Шацкий Владислав Вадимович
студент четвертого курса
юридического факультета
кафедры государственно-правовых дисциплин,
Российский Государственный
Социальный Университет,
г. Москва, Российская Федерация

Shatskiy Vladislav Vadimovich
fourth year student
Faculty of Law
Department of State and Legal Disciplines,
Russian State Social University,
Moscow, Russian Federation

СОЗДАНИЕ, ИСПОЛЬЗОВАНИЕ И РАСПРОСТРАНЕНИЕ ВРЕДОНОСНЫХ КОМПЬЮТЕРНЫХ ПРОГРАММ

Creation, use and distribution of malicious computer programs

Аннотация: Вредоносное ПО является оружием хакера, главной целью которого является нанесение какого либо ущерба ЭВМ. В 2020 году, проблема связанная с вредоносным по должна заслуживать максимального внимания, так как преступления в данной сфере уже являются не редкостью, а на оборот то явление, с которым сталкиваются всё чаще современные пользователи.

Ключевые слова: Защита информации, вредоносные программы, ПО.

Abstract: Malicious software is a hacker's weapon, whose main goal is to cause any damage to computers. In 2020, the problem associated with malware should deserve maximum attention, since crimes in this area are no longer uncommon, but on the contrary, the phenomenon that modern users are increasingly faced with.

Key words: Information protection, malware, software.

Введение:

В данной статье мы познакомимся с таким понятием, как «Вредоносное ПО» и раскроем его сущность. В настоящее время научно-технический прогресс не стоит на месте, а только развивается и всё больше людей разных поколений вовлекаются в мир компьютерной техники. Бесспорно, что без компьютера современное общество уже не способно существовать, но не всё так хорошо, как кажется на первый взгляд. В глобальной сети, особенно для начинающего пользователя существуют множество опасностей, вызываемые именно из-за вредоносного программного обеспечения. Примером послужит такие технологические недуги, как потеря личных данных и впоследствии выхода из строя отдельных частей персонального компьютера. Происходит это, по большей части, из-за неопытности пользователя, когда последний скачивает информацию из сомнительных источников, тем самым подвергая свой компьютер опасности. Стоит отметить, что вредоносное по является оружием хакера, главной целью которого является нанесение какого либо ущерба ЭВМ. В 2020 году, проблема связанная с вредоносным по должна заслуживать максимального внимания, так как преступления в данной сфере уже являются не редкостью, а на оборот то явление, с которым сталкиваются всё чаще современные пользователи.

Вредоносное программное обеспечение, его сущность и классификация.

Сущностью вредоносной программы является её цель, которая ведет к краже, искажению или удалению личной информации путем несанкционированного доступа к персональному компьютеру. Принято выделять три типа вредоносного программного обеспечения, а именно: троянские программы, сетевые черви и компьютерные вирусы. Перейдем к ним ниже

Компьютерные вирусы

Данный тип вредоносного по является самым распространённым, его главной способностью является способность к самокопированию, что приводит к повреждению или конечному уничтожению данных , принадлежащему пользователю, а в крайний случаях данный вирус способен уничтожить операционную систему в целом.

Практика показывает, что в большинстве случаев заражения виноват сам пользователь, путём пренебрежения проверки файла антивирусной программой. Существуют различные способы заражения. Обычно это происходит через внешний носитель и различные интернет ресурсы.

Вирусы обладают собственными признаками и поэтому делятся по способу заражения или по среде обитания.

Говоря о среде обитания вируса, стоит выделить те вирусы, которые внедряются в выполняемый файл. Также бывают вирусы, которые внедряются в загрузочный сектор диска и сетевые, которые распространяются по всей компьютерной сети. Стоит так же отметить комбинированные вирусы, которые совмещают в себе различные комбинации проникновения в компьютер. Перейдем к способу заражения. Одним из самых распространённых способов , является перезаписывание кода программы, что в последствии приводит к потери работоспособности файла. Следующим идёт паразитический вирус, который изменяет содержимое файла, но оставляет его работоспособным. Существуют также стелс вирусы, которые перехватывают обращение ОС к поражённым файлам и позже направляют их на не зараженные участки информации.

Существуют и Макровирусы, которые используют возможности макроязыков, которые встроены в программы и системы по обработке данных. Примером послужат текстовые редакторы и электронные таблицы.

Сетевые черви

К следующему классу вредоносных программ стоит отнести сетевые черви.

Они являются вредоносным программным кодом, который распространяет свои копии по глобальным или локальным сетям. Конечной целью является проникновение на компьютер, где в дальнейшем уже на компьютере пользователя происходит процесс распространения. «Подцепить» такой вирус можно через электронную почту или в ходе обмена данных между мобильными телефонами. Перейдём к классам сетевых червей.

К первому отнесём класс почтовых червей, где вреданосная программа находится в файле совместно с электронным письмом,

маскируясь под какую либо популярную программу или же попросту обновление системы. Ко второму стоит отнести червя, который использует интернет пейджеры, принцип которого схож с первым примером. Существуют также прочие сетевые черви, способ заражения которого направленна на удалённых компьютерах, где происходит процесс копирования червя на сетевые ресурсы, использования лазеек в операционной системе и паразитирование на других вредоносных программах.

Троянский конь

Программа класса троянский конь была сделана лишь для одной цели, а именно нанесение ущерба компьютера путем противозаконных действий, таких как удаление конфиденциальных данных или их порча, а также нарушение работоспособности компьютера или же использование его ресурсов. Троян коварен, в его способности входят обход системы защиты персонального компьютера. Его «жизненный цикл» таков: Сначала он проникает в систему, позже активируется и в конечном итоге выполняет свою грязную работу. Трояны отличаются между собой по действию, которую они производят непосредственно в персональном компьютере. К первому виду отнесём Троян PSW , чьё назначение является кража паролей. Троян Dowlander доставляет и активирует прочие вредоносные программы. Троян Proxy осуществляет анонимный доступ к компьютеру жертвы. Троян Spy представляет собой шпионскую программу , которая осуществляет шпионаж за пользователем заражённого компрьютера. RootKit, который скрывает присутствия в операционной системе. С помощью программного кода происходит сокрытие присутствия в системе некоторых объектов: процессов, файлов, данных реестра.

История возникновения вредоносного ПО.

В 1949 году, американским учёным Джоном Фон Нэйманом была разработана метематическая теория создания самовоспроизведения программ. В начале семидесятых годов был обнаружен вирус Creeper, который находился в военной компьютерной сети под названием APRAnet, для удаления которого была разработана программа Reaper. Девяностые года двадцатого столетия ознаменовали как годом огромного количества новых вирусов. Предположительно на территории Болгарии, где отличился некий Дарк Эвенджер, чьими усилиями было разработано большое количество новых вирусов. Под конец 90х годов большую популярность получили файловые, загрузочные и файлово загрузочные вирусы. Появляется первый антивирус. В августе 2000 года мир увидел первую вредоносную программу типа Троянский конь. В настоящее время идея вируса превратилась в

криминальный бизнес, поэтому в ряду стран за данное деяние предусмотрено уголовное наказание.

Библиография:

1. Википедия. Свободная энциклопедия: ru.wikipedia.org
2. Классификация вредоносного ПО: http://virus.e-pls.ru
3. Компьютерные вирусы и информационная безопасность: http://inf1.info/book/export/html/118
4. История компьютерных вирусов и вредоносных программ: www.securelist.com
5. Классификация вредоносного ПО: www.winline.ru
6. Анализ наиболее распространенных вредоносных программ и способов защиты от них// Фундаментальные и прикладные исследования в современном мире - Марин Е.А. СПб.: «Стратегия будущего», 2013, №4
7. Энциклопедия компьютерных вирусов. - Козлов Д.А., Парандовский А.А., Парандовский А.К. М.: "СОЛОН-Р", 2001.
8. Никодимов И.Ю. ИНФОРМАЦИОННО-КОММУНИКАТИВНАЯ ФУНКЦИЯ ГОСУДАРСТВА И МЕХАНИЗМ ЕЕ РЕАЛИЗАЦИИ В СОВРЕМЕННОЙ РОССИИ (ТЕОРЕТИЧЕСКИЙ И СРАВНИТЕЛЬНО-ПРАВОВОЙ АНАЛИЗ) диссертация на соискание ученой степени доктора юридических наук / Санкт-Петербург, 2001
9. Никодимов И.Ю. МЕСТО И РОЛЬ СРЕДСТВ МАССОВОЙ ИНФОРМАЦИИ В МЕХАНИЗМЕ РЕАЛИЗАЦИИ ИНФОРМАЦИОННОКОММУНИКАТИВНОЙ ФУНКЦИИ ГОСУДАРСТВА Гуманитарные, социально-экономические и общественные науки. 2014. № 9. С. 216-219.
10. Никодимов И.Ю. ПРИНЦИПЫ И ИСТОЧНИКИ ИНФОРМАЦИОННОГО ПРАВА Юридическая наука: история и современность. 2016. № 3. С. 97-108.
11. Никодимов И.Ю. ТЕОРИЯ ИНФОРМАЦИОННОГО ПРАВА И НЕКОТОРЫЕ АКТУАЛЬНЫЕ ПРОБЛЕМЫ ЕЕ РАЗВИТИЯ Юридическая наука: история и современность. 2015. № 12. С. 91-99.
12. Никодимов И.Ю. СЛОВАРЬ ОПРЕДЕЛЕНИЙ, ПОНЯТИЙ И ТЕРМИНОВ ИСПОЛЬЗУЕМЫХ В ОБЛАСТИ ТЕЛЕКОММУНИКАЦИЙ Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А.Бонч-Бруевича. Рецензенты: Доктор технических наук, профессор А. А. Гоголь; Кандидат юридических наук, доцент В. Ю. Голубовский. Санкт-Петербург, 1999. Сер. Учебники для вузов. Специальная литература