План

1. Історія виникнення комп'ютерних вірусів.
2. Визначення комп'ютерного вірусу.
3. Творці комп'ютерних вірусів.

Історія починається в 1983 році, коли американський учений Фред Коэн (Fred Cohen) у своїй дисертаційній роботі, присвяченої дослідженню комп'ютерних програм, що самовідтворюються, уперше ввів термін комп'ютерний вірус. Відома навіть точна дата - 3 листопада 1983 року, коли на щотижневому семінарі по комп'ютерній безпеці в Університеті Південної Каліфорнії (США) був запропонований проект по створенню програми, що самопоширюється, що відразу охрестили вірусом. Для її налагодження треба було 8 годин комп'ютерного часу на машині VAX 11/750 під керуванням операційної системи Unix і рівно через тиждень, 10 листопада відбулася перша демонстрація. Фредом Коэном за результатами цих досліджень була опублікована робота "Computer Viruses: theory and experiments" с докладним описом проблеми.

Теоретичної ж основи програм, що самопоширюються, були закладені в 40-х роках минулого сторіччя в працях по вивченню математичних автоматів, що самовідтворюються, американського вченого Джона фон Неймана (John von Neumann) , що також відомий як автор базових принципів роботи сучасного комп'ютера. В 1951 році фон Нейманом був розроблений метод, що демонстрував можливість створення таких автоматів, а в 1959 журнал "Scientific American" опублікував статтю Л. С. Пенроуза (L. S. Penrose) "Self-Reproducing Machines", присвячену механічним структурам, що самовідтворюються. На відміну від раніше відомих робіт, тут була описана найпростіша двовимірна модель подібних структур, здатних до активації, розмноженню, мутаціям, захватові. Пізніше, слідами цієї статті інший учений Ф. Ж. Шталь (F. G. Stahl) реалізував модель на практиці за допомогою машинного коду на IBM 650.

Перші програми, що самопоширюються, не були шкідливими в змісті, що нині розуміє. Це були скоріше програми-жарти або наслідки помилок у програмному коді, написаному в дослідницьких цілях. Складно представити, що вони були створені з якоюсь конкретною шкідливою метою.

Перші віруси

Pervading Animal (кінець 60-х - початок 70-х) — так називалася перший відомий вірус-гра для машини Univac 1108. За допомогою навідних запитань програма намагалася визначити ім'я тварини, задуманого граючої. Завдяки наявності функції додавання нових питань, коли модифікована гра записувалася поверх старої версії плюс копіювалася в інші директорії, через якийсь час диск ставав переповненим.

Перший мережний вірус Creeper з'явився на початку 70-х у військовій комп'ютерній мережі Arpanet, прототипі Інтернет. Програма могла самостійно вийти в мережу через модем і зберегти свою копію на вилученій машині. На заражених системах вірус виявляв себе повідомленням: "I' THE CREEPER : CATCH ME IF YOU CAN". Для видалення настирливого, але в цілому необразливого вірусу невідомим була створена програма Reaper. По суті це був вірус, що виконував деякі функції, властиві антивірусу: він поширювався по обчислювальній мережі й у випадку виявлення тіла вірусу Creeper знищував його.

Перші вірусні епідемії

Можливості перших вірусів були сильно обмежені малою функціональністю існуючих на той момент обчислювальних машин. Тільки наприкінці сімдесятих, слідом за випуском нового покоління персональних комп'ютерів Apple (Apple II) і згодом IBM Personal Computer (1981 рік), стали можливі вірусні епідемії. Поява BBS (Bulletin Board System) забезпечило швидкий обмін інформацією між навіть самими віддаленими крапками планети.

Elk Cloner (1981 рік) споконвічно використав для поширення піратські копії комп'ютерних ігор. Оскільки жорстких дисків тоді ще не було, він записувався в завантажувальні сектори дискет і проявляв себе перекиданням зображення на екрані й виводом тексту:

ELK CLONER:

THE PROGRAM WITH A PERSONALITY

IT WILL GET ON ALL YOUR DISKS

IT WILL INFILTRATE YOUR CHIPS

YES, IT' CLONER

IT WILL STICK TO YOU LIKE GLUE

IT WILL MODIFY RAM, TOO

SEND IN THE CLONER!

Перші антивірусні утиліти (1984 рік) були написані Анди Хопкинсом (Andy Hopkins). Програми CHK4BOMB й BOMBSQAD дозволяли робити аналіз завантажувального модуля за допомогою контекстного пошуку й перехоплювати операції запису й форматування, виконувані через BIOS. На той час вони були дуже ефективні й швидко завоювали популярність.

Brain (1986 рік) — перший вірус для IBM-сумісних комп'ютерів, що викликав глобальну епідемію. Він був написаний двома братами-програмістами Баситом Фарук й Амжадом Алви (Basit Farooq Alvi й Amjad Alvi) з Пакистану з метою визначення рівня піратства в себе в країні: вірус заражав завантажувальні сектори, міняв мітку диска на "(c) Brain" і залишав повідомлення з іменами, адресою й телефоном авторів. Відмітною рисою його була функція підміни в момент звертання до нього зараженого сектора незараженим оригіналом. Це надає право назвати Brain першим відомим стелс-вирусом. Протягом декількох місяців програма вийшла за межі Пакистану й до лету 1987 року епідемія досягла глобальних масштабів. Нічого деструктивний вірус не робив.

У цьому ж році відбулася ще одна знаменна подія. Німецький програміст Ральф Бюргер (Ralf Burger) відкрив можливість створення програмою своїх копій шляхом додавання свого коду до виконуваних DOS-файлів формату COM. Досвідчений зразок програми, що одержала назва Virdem, був продемонстрований на форумі комп'ютерного андеграунда - Chaos Computer Club (грудень 1986 року, Гамбург, ФРН). По результатами досліджень Бюргер випустив книгу "Computer Viruses. The Disease of High Technologies", що послужила поштовхом до написання тисяч комп'ютерних вірусів, частково або повністю використали описані автором ідеї.

Lehigh (1987 рік) — перший по-справжньому шкідливий вірус, що викликав епідемію в Лехайском університеті (США), де в той час працював Фред Коэн. Він заражав тільки системні файли COMMAND.COM і був запрограмований на видалення всієї інформації на поточному диску. Протягом декількох днів був знищений уміст сотень дискет з бібліотеки університету й особистих дискет студентів. Усього за час епідемії було заражено біля чотирьох тисяч комп'ютерів. Однак за межі університету Lehigh не вийшов.

Сімейство резидентних файлових вірусів Suriv (1987 рік) — утвір невідомого програміста з Ізраїлю. Найвідоміша модифікація, Jerusalem, стала причиною глобальної вірусної епідемії, першою дійсною пандемією, викликаної MS-DOS-вірусом.

Действие вірусів Suriv зводилося до завантаження коду на згадку комп'ютера, перехоплюванні файлових операцій і зараженні запуска користувачем COM- і/або EXE-файлів. Ця обставина забезпечувала практично миттєве поширення вірусу по мобільних носіях. Jerusalem відрізнявся від своїх попередників додатковою деструктивною функцією - знищенням всіх програм, що запускають, у п'ятницю, 13. Такою чорною датою стало 13 травня 1988 року, коли відразу перестали працювати комп'ютери багатьох комерційних фірм, державних організацій і навчальних закладів, у першу чергу Америки, Європи й Близького Сходу.

Примітно, що в тім же 1988 року відомий програміст Питер Нортон (Peter Norton) висловився різко проти існування вірусів. Він офіційно оголосив їхнім неіснуючим міфом і зрівняв з казками про крокодилів, що живуть у каналізації Нью-Йорка. Це показує як низка була культура антивірусної безпеки в той час.

Mike RoChenle — псевдонім автора першої відомої вірусної містифікації. У жовтні 1988 року він розіслав на станції BBS велика кількість повідомлень про вірус, що передається від модему до модему зі швидкістю 2400 біт/с. Як панацея пропонувалося перейти на використання модемів зі швидкістю 1200 біт/с. Як це ні смішно, багато користувачів дійсно пішли цій раді.

Хробак Морриса (листопад 1988) — з ним зв'язана перша епідемія, викликана мережним хробаком. 60000-байтная програма, написана 23-літнім студентом Корнельского університету (США) Робертом Моррисом, використала помилки в системі безпеки операційної системи Unix для платформ VAX й Sun Microsystems. З метою непомітного проникнення в обчислювальні системи, пов'язані з мережею Arpanet, використався підбор паролів (зі списку, що містить 481 варіант). Це дозволяло маскуватися під завдання легальних користувачів системи. Однак через помилки в коді нешкідлива за задумом програма необмежено розсилала свої копії по інших комп'ютерах мережі, запускала їх на виконання й у такий спосіб забирала під себе всі мережні ресурси.

Хробак Морриса заразив за різними оцінками від 6000 до 9000 комп'ютерів у США (включаючи Дослідницький центр NASA) і практично паралізував їхню роботу на строк до п'яти доби. Загальні збитки були оцінені в мінімум 8 мільйонів годин втрати доступу й понад мільйон годин прямих втрат на відновлення працездатності систем. Загальна вартість цих витрат оцінюється в 96 мільйонів доларів. Збиток був би набагато більше, якби хробак споконвічно створювався з руйнівними цілями.

4 травня 1990 року вперше в історії відбувся суд над автором комп'ютерного вірусу, що присудив Роберта Морриса до 3 рокам умовно, 400 годинникам суспільних робіт і штрафу в 10 тисяч доларів США.

Епідемія хробака Морриса стала причиною створення організації CERT (Computer Emergency Response Team), у функції якої входить надання сприяння користувачам у запобіганні й розслідуванні комп'ютерних інцидентів, що мають відношення до інформаційних ресурсів. На сайті цієї організації оперативно публікуються самі останні відомості про нові шкідливі програми, виявлених уязвимостях у ПО, методах захисту корпоративних мереж, аналітичні статті, а також результати різних досліджень в області комп'ютерної безпеки.

Dr. Solomon's Anti-Virus Toolkit (1988) — перша широко відома антивірусна програма. Створена англійським програмістом Аланом Соломоном (Alan Solomon), вона завоювала величезну популярність і проіснувала до 1998 року, коли компанія Dr. Solomon була поглинена іншим виробником антивірусів - американської Network Associates (NAI).

Крім офіційного перейменування Arpanet в Інтернет, що випливає рік ознаменувався виходом у світло першого номера Virus Bulletin (липень 1989) — самого популярного на сьогоднішній день видання, що містить останні новини в сфері вірусних й антивірусних технологій: докладну інформацію про нові шкідливі програми, методи захисту від вірусів й усунення наслідків зараження. Засновниками журналу виступили керівники англійської антивірусної компанії Sophos Ян Храске (Jan Hruska), Питер Лэммер (Peter Lammer) і Эд Уайлдинг (Ed Wilding). Згодом редакція Virus Bulletin (1991) початку проводити щорічні конференції для антивірусних експертів, де корпоративні замовники мають можливість прямо спілкуватися із провідними спеціалістами в цій області. У січні 1998 року була заснована нагорода VB 100%, присуджувана антивірусним програмам за результатами проведеного редакцією Virus Bulletin тестування. Кількість нагород VB 100%, отриманих у результаті тестування сьогодні найчастіше є одним з основних критеріїв у виборі засобів антивірусного захисту.

Як відповідь через пару місяців Dr. Solomon's запустила свій власний видавничий проект - Virus Fax International, згодом перейменований в Secure Computing. Сьогодні цей журнал є одним з найбільш популярних видань в області захисту інформації, спеціалізуючись на аналізі не тільки антивірусних програм, але також усього спектра програмних й апаратних засобів, застосовуваних для забезпечення комп'ютерної безпеки.

Datacrime (1989) — вірус, що незважаючи на порівняно невелике поширення, викликав повальну істерію у світових засобах масової інформації. Він відрізнявся тим, що з 13 жовтня по 31 грудня ініціював низькорівневе форматування нульового циліндра жорсткого диска, що приводило до знищення таблиці розміщення файлів (FAT) і безповоротній втраті даних.

У відповідь корпорація IBM випустила (4 жовтня 1989 року) комерційний антивірус Virscan для MS-DOS, що дозволяє шукати характерні для ряду відомих вірусів рядка у файловій системі. Вартість програми склала всього 35 доларів США.

Aids Information Diskette (грудень 1989) — перша епідемія троянської програми. Її автор розіслав близько 20000 дискет з вірусом по адресах у Європі, Африці й Австралії, викраденим з баз дані Організації всесвітньої охорони здоров'я й журналу PC Business World. Після запуску шкідлива програма автоматично впроваджувалася в систему, створювала свої власні сховані файли й директорії й модифікувала системні файли. Через 90 завантажень операційної системи всі файли на диску ставали недоступними, крім одного - з повідомленням, що пропонувало надіслати $189 на зазначену адресу. Автор троянца, Джозеф Попп (Joseph Popp), визнаний пізніше несамовитим, був затриманий у момент пред’яви чека й засуджений за вимагання. Фактично, Aids Information Diskette - це перший й єдиний вірус, який для масового розсилання використовував дійсну пошту.

Cascade (1989) — резидентний зашифрований вірус, що викликає характерний відеоефект - опадання букв на екрані. Примітний тим, що послужив поштовхом для професійної переорієнтації Євгенія Касперского на створення програм-антивірусів, будучи виявленим на його робочому комп'ютері. Уже через місяць другий інцидент (вірус Vacsina) був закритий за допомогою першої версії антивірусу — V, що декількома роками пізніше був перейменований в AVP — AntiViral Toolkit Pro.

Eddie (також відомий як Dark Avenger, 1989 рік) — перший вірус, що протидіє антивірусному програмному забезпеченню: він заражає нові файли, поки антивірус перевіряє жорсткий диск комп'ютера. Це досягалося застосуванням особливої технології, що дозволяє заражати не тільки COM/EXE- програми в момент їхнього запуску, але й будь-які файли при спробі прочитання.

Автором ідеї, завдяки якій значно пізніше виникла технологія створення програмних вірусів, прийнято вважати американського програміста Боба Томаса. В 1971 році обчислювальна лабораторія компанії Bolt, Beranek and Newman, у якій працював Томас, одержала замовлення на розробку розподіленого програмного комплексу для авіадиспетчерських служб, керуючих рухом пасажирських літаків. Відповідно до вимог замовників, що входять у комплекс програми повинні були автоматично передавати керування курсом літаків з одного комп'ютера на іншій по обчислювальній мережі, відображаючи на екранах усіх підключених до цієї мережі комп'ютерів постійно змінювану інформацію, про поточне положення авіалайнерів у повітрі. Експериментуючи із системами передачі даних між різними обчислювальними машинами, Томас написав програму, що назвав «Повзуном». «Повзун» самостійно копіював себе з одного комп'ютера на інший, переміщаючись у такий спосіб по мережі, і виводив на екран кожного термінала наступне повідомлення: «Я - Повзун! Якщо зможеш, піймай мене!». Ця невелика програма не розмножувалася, а просто «плазувала» з одного мережного вузла на інший, розважаючи користувачів і системних адміністраторів. Коли інші програмісти довідалися про винахід Томаса, вони прийнялися створювати аналогічні програми, що демонстрували на екранах колег по лабораторії різні забавні фрази. Коли комусь із фахівців Bolt, Beranek and Newman набридло боротися з нескінченно відволікаючими його від роботи «Повзунами», він написав іншу програму, що в точності так само самостійно переміщалася по мережі, але із зовсім іншою метою: вона виловлювала й безжалісно знищувала всіх «Повзунів», які попадалися їй на шляху. Зачеплені за живе розроблювачі «Повзунів» не відставали: удосконаливши вихідний код, вони навчили свої програми ховатися від «убивці» у надрах операційної системи, маскуючись під її компоненти в необхідні для нормальної роботи комп'ютера бібліотеки. Кривава боротьба між «Повзунами» і «Кілерами» тривала кілька місяців, після чого це захоплення втратило свою новизну й було закинуто, так і не одержавши серйозного розвитку.

Однак ідея Боба Томаса не була забута. В 1975 році американський письменник-фантаст Джон Браннер випустив фантастичний роман «Осідлавший Вибухову Хвилю», в основу якого лягла трохи видозмінена історія з «Повзунами». Книга розповідала про комп'ютеризоване суспільство, яким керувало за допомогою глобальної електронної мережі уряд диктаторів і тиранів. Програміст, що вирішив урятувати світ від диктатури, написав програму, що автор роману назвав «глистом»; ця програма копіювала себе з одного комп'ютера на інший, руйнуючи інформацію, що зберігалася в них. Щоб зупинити «глиста», уряд змушений було відключити мережу, позбавившись у такий спосіб влади. Роман швидко став бестселером, зробившись воістину культовою книгою в тільки тоді зароджуваному середовищі комп'ютерних хакерів. Саме завдяки цьому роману в 1980 році двоє співробітників компанії Xerox, що у ті часи випускала дуже популярні персональні комп'ютери, що мають можливість об'єднання в локальні мережі, вирішили створити програму, що за аналогією зі згадуваним у романі Браннера дітищем програміста-бунтаря назвали «Хробаком». Властиво, «Хробак» Іона Хеппа й Джона Шоку повинен був нести позитивну місію: за задумом розроблювачів, переміщаючись між підключеними до мережі комп'ютерами, «Хробак» був покликаний перевіряти операційну систему на наявність прихованих дефектів і по можливості усувати їх. Хепп і Шок задумали ще два варіанти «Хробака»: один з них призначався для поширення оголошень, які адміністратор міг направляти всім користувачам обчислювальної мережі, другий дозволив би гнучко перерозподіляти ресурси між різними об'єднаними в мережу комп'ютерами. Однак на практиці все вийшло зовсім не так, як задумали розроблювачі. Запустивши ввечері експериментальну версію «Хробака», Хепп і Шок відправилися додому. Коли ранком програмісти повернулися на роботу, вони побачили, що всі комп'ютери, встановлені в багатоповерховому будинку дослідницького центра Xerox, розташованого в містечку Паоло-Альто, благополучно зависли. У вихідному коді «Хробака» була допущена незначна помилка, завдяки якій програма почала безконтрольно поширюватися між різними вузлами мережі й блокувати їхню роботу. Перезавантаження машин не допомагало: частина ввімкнених у мережу комп'ютерів були встановлені в закритих кімнатах, до яких Хепп і Шок не мали доступу, і як тільки на перезавантаженій машині запускалася операційна система, «Хробак» відразу копіював себе в її пам'ять з іншого комп'ютера, після чого система миттєво виходила з ладу. Відключивши одну з машин від локальної мережі, програмісти змушені були негайно створити іншу програму, що знищила б «Хробака». На повну ліквідацію наслідків їхньої спільної творчості пішло кілька днів.

Провідний програміст компанії Bell Labs Боб Морріссон по визнаннях колег був кращим фахівцем у своїй області, до нього часто зверталися за всілякими консультаціями, зокрема - у сфері безпеки комп'ютерних систем. Морріссон був небагатослівний, але нерідко доводив опонентам свою правоту на практиці. Один раз співробітники відділу, у якому трудився Боб, кілька місяців підряд працювали над удосконалюванням системи безпеки експлуатованої ним комп'ютерної мережі, винаходячи всі нові й нові програмні модулі. Коли робота була закінчена, вони похвасталися Бобові, що тепер ця мережа захищена від можливих збоїв на всі сто відсотків. Знизавши плечима, Морріссон мовчачи викинув палаючий недокурок у стояче поблизу відро для сміття з паперами, вміст відра миттєво зайнявся, спрацювала протипожежна сигналізація й з вмонтованих у стелю лабораторії труб вода за дві секунди привела всю обчислювальну систему в неробочий стан. Тоді, наприкінці вісімдесятих років, серед програмістів була дуже популярна гра за назвою Core Wars. Гра мала вбудовану мову програмування, від гравця було потрібно написати на цій мові спеціальну «бойову програму». Призначення такої програми було простим: знищити аналогічні програми суперників, відшукуючи слабкі місця в їхньому коді. Перемагав той програміст, чий витвір продовжував працювати, коли всі інші програми були ушкоджені або зруйновані. Віртуальні баталії «бойових програм» на кілька місяців стали «коником» програмістів з Bell Labs; це тривало доти, поки за справу не узявся Боб Морріссон. Його «бойова програма» виявилася непереможною: код складався всього лише з 30 рядків, однак цей малюсінький файл не просто атакував суперників: він аналізував методи їхнього захисту й, відповідним чином видозмінюючись, знищував файл супротивника «зсередини», вибираючи стратегію атаки виходячи з його логічної структури. Після цього гра Core Wars втратила всякий зміст: винайдений Морріссоном «поліморф» не залишав конкурентам жодного шансу. Незабаром Боб Морріссон залишив роботу в Bell і одержав посаду експерта по комп'ютерному захисту в Національному Агентстві Безпеки США - єдиної в Америці організації, що займалася розслідуванням комп'ютерних злочинів.

Старший син Боба Морріссона Роберт ріс тихим і скромним хлопчиком, його єдиною пристрастю були комп'ютери. Уже в чотирнадцятилітньому віці він переписав популярну в підлітків комп'ютерну гру The Four Corners, додавши в неї безліч нових функціональних можливостей, в 16 років він став дійсним експертом по системі безпеки UNIX, виявивши в «класичному» берклієвському коді цієї платформи безліч помилок, які одразу виправив. Однак він і сам не гидував користуватися виявленими «дірами» у захисті, час від часу підключаючись до віддалених електронних мереж у пошуках інформації, що його цікавила. Це захоплення привело до того, що незабаром у комп'ютерному журналі Smitsonian з'явився матеріал, у якому Роберта називали одним з найбільш відомих молодих хакерів в Америці. Саме Роберт Морріссон є автором і розроблювачем однієї з найбільш відомих реалізацій протоколу передачі даних UUCP - Unix-To-Unix CoPy. Навчаючись на четвертому курсі Гарвардського університету, Роберт уже читав лекції в Національному Агентстві Безпеки США й дослідницьких лабораторіях військово-морського флоту по безпеці операційної системи UNIX.

Отримані Робертом у ході його самостійних розробок і вивчення вже існуючого досвіду інших програмістів знання вимагали практичного застосування. Як експеримент Роберт вирішив написати програму, що, використовуючи виявлені їм недоробки в створеному для UNIX протоколі FTP і програмі sendmail могла б самостійно поширюватися між об'єднаними в мережу комп'ютерами, подібно «Хробакові» Хеппа й Шоку, але при цьому вміла б ефективно «ховатися» в операційній системі й самостійно розмножуватися. Іншими словами, «Хробак» Морріссона повинен був поєднувати в собі всі достоїнства попередніх спроб створення аналогічних програм. Оскільки ця розробка була всього лише науковим експериментом, тестом на безпеку об'єднаних у мережі комп'ютерних систем, Роберт заклав у код «Хробака» алгоритми, що стримують його поширення, ніяких модулів, що руйнують файлову систему атакованих комп'ютерів, також задумано не було. 2 листопада 1988 року в 18.30 Роберт Морріссон підключився до комп'ютерів лабораторії штучного інтелекту MIT і запустив свою програму на виконання. Коли через півгодини він знову спробував підключитися до мережі, щоб перевірити хід експерименту, віддалений комп'ютер не відповів: завдяки помилки, яка закралася у вихідний код «Хробак» почав безконтрольно розмножуватися, блокуючи нормальну роботу обчислювальних систем, і незабаром вирвався з локальної мережі MIT на простори Інтернету.

Програма Морріссона - молодшого стала дійсним нещастям для США, протягом декількох днів функціонування Інтернету було паралізовано практично повністю. Саме тоді за здатність до швидкого поширення й зараження всі нових і нових вузлів мережі журналісти вперше охрестили витвір Роберта «вірусом». По різних підрахунках епідемія вразила порядку 6000 комп'ютерів - близько 10% всіх обчислювальних машин, що працювали тоді в Інтернеті, нанесений вірусом збиток оцінювався від скромної цифри в 150 000 до значної суми в 75 мільйонів доларів США. Незабаром до справи підключилося ФБР, однак розслідування тривало недовго: Морріссон сам зізнався у вчиненому. Преса роздула скандал до неймовірного масштабу, особливу пікантність ситуації надавав той факт, що батько Роберта Морріссона - Боб Морріссон був одним із провідних експертів відділу Агентства Національної Безпеки, що займались розслідуванням комп'ютерних злочинів.

Судова справа Роберта Морріссона була однією з перших справ в обвинуваченні в здійсненні комп'ютерного злочину в США, до цього по даній статті під суд потрапив лише відомий в усьому світі хакер Кевін Митник. Морріссона визнали винним і присудили до виплати штрафу в розмірі 10 000 доларів і 400 годин виправних робіт. Однак слава Роберта Морріссона набула широкої популярності завдяки створеному ним вірусу, дотепер не дає спокою сотням і тисячам хакерів на різних континентах. Останньою спробою переплюнути творця першого в історії людства вірусу «масової поразки» була відома програма «Меліса», що знищила в цілому більше 30 000 комп'ютерів. З тих пір сотням і тисячам амбіційних молодих людей, що розбираються в програмуванні, рано або пізно спадає на думку спробувати свої сили в створенні програми, що, поширюючись по мережі, могла б дестабілізувати роботу різних обчислювальних систем. Саме їхнє прагнення до дешевої слави приносить тепер безліч безсонних ночей, проведених користувачами за відновленням зруйнованих систем, і значний прибуток компаніям, що займаються розробкою антивірусних програм.

Віруси - даність сьогоднішнього часу, прибутковий бізнес як для вірусотворців, так і для антивірусних компаній. Але так було не завжди. Комп'ютерні віруси, здається, давно вже ніхто не сприймає як щось надзвичайне і смертельно небезпечне (за винятком, можливо, Stuxnet, але про нього розмова окрема). Це вже просто даність.

Так було, ясна річ, не завжди: траплялися і масовані паніки, і гучні пророцтва з боку антивірусних компаній, що пророкують, що віруси скоро влаштують кінець якщо не світу, то інтернету точно, ну і численні міські легенди про комп'ютерні віруси, здатні викликати напади епілепсії та інсульт у людей, які сидять за комп'ютерами. Як і будь-які інші конспірологічні теорії та міські легенди, спростовувати і розвінчувати їх безглуздо і неможливо.

Найперший вірус був створений як експериментальна програма, що демонструє здатність комп'ютерного коду самовідтворюватися без участі людини. Зараз комп'ютерні віруси - засіб заробітку як для тих, хто їх пише, так і для тих, хто з ними бореться: і з одного, і з іншого боку є відмінний бізнес, щоправда, з боку вірусотворців - суто кримінальний, але зате який дохідний!

Найбільш ранній з відомих вірусів писався в порядку експерименту - досліджувалася можливість автоматичної самореплікації комп'ютерного коду. Боб Томас, співробітник ІТ-компанії BBN Technologies, написав програму, яка отримала назву Creeper ("повзун", читається як "кріпер"), - цілком натурального "хробака", який "заражав" комп'ютери DEC PDP-10 на базі ОС TENEX, використовуючи як засіб поширення ARPANET.

На екрані зараженої системи з'являвся напис "Я - повзун, злови мене, якщо зможеш". Пізніше, у відповідності з золотим принципом "клин клином вибивають", була написана програма Reaper ("жнець", читається як "Ріпер"), яка відшукувала і винищувала копії "кріпера".

Залишається додати, що BBN Technologies займалася розробкою методу пакетної комутації (packet switching) для APRANET - і, у підсумку, того, що стане інтернетом. Тобто, виходить, що "черв'яки" і інтернет народилися практично одночасно. Хоча варто уточнити: терміни "вірус" і, тим більше, "хробак" щодо комп'ютерних програм тоді ще не застосовувалися.

Саме поняття "комп'ютерний вірус" з'явилося в 1983-1984 роках завдяки професору інформатики в Університеті Південної Каліфорнії Леонарду Едлману і його студенту Фредріку Коену. Власне термін придумав Едлман, а Коен - створив демонстративну паразитичну програму, здатну "заражати" інші програми, впроваджуючи в них свою копію, іноді видозмінену. Майже так само, як діє біологічний вірус.

Між тим, двома роками раніше - в 1981 році - 15-річний гик на ім'я Річард Скрента, любитель образливих розіграшів, написав перший "завантажувальний" вірус (boot sector virus) для операційної системи Apple II, живенько так розповсюджувався через флоппі-дискети. Це був перший в історії випадок широкого, неконтрольованого розповсюдження вірусу, який, на щастя, не заподіював цілеспрямованого збитку.

Про те, що шкідливе програмне забезпечення взагалі може існувати, більшість користувачів просто не знала.

Досить скоро, втім, довелося дізнатися: у 1986 році брати Басіт і Амджад Фарук Альва написали програму (c)Brain, вірус, який заміняв завантажувальний сектор флоппі-диска своєю копією, а сам цей сектор викрадав в інше місце і помічав як непридатний (bad sector). Вірус створював на дискеті до п'яти кілобайт зіпсованих секторів, сповільнював роботу дисководів і робив близько 7 кілобайт оперативної пам'яті недоступною для DOS.

Як потім пояснювали брати Альва, вони писали свій вірус як засіб захисту своєї основної програмної розробки від піратів - передбачалося, що (c)Brain дозволить відстежувати піратські копії цієї програми. Брати навіть чесно вказали в програмному коді свої координати, зокрема, телефон, за яким можна телефонувати в разі зараження - і в підсумку отримали колосальну кількість дзвінків від обурених жертв свого вірусу. Нічим хорошим це для них не закінчилося.

1987 виявився якимось особливо врожайним на шкідливий софт. Бельгійські офіси IBM піддалися атаці з боку першого в історії вірусу Cascade, після чого в IBM почали всерйоз розробляти антивірусне ПЗ. З'явився перший вірус для Commodore Amiga, і не те щоб зовсім нешкідливий.

Втім, він був непорівнянний з Jerusalem, вірусом для DOS, виявленим у жовтні 1987 року. Ця безбожна тварюка сідала резидентом в оперативну пам'ять і заражала всі виконувані файли. Обходила тільки command.com (у своїй оригінальній версії). файли EXE Jerusalem заражав по кілька разів, до тих пір, поки вони не переставали влазити в пам'ять. Повільні машини (PC-XT) вірус міг уповільнювати в п'ять разів, на PC-AT наслідки зараження були менш помітні.

Головна ж проблема полягала в тому, що, починаючи з 1988 року, кожну п'ятницю тринадцятого, цей вірус повинен був знищувати всі програми, що запускалися з моменту зараження комп'ютера. Згодом у нього було кілька десятків різновидів, що відрізнялися ступенем деструктивності і датами знищення програм, що запускалися.

У грудні того ж 1987 року з'явився Christmas Tree EXEC, вірус, що репродукується, який паралізував декілька міжнародних комп'ютерних мереж.

У листопаді 1988 року фахівці виявили вірус, який "офіційно" називався "хробаком" - Morris worm.

Історія з ним була дуже драматичною. Автором "хробака" був якийсь Роберт Таппан Морріс, студент Корнельського університету, який створив програму, за допомогою якої хотів - за його словами - просто з'ясувати, скільки в світі комп'ютерів підключено до інтернету. Незрозуміло, правда, чому тоді Морріс розіслав своє дітище з мереж Массачусетського технологічного інституту (MIT), а не з Корнельського університету...

"Черв'як" повинен був заражати машини під управлінням BSD, використовуючи найрізноманітніші вразливості - від програмних проломів до слабких паролів. Крім того, йому належало самовідтворюватися і перед зараженням опитувати кожну машину на наявність на ній своєї копії. Правда, Моріс подумав, що системні адміністратори можуть спробувати перешкодити його вірусу, налаштувавши комп'ютери так, щоб ті давали неправдиві позитивні відповіді. Тому автор хробака настроїв його так, щоб той у 14% випадків самовідтворювався, незалежно від відповіді опитуваних машин.

Наслідком цього стала страшна епідемія і значний фінансовий збиток для організацій, чиї мережі виявилися наглухо забиті хробаком Морріса. Сам Морріс, дізнавшись про те, що накоїв, заявив, що спочатку повинен був випробувати свого хробака на симуляторі. Програміст виявився першою в історії людиною, засудженою за законом 1986 року про зловживання і шахрайство при використанні комп'ютерних технологій (Computer Fraud and Abuse Act), але покараний був досить м'яко: три роки умовного терміну і штраф в 10 тисяч доларів. Згодом він став професором в тому ж самому MIT.

Наступними передбачуваним чемпіоном за шкідливістю мав стати вірус Michelangelo (1992 рік), але не став. Виявилося, що це ЗМІ розвели істерику, і намалювали дідька так страшно, що 6 березня всі чекали "цифрового апокаліпсису". Не сталося.

У 1995 році на світ з'явився перший макровірус, що використав уразливості в Microsoft Word - Concept. Згодом макровіруси стали надзвичайно популярні у вірусотворців. Чим більше поширювалися операційні системи та офісні пакети Microsoft, тим більше ставало макровірусів.

Стрімке поширення Microsoft Windows - з усіма численними проломи в безпеці у ранніх версій (з Windows 95 починаючи) - поклало початок зовсім новій епосі.

У 1998 році на світ з'явився надзвичайно небезпечний вірус китайського походження, CIH. Як потім стало відомо, компанія Yamaha почала поширювати оновлену прошивку для своїх CD-приводів CD-R400, в якій сидів цей вірус, потім з дзеркала сайту Activision пішла поширюватися заражена вірусом демоверсія гри SiN, а в березні 1999 року IBM поставила клієнтам кілька тисяч комп'ютерів Aptiva, заражених вірусом CIH, що став згодом відомим ще й як Chernobyl. І не випадково: першого масованого удару вірус завдав як раз 26 квітня 1999 року, в річницю чорнобильської аварії.

Вірус заповнював перше 1024 кб завантажувального сектора нулями і виводив з ладу BIOS. Для простих людей це фактично означало знищення комп'ютера.

Згодом CIH зробив друге пришестя, але це окрема історія.

Наступні п'ять років, з 1999 по 2004 роки - це період справжньої гонки озброєння між вірусотворцями, антивірусниками, програмістами Microsoft і користувачами, які ставали все менш довірливими до нехитрих вивертів розповсюджувачів вірусної погані.

Велика частина найбільш небезпечних хробаків цих років використовували численні вразливості в розробках Microsoft - офісних пакетах, операційних системах Windows і Windows Server, серверних додатках Microsoft Internet Information Services, браузерах Internet Explorer і т.д. Продукція Microsoft була вкрай популярною, і її дуже лаяли за її вразливість: для вірусотворців створення черв'яків, що експлуатували проломи, стало справжнім видом спорту.

Melissa (1999) - макровірус, що поширювався самостійно по електронній пошті, використовуючи адресну книгу Microsoft Outlook.

ExploreZip (1999) - вірус, що знищував документи Microsoft Office.

ILOVEYOU, він же LoveLetter (2000) - один з найбільш шкідливих в історії вірусів. Вивуджуючи адреси з адресної книги Outlook, розсилав сам себе по електронній пошті у вигляді вкладення з таким ось файлом: LOVE-LETTER-FOR-YOU.TXT.vbs. За замовчуванням Outlook приховував розширення VBS (а це скрипт на Visual Basic), тому наївному одержувачу здавалося, що це звичайний текстовий файл. А яка може бути шкода від відкриття файлу TXT? Увага, відповідь: від 5,5 до 10 млрд доларів.

Ранні версії ILOVEYOU довантажувати в систему ще і троян Barok, а більш пізні (з 2001 року) "підганяли" і дідуся CIH. Вже якщо пакостити, так по-крупному.

2001 рік - це AnnaKournikova, знову поштовий хробак, вдавав, що у вкладенні листа є малюнок Анни Курнікової в чому мати народила. Автора вірусу зловили і відправили на 150 годин громадських робіт.

2001 рік - вірус Sircam, що поширювався по пошті і через локальні мережі, Code Red і Code Red II, який атакував Microsoft IIS, черв'яки Nimda і Klez. Останній міг забирати із зараженої машини на наступну який-небудь випадково вибраний файл.

Наступним воістину знаменним роком став 2003-й: SQL Slammer, Blaster/Lovesan, Sobig.F і Sober.

SQL Slammer, він же Sapphire і Helkern, з них найвидатніший: 24 січня 2003 року він влаштував формену глобальну катастрофу, залишив без інтернету Південну Корею, порушив роботу банкоматів у США і серйозно сповільнив роботу всього інтернету в цілому - Росії теж дісталося.

Дуже дрібний (менше 400 байт) і спритний, вірус зі страшною швидкістю генерував випадкові IP-адреси і відразу ж відправляв туди свою копію "на удачу". За перші три хвилини атаки вірус уразив 75 тисяч адрес і продовжував розмножуватися як той самий горезвісний штам Андромеди. Втім, атака швидко спала саме тому, що вірус забив всі канали зв'язку і йому більше нікуди було розмножуватися. До того ж, системні адміністратори кинулися латати діри в Microsoft SQL Server, які і використовував черв'як, тож його вдалося швидко приборкати.

Надалі (після того, як у 2004 році MyDoom став вірусом, що найбільш стрімко розповсюджувався в історії) шкідливі програми стали чомусь значно рідше привертати до себе масову увагу. Їх не стало менше, вони змінилися самі - і за формою, і за призначенням.

Вірусотворцям, схоже, набридло в масі своїй змагатися, чий вірус швидше заразить все на світі, розробники ПЗ почали ретельніше ставитися до безпеки, а рядові користувачі стали менш довірливими. Досить разок вляпатися, щоб здорова параноя щодо "лівих" вкладень і дивних посилань виробилася навіки.

Зараз у вірусотворців дещо інші інтереси. Трояни і віруси пишуться не для того, щоб завдати прямої шкоди комп'ютерам, а для того, щоб красти особисту інформацію на зразок номерів кредитних карт і паролів до них (а то навіть й акаунти в онлайнових іграх, благо на них теж можна заробити).

Формовані за допомогою вірусів гігантські ботнети - це теж бізнес. Великий, добротний ботнет - ходовий товар, відмінна зброя, що активно використовується, до речі, в політичній і конкурентної боротьби (особливо в Росії).

У 2007 році багато шуму наробив, наприклад, вірус Storm Worm, за допомогою якого якраз і формувався потужний ботнет, обсяги якого у результаті оцінювалися десь у 50 млн заражених машин (втім, це найбільш песимістична оцінка).

Через такі великі ботнети розсилається велика частина спаму, трояни для розширення ботнету, з їх допомогою організуються DDoS-атаки та інші "принади життя". Оренда ботнетів зараз стала, за деякими оцінками, зовсім недорогою: 9 доларів за годину.

Вінцем творення вірусів на сьогоднішній день є, можливо, все той же Stuxnet - просто в силу своєї оригінальності: такого не бачив ніхто і ніколи.

Про нього вже дуже багато написано. За технічними подробицями можна звернутися, наприклад, до статей Берда Ківі.

Так чи інакше, Stuxnet є серйозною зброєю. Можливо, менш серйозною, ніж хотілося б думати конспірологам, - зрештою, він спочатку призначений для атаки на абсолютно конкретні промислові установки. Але це початок. Історія вірусів не завершена.

22222222