Минитаева А.М., Соколов А.В. Способы и виды инфицирования компьютера загрузочными вирусами // Международный журнал информационных технологий и энергоэффективности. – 2023. –
Т. 8 № 4(30) с. 64–69

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.49

СПОСОБЫ И ВИДЫ ИНФИЦИРОВАНИЯ КОМПЬЮТЕРА ЗАГРУЗОЧНЫМИ ВИРУСАМИ

[1]Минитаева А.М., [2]Соколов А.В.
ФГБОУ ВО "Московский Государственный Технический Университет имени Н.Э. Баумана (Национальный Исследовательский Университет), Москва, Россия (105005, Москва, 2-Я Бауманская ул, д. 5 стр. 1), e-mail: [1]minitaeva@bmstu.ru, [2]andrey.sokolov515@gmail.com

Компьютерные вирусы могут вызывать программные и аппаратные сбои в работе ПК, уничтожать или похищать хранимую на них информацию. Также они могут блокировать работу пользователей, разрушать структуру размещения данных. Они потребляют ресурсы системы и захватывают место на накопителях информации, ухудшают функционирование ПК. В статье рассматриваются виды и способы заражения загрузочными компьютерными вирусами, которые направлены на различные системные области. Представлено описание и характер их воздействия на систему. Результаты анализа и приведенные виды инфицирования являются необходимыми для последующего предотвращения заражения.

Ключевые слова: Загрузочный вирус, главная загрузочная запись, система, инфицирование, сектор.

WAYS AND TYPES OF INFECTING A COMPUTER WITH BOOT VIRUSES

[1]Minitaeva A.M., [2]Sokolov A. V.
Bauman Moscow State Technical University (National Research University), Moscow, *Russia (*105005, *Moscow, 2nd Baumanskaya street, 5 bldg.* 1*), e-mail: [1]minitaeva@bmstu. ru, [2]andrey. sokolov515@gmail. com*

Computer viruses can cause software and hardware malfunctions on PCs and destroy or steal information stored on them. They can also block the user's work and disrupt the data layout. They consume system resources and take up storage space and impair the functioning of a PC. The article discusses the types and methods of infection by bootable computer viruses, which target different system areas. A description and the nature of their impact on the system is presented. The results of the analysis and the types of infection given are essential for the subsequent prevention of infection.

Keywords: Boot virus, master boot record, system, infection, sector.

Введение

Первыми известными успешными компьютерными вирусами были вирусы загрузочного сектора. В 1986 году два пакистанских брата на IBM PC создали первый такой вирус под названием Brain.

В настоящее время методика заражения при загрузке используется редко. Тем не менее, следует ознакомиться с загрузочными вирусами, поскольку они могут заразить компьютер независимо от установленной на нем фактической операционной системы.

1. Вирусы загрузочного типа

Загрузочные вирусы – это наиболее опасный вид вредоносных программ. В отличие от файловых вирусов они записывают свой код не в файлы, а в загрузочный сектор накопителя информации, изменяя программу начальной загрузки, которая должна была загрузить саму операционную систему и передать ей управление.

Вирусы загрузочного сектора используют процесс загрузки персональных компьютеров (ПК). Поскольку большинство компьютеров не содержат операционной системы (ОС) в своей постоянной памяти (ПЗУ), им необходимо загружать систему откуда-то еще, например, с диска или из сети (через сетевой адаптер) [1].

Типичный диск IBM PC состоит из четырех разделов, которым в нескольких операционных системах, таких как MS-DOS и Windows NT, присвоены логические буквы, обычно C:, D: и так далее. Большинство компьютеров используют только два из этих разделов, к которым можно легко получить доступ.

Некоторые поставщики компьютеров, такие как COMPAQ и IBM, часто используют скрытые разделы для хранения на диске дополнительных средств настройки BIOS. Скрытые разделы не имеют назначенных им логических имен, что затрудняет доступ к ним.

Обычно ПК загружают ОС с жесткого диска. Однако в ранних системах порядок загрузки нельзя было определить, и поэтому машина загружалась с дискеты, что давало большие возможности для загрузки компьютерных вирусов до загрузки ОС. ROM-BIOS считывает первый сектор указанного загрузочного диска в соответствии с настройками порядка загрузки в настройках BIOS, в случае успеха сохраняет его в памяти по адресу 0:0x7C00 и запускает загруженный код.

В более новых системах каждый раздел делится на дополнительные разделы. Диск всегда делится на головки, дорожки и сектора. Основная загрузочная запись (MBR) расположена в головке 0, дорожке 0, секторе 1, который является первым сектором на жестком диске. MBR содержит общий, специфичный для процессора код для поиска активного загрузочного раздела из записей таблицы разделов (TP). TP хранится в области данных MBR. В начале MBR находится небольшой код, который часто называют загрузчиком начальной загрузки.

Каждая запись PT содержит следующее:

- адреса первого и последнего секторов раздела
- флаг - всякий раз, когда раздел является загрузочным
- байт типа
- смещение первого сектора раздела от начала диска в секторах
- размер раздела в секторах.

Загрузчик находит активный раздел и загружает его первый логический сектор в качестве загрузочного. Загрузочный сектор содержит код, специфичный для ОС. MBR — это код общего назначения, не связанный с какой-либо ОС. Таким образом, IBM PC могут легко

поддерживать более одного раздела с различными типами файловых систем и операционных систем. Это также делает работу компьютерных вирусов очень простой.

Код MBR может легко заменяться кодом вируса, который загружает исходную MBR после себя и остается в памяти, в зависимости от установленной операционной системы. В случае с MS-DOS загрузочные вирусы могут легко оставаться в памяти и на лету заражать другие вставленные носители. Некоторые загрузочные вирусы, такие как Exebug, всегда заставляют компьютер сначала загружать их в систему, а затем самостоятельно завершать процесс загрузки. Exebug изменяет настройки CMOS в BIOS, чтобы обмануть ПК, заставив его думать, что у него нет дисковода для гибких дисков. Таким образом, ПК сначала загрузится с зараженной MBR. При запуске вирус (с жесткого диска) проверяет, есть ли дискета в дисководе A:, и если есть, загружает загрузочный сектор дискеты и передает ему управление. Таким образом, когда происходит загрузка с дискеты, вирус может заставить поверить, что загрузка действительно произошла с дискеты, но на самом деле это не так.

В случае гибких дисков загрузочным сектором является первый сектор дискеты. Загрузочная запись содержит имена файлов для загрузки, характерные для ОС, например IBMBIO.COM и IBMDOS.COM [2]. Желательно настроить процесс загрузки таким образом, чтобы сначала загружаться с жесткого диска. В IBM PC первого поколения процесс загрузки не был разработан таким образом, поэтому всякий раз, когда дискета оставалась в дисководе A:, ПК пытался загрузиться с нее. Загрузочные вирусы воспользовались этой ошибкой проектирования.

2. Методы заражения основной загрузочной записи

Заражение MBR — относительно тривиальная задача для вирусов. Размер MBR составляет 512 байт. Туда влезает только короткий код, но для небольшого вируса его более чем достаточно. Обычно MBR заражается сразу после загрузки с зараженной дискеты в дисководе A.

2.1. Заражение MBR путем замены кода начальной загрузки

Классический тип MBR-вирусов использует дисковую процедуру INT 13h BIOS для доступа к дискам для чтения и записи. Большинство вирусов MBR заменяют загрузочный код в начале MBR своей собственной копией и не изменяют TP. Это важно, поскольку доступ к жесткому диску возможен только при загрузке с дискеты, когда ПТ находится на месте. В противном случае DOS не сможет найти данные на диске.

Вирус Stoned является типичным примером этой техники. Вирус сохраняет исходную MBR в секторе 7, как показано на Рисунке 1. После того, как вирус получает управление через замененную MBR, он считывает сохраненную MBR, расположенную в 7-м секторе памяти, и передает ему управление. Пара пустых секторов обычно доступна после MBR, и Stoned этим пользуется. Однако это условие не может быть выполнено на 100%, и именно поэтому некоторые вирусы MBR делают систему не загружаемой после заражения.

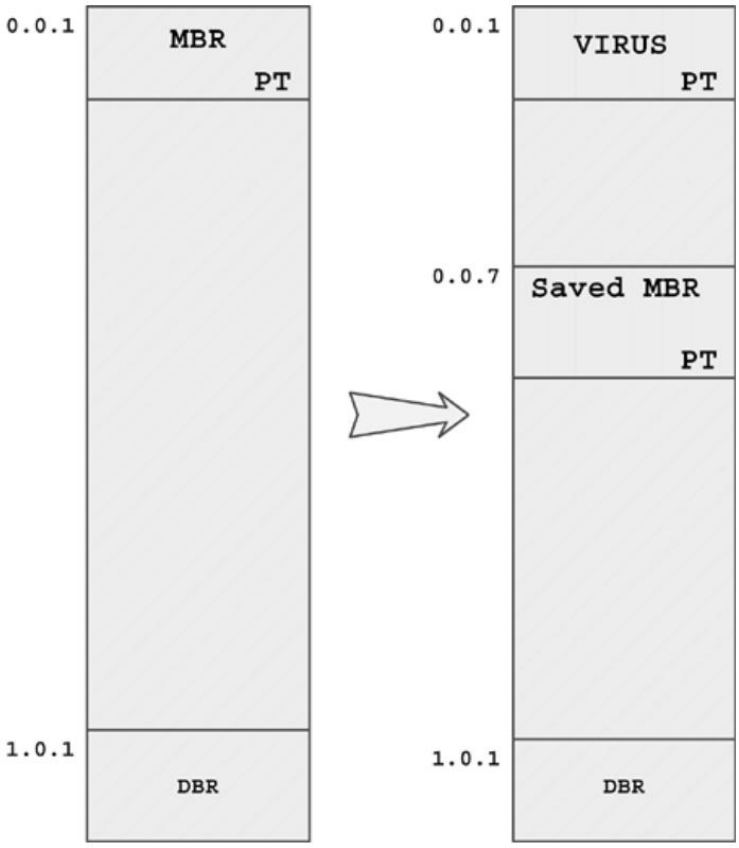

Рисунок 1 – Типичная схема диска до и после заражения Stoned

2.2. Замена кода главной загрузочной записи без его сохранения

Другой способ заражения MBR вирусами заключается в перезаписывании загрузочного кода, оставляя записи TP на месте, но нигде не сохраняя исходную MBR. Такие вирусы выполняют функцию исходного кода MBR. В частности, они ищут активный раздел, загружают его и передают ему управление после себя.

Одним из первых вирусов, использовавших этот метод, был Azusa, обнаруженный в январе 1991 года в Онтарио, Канада [3]. Такие вирусы нельзя вылечить штатными методами, потому что исходная копия MBR нигде не хранится. Антивирусные компании быстро отреагировали на эту угрозу, придумав единый код MBR. Для лечения этот универсальный код MBR был использован для перезаписи кода вируса.

2.3. Сохранение MBR в конец жесткого диска

Распространенный метод заражения MBR — полная замена MBR и сохранение оригинала в конце жесткого диска в надежде, что его там ничего не перезапишет. Некоторые из наиболее осторожных вирусов уменьшают размер раздела, чтобы гарантировать, что эта область диска не будет перезаписана снова. Многокомпонентный вирус Tequila использует эту технику.

3. Методы заражения DOS BOOT Record (DBR)

Вирусы загрузочного сектора заражают первый сектор, загрузочный сектор дискеты. При желании они также могут поражать загрузочные сектора жесткого диска. Существует большое количество известных методов заражения загрузочных секторов. Речь пойдет о самых основных.

3.1. Стандартный метод заражения при загрузке

Один из наиболее часто используемых методов заражения при загрузке был разработан для таких вирусов, как Stoned [4]. Stoned заражает загрузочный сектор дискеты, заменяя 512-байтный загрузочный сектор собственной копией и сохраняя оригинал в конец корневого каталога.

На практике этот метод в большинстве случаев безопасен, но может произойти случайное повреждение содержимого дискеты, если в каталоге дискеты хранится слишком много имен файлов. В таком случае содержимое исходного сектора может перезаписать содержимое каталога.

3.2. Загрузочные вирусы, форматирующие лишние сектора

Некоторые загрузочные вирусы просто слишком велики, чтобы поместиться в одном секторе. Большинство дискет можно отформатировать для хранения большего количества данных, чем их фактический форматированный размер. Не все дисководы гибких дисков поддерживают форматирование дополнительных секторов, но многие имеют это свойство.

Программное обеспечение для защиты от копирования часто использует специально отформатированные «лишние» сектора дискеты, расположенные за пределами обычных диапазонов. В результате обычные инструменты копирования дискет, такие как DISKCOPY, не могут создать идентичную копию таких дискет [5].

Некоторые вирусы специально форматируют набор дополнительных секторов дискеты, чтобы антивирусной программе было труднее получить доступ к исходной копии во время восстановления. Однако обычно дополнительные сектора используются для того, чтобы освободить больше места для более крупного тела вируса.

Заключение

Загрузочные вирусы действуют глубоко внутри компьютера на уровне Master Boot Record (MBR). При запуске электронное устройство действует согласно прописанному в БИОС протоколу. Там ему указывается, какую информацию показать первой, и обычно в приоритетах операционная система. Вирус меняет этот параметр. В итоге вирус загружается первым и может даже уничтожить файлы на жестком диске. Таким образом данный тип вредоносных носителей является одним из самых опасных для информационных систем.

Список литературы

1. Петер С. Искусство нахождения и защиты от компьютерных вирусов. 2005. С. 108-111.
2. Константин К. Компьютерные вирусы и антивирусы: взгляд программиста. 2018. С. 49-60.
3. Усманов А. А. Простые эффективные способы максимальной защиты компьютера от вирусов. 2019. С. 3-7.

4. Блазуцкая Е.Ю., Шарафутдинов А.Г. Вирусы нового поколения и антивирусы. 2015. Т. 1. № 35. С. 92-94.
5. Жуков Д.О. Модели различных стратегий распространения вирусов в компьютерных сетях. 2013. С. 113.

References

1. Peter Szor The art of computer virus research and defense. 2005. pp. 108-111.
2. Konstantin K. Computer viruses and antiviruses: a programmer's view. 2018. pp. 49-60.
3. Usmanov A. A. Simple tests of computer virus protection. 2019. pp. 3-7.
4. Blazutskaya E.Y., Sharafutdinov A.G. New Generation Viruses and Antiviruses. 2015. T. 1. No. 35. pp. 92-94.
5. Zhukov D.O. Models of different strategies of virus spreading in computer networks. 2013. pp. 113.