, Mondeles и Nivea. На Украине вирусной атаке подверглись компьютеры "Киевэнерго", "Укрэнерго", "Ощадбанка" и концерна "Антонов". Также из-за вируса временно отключился автоматический мониторинг промышленной площадки на Чернобыльской АЭС. Вирус Petya распространяется через ссылки в сообщениях электронной почты и блокирует доступ пользователя к жесткому диску компьютера, требуя выкуп в размере $300 в биткойнах. Этим он схож с вредоносной программой WannaCry, с которой была связана предыдущая крупная вирусная атака в мае 2017 года.

2020 - Червь-вымогатель WastedLocker прицельно атаковал фирму Garmin и потребовал 10 миллионов долларов. Взлом больницы в Дюссельдорфе привел к смерти человека.

Современные вирусы пишутся уже не только для ПК, но и для устройств под управлением Android, iOS и других мобильных ОС. Однако принцип их действия всё тот же, и в целом они укладываются в приведённую выше классификацию.

Кибепреступники по-прежнему используют любую возможность причинить вред другим в корыстных целях. Вот и недавно объявленная пандемия COVID-19 стала почвой для злоумышленников, стремящихся завладеть пользовательскими ценными данными. Так, в марте было запущено новое приложение, ворующее данные пользователей под видом приложения от ВОЗ по короновирусу. Запуская его, активируется троянец, который начинает собирать и пересылать своему создателю информацию об аккаунтах пользователей.

Также было организовано несколько кибератак на медицинские учреждения — одни злоумышленники пытались парализовать работу больниц, а другие (разработчики программы-вымогателя Maze) попытались заработать на шантаже, пообещав в случае невыполнения материальных требований слить данные о пациентах одного исследовательского центра в сеть. Денег вымогатели не получили, поэтому данные всех бывших пациентов были обнародованы.

Немного подробнее о некоторых из вышеперечисленных

Программа Creeper

Как отмечается на сайте Discovery, программа Creeper, о которой часто говорят как о первом вирусе, была создана в 1971 году сотрудником компании BBN Бобом Томасом. По факту, Creeper был создан как тестовая программа, чтобы проверить, возможна ли в принципе самовоспроизводящаяся программа. Оказалось, что в некотором смысле возможна. Заразив новый жесткий диск, Creeper пытался удалить себя с предыдущего компьютера. Creeper не совершал никаких вредоносных действий – он только выводил простое сообщение: "I'M THE CREEPER. CATCH ME IF YOU CAN!" (Я CREEPER. ПОЙМАЙ МЕНЯ, ЕСЛИ СМОЖЕШЬ!)

Вирус Rabbit

Согласно сайту InfoCarnivore, вирус Rabbit (также известный как Wabbit) был создан в 1974 г. с вредоносной целью и мог самовоспроизводиться. Попав на компьютер, он делал большое количество копий себя, значительно ухудшал работоспособность системы и в итоге приводил к отказу компьютера. Имя («Кролик») было дано вирусу из-за того, что он очень быстро самовоспроизводился.

Первый троянец

Согласно сайту Fourmilab, первый троянец по названием ANIMAL (хотя есть споры относительно того, были ли это действительно троянец или просто вирус) был разработан компьютерным программистом Джоном Уолкером в 1975 г. В то время были очень популярны компьютерные игры, в которых пользователь загадывал какое-нибудь животное, а программа должна была его угадать за 20 вопросов. Уолкер написал одну из таких игр, и она стала популярной. Чтобы поделиться ее со своими друзьями, Уолкер записывал и передавал ее на магнитной ленте. Чтобы упростить эту процедуру, Уолкер создал программу PERVADE, которая устанавливалась на компьютер вместе с игрой ANIMAL. Пока пользователь играл в игру, PREVADE проверял все доступные пользователю директории на компьютере, а затем копировал ANIMAL во все директории, где этой программы не было. Вредоносной цели здесь не было, но ANIMAL и PREVADE подпадают под определение троянца: по сути, внутри программы ANIMAL была запрятана другая программа, которая выполняла действия без согласия пользователя.

Вирус загрузочного сектора Brain

Brain, первый вирус для IBM-совместимых компьютеров, появился в 1986 году – он заражал пятидюймовые дискеты. Как сообщает Securelist, вирус был написан двумя братьями – Баситом и Амджадом Фаруком Алви, которые держали компьютерный магазин в Пакистане. Братьям надоело, что покупатели нелегально копировали купленное у них ПО, и они создали этот вирус, которые заражал загрузочные сектора дискет. Brain заодно оказался и первым вирусом-невидимкой: при обнаружении попытки чтения зараженного сектора диска вирус незаметно подставлял его незараженный оригинал. Также он записывал на дискету фразу «(c) Brain», но при этом не портил никаких данных.

Вирус Иерусалим (Jerusalem)

В 1988 году была отмечена эпидемия компьютерного вируса Иерусалим, который был запрограммирован на особенно разрушительные действия, если активировался в пятницу 13-го. Вирус Иерусалим появился в Израиле в конце 1987 г. Это первый известный вирус, заражавший EXE-файлы достаточно универсальным способом. Проявил себя в Европе, США, на Ближнем Востоке.Первый удар данного вируса пришелся на пятницу 13. Все последующие активности данного вируса связаны только с 13 днём месяца, при условии, конечно же, что это пятница. Всё оставшееся время вирус спокойно и весьма доброжелательно распространялся по всему миру, что обеспечило его достаточно большую «популярность», а так же принесло звание первого в мире компьютерного вируса, который вызвал пандемию. Из всех деструктивных действий вируса Иерусалим можно выделить два основных: -вирус удалял все файлы, которые тем или иным образом были запущены в пятницу 13; -особое внимание в данном процессе вирус уделял приложениям. Через 30 минут после запуска компьютера вирус Иерусалим замедлял работу компьютера в 5 раз. Чтобы провернуть такую операцию, вирус изменял время прерывания процессов, которые в свою очередь некоторое время просто-напросто валяли дурака, прежде чем выполнить то, о чем просил его пользователь. Иерусалим был первоначально очень характерен (для вируса дня) и породил большое количество разновидностей. Однако, начиная с появления Windows, эти перерывы ДОСА больше не используются, таким образом, Иерусалим и его разновидности стали устаревшими.

"Чернобыль"

2 июня 1997 года студент Датунского университета (Тайбэй, Тайвань; КНР) Чэнь Инхао создал первую версию вируса Chernobyl ("Чернобыль" или CIH - по первым слогам имени автора). Вирус заражал компьютеры с операционными системами Windows 95 и 98. 26 апреле 1999 года виртуальный мир узнал о новой угрозе —

смертоносном для информации и ОС тайваньском вирусе. «Чернобыль» не только уничтожал файлы на жёстких дисках пользователей, но даже повреждал предустановленную систему BIOS, заразив таким образом около 500 тысяч ПК по всему миру. Впрочем, до массового распространения своего вируса тайваньский студент Чэнь Инхао (в 2000 году он был арестован, но затем отпущен) сначала потренировался «на кошках», беспечно заразив в июне 1998 года компьютеры родного университета, а затем под уже не контролируемую атаку вируса попали американские серверы, распространявшие компьютерные игры. Как потом выяснилось, ничего плохого Чэнь не замышлял, а вирус создал просто забавы ради, и после массового заражения переживал так сильно, что даже публично извинился перед пользователями китайского интернета, которые больше всего пострадали от «Чернобыля».

Melissa

Эпидемия вируса Melissa началась 26 марта 1999 г. Тогда это был **вирус нового типа**. Поскольку это не была отдельная программа, она не была классифицирована как червь. Он нацелился на системы на базе Microsoft Word и Outlook и создал значительный сетевой трафик. Он распространялся по электронной почте в присоединенном файле, и после того как пользователь открывал этот файл, вирус рассылал себя по первым 50 адресам в адресной книги почтовой программы Microsoft Outlook. Он не наносил никакого ущерба самому компьютеру, но порождал лавину новых писем, и из-за перегрузки выходили из строя корпоративные серверы.

Вирус заражал компьютеры через электронное письмо, в письме с заголовком «Важное сообщение от», за которым следует текущее имя пользователя. После щелчка по сообщению тело будет читать: «Вот тот документ, который вы просили. Больше никому не показывать;)». Прикрепленный был документ под названием Слово list.doc, содержащий список порнографических сайтов и сопровождающих логинов для каждого. Затем он будет массово рассылать себя первым 50 людям в списке контактов пользователя, а затем отключать несколько защитных функций в Microsoft Word и Microsoft Outlook. Через неделю после начала эпидемии полиция Нью-Джерси и агенты ФБР вычислили, что вирус был выпущен в Internet с адреса онлайновой службы AOL, принадлежащего некоему 30-летнему Дэвиду Смиту. Он признался в том, что именно он создал вирус Melissa. Он также согласился сотрудничать со следствием, поэтому ему было предъявлено обвинение в нанесении ущерба в размере 80 млн дол. по статье, которая предусматривала тюремное заключение сроком от 46 до 57 месяцев. Потом Смит был выпущен под залог в 100 тысяч дол. и дело начали спускать на тормозах. Слушания неоднократно переносились, и обвинители, так шумно начавшие это дело, теперь хранят молчание. Молчат также сам Джим Смит и его адвокат.

Вирус ILoveYou

В начале 21 века появился надежный высокоскоростной интернет-доступ, и это изменило методы распространения вредоносных программ. Теперь они не были ограничены дискетами и корпоративными сетями и могли очень быстро распространяться через электронную почту, популярные веб-сайты и даже напрямую через интернет. Начало формироваться вредоносное ПО в современном виде. Ландшафт угроз оказался заселенным вирусами, червями и троянцами. Возник собирательный термин «вредоносное ПО». Одна из самых серьезных эпидемий новой эры была вызвана червем ILoveYou, который появился 4 мая 2000 г.

Как указывает Securelist, ILoveYou следовал модели ранее существовавших вирусов, распространявшихся по почте. При этом, в отличие от макровирусов, широко распространенных с 1995 года, ILoveYou распространялся не в виде зараженного документа Word, а в виде VBS-файла (такое расширение имеют скрипты, написанные в Visual Basic). Метод оказался простым и действенным – пользователи еще не привыкли остерегаться незапрошенных электронных писем. В качестве темы письма была строчка «I Love You», а в приложении к каждому письму был файл «LOVE-LETTER-FOR-YOU-TXT.vbs». По задумке создателя Онеля де Гузмана, червь стирал существующие файлы и поверх них записывал собственные копии, благодаря которым червь рассылался по всем адресам из списка контактов пользователя. Поскольку письма, как правило, приходили со знакомых адресов, получатели обычно открывали их – и заражали червем свой компьютер. Таким образом, ILoveYou на практике подтвердил эффективность методов социальной инженерии.

Червь CodeRed

Червь CodeRed был так называемым бестелесным червем – он существовал только в памяти и не предпринимал попыток заразить файлы в системе. Используя брешь в системе безопасности Microsoft Internet Information Server, червь всего за несколько часов распространился по всему миру и вызвал хаос, внедряясь в протоколы обмена информацией между компьютерами.

Как пишет сайт Scientific American, зараженные компьютеры в итоге были использованы для проведения DDoS-атаки на веб-сайт Белого дома – Whitehouse.gov.

Heartbleed

Угроза Heartbleed появилась в 2014 г. и сразу поставила под угрозу множество интернет-серверов. В отличие от вирусов и червей, Heartbleed – это уязвимость в OpenSSL – криптографической библиотеке универсального применения, широко использующейся по всему миру. OpenSSL периодически рассылает соединенным

устройствам специальные сигналы, подтверждающие актуальность соединения. Пользователи могут отослать некоторый объем данных и в ответ запросить такое же количество данных – например, отослать один байт и получить в ответ тоже один байт. Максимальное количество данных, отправляемых за один раз – 64 килобайта. Как объясняет специалист по безопасности Брюс Шнайер, пользователь может объявить, что отсылает 64 килобайта, а по факту отправить только один байт – в этом случае сервер в ответ пришлет 64 килобайта данных, хранящихся в его оперативной памяти, в которых может оказаться все что угодно – от имен пользователей до паролей и криптостойких ключей.

WannaCry (англ. "хочу плакать")

WannaCry — смешанная угроза, сочетающая в себе аспекты червя и программы-вымогателя.

12 мая 2017 года значительное число компьютеров с операционной системой Windows подверглось атаке вируса-вымогателя WannaCry (англ. "хочу плакать"). Вирус шифрует файлы пользователя, чтобы их нельзя было использовать; за расшифровку данных злоумышленники требовали заплатить $600 в криптовалюте биткойн. Всего было заражено до 300 тыс. компьютеров в по меньшей мере 150 странах мира. Предполагаемый ущерб превысил $1 млрд. От атаки, в частности, пострадали Национальная система здравоохранения (NHS) Великобритании, испанская телекоммуникационная компания Telefonica, электронная система суда бразильского штата Сан-Паулу и др. Глобальная хакерская атака также затронула компьютеры российских силовых ведомств и телекоммуникационных компаний. Атакам подверглись системы МЧС, МВД, РЖД, Сбербанка, мобильных операторов "Мегафон" и "Вымпелком", Telefónica, FedEx и Deutsche Bahn. Nissan и Renault остановили производство. Пострадали больницы. По данным американских экспертов, вымогавшим средства злоумышленникам поступило всего 302 платежа в общем размере около $116,5 тыс. По оценкам Сбербанка, более 70% "успешно" атакованных компьютеров принадлежали российским организациям и физическим лицам. После атаки Microsoft выпустила обновления пакетов безопасности для уже не поддерживавшихся операционных систем Windows XP, Windows Server 2003 и Windows 8.