УДК 004

ПРОДИВОДЕЙСТВИЕ ВРЕДОНОСНЫМ ПРОГРАММАМ

Умрихина О.А., студентка 3курса экономического факультета
Научный руководитель – Голубев С.В., к.э.н, доцент
ФГБОУ ВО Ульяновский ГАУ

Ключевые слова: *вредоносное программное обеспечение, антивирус, сканирование, имунизаторы.*

В настоящее время имеется около тысячи видов вредоносных программ. Учитывая тот факт, что каждый из них существует в нескольких модификациях, нужно увеличить это число в 5-10 раз Большинство распространяется одним из двух методов: заражая файлы или загрузочные сектора.

Вредоносное программное обеспечение – это специально разработанная программа, которая может сделать их собственные копии и выполнить их в системных ресурсах. Пользователь замечает, что, когда нарушается работа его техники, не запускается приложение, прекращает работать компьютер. Мир этих вредоносных программ все еще не изучен. Всегда есть новые и более сложные вредители. Даже опытные системные администраторы часто не знают, как они распространяются и что собой представляют.

В настоящее время теория и практика информационной безопасности разработали в двух существенно различных направлениях для способов антивируса:

1. На основе понятия структурно -независимых механизмов для обеспечения информации и предполагает независимость информационных процессов и процессов противодействия программ. В этом направлении программы антивируса и программное обеспечение (ПО) для безопасных информационных систем проектированы и разработаны независимо друг от друга, и программы антивируса уже присоединяют к разработанному ПО.

2. На основе понятия структурно-зависимых механизмов защиты информации предполагает зависимость этих процессов. Это принимает двухуровневая система, идентификации воздействия вредоносного программного обеспечения: идентификация факта воздействия и идентификация трассировок влияния.

Реализация структурно-независимых механизмов идентифицирует вредоносное программное обеспечение в безопасных информационных системах на основе методов их обнаружения с помощью профессиональных инструментов антивируса пакетов. Основные методы:

- сканирование;
- эвристическое сканирование;
- антивирусный контроль;
- иммунизация.

Принцип работы антивирусного сканера на основе сканирования файлов, секторов и системной памяти, а также поиска известного и нового вирусы. Искать известные вирусы, используя так называемую последовательность «подписи» байтов, которая исключительно характерна для определенного вируса.

Универсальность методов эвристического сканирования позволяет обнаружение большого количества вредоносного программного обеспечения. Антивирусный монитор - резидентные программы, которые управляют возникновением ситуаций, связанных с работой вредоносного программного обеспечения.

Имунизаторы - программы, которые подражают зараженным файлам с вредоносным программным обеспечением.

Чтобы снизить риск потерь от влияния вредоносного программного обеспечения, рекомендуется что:

- использовать современную операционную систему с серьезным уровнем защиты из вредоносных программ;

- работайте только с разрешенными пользовательскими правами на своем персональном компьютере;

- используйте специализированное программное обеспечение для использования антивируса;

- используйте продукты антивирусного программного обеспечения известные производители с автоматическим обновлением баз данных;

- не открывайте компьютерные файлы, полученные от не доверяемых источников;

Современные средства защиты от различных форм вредоносного программного обеспечения включают много компонентов программного обеспечения и методов открытия «хорошие» и «плохие» приложения. Сегодня поставщики продуктов встраивают в их программы скане-

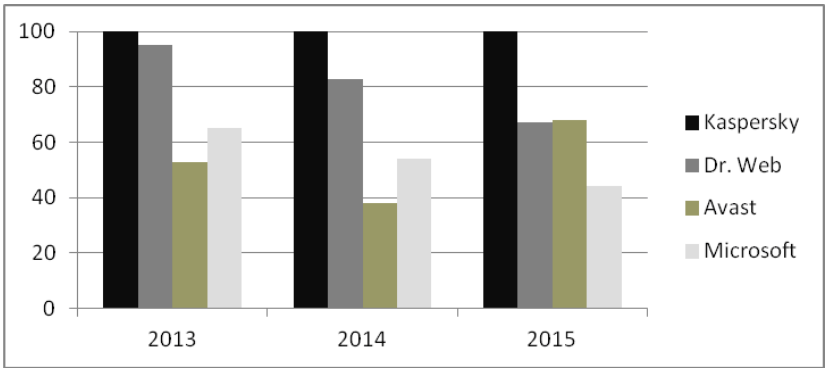

Рисунок 1 - Динамика изменения возможностей антивирусов по лечению вредоносных программ

ры, чтобы обнаружить «шпиона» и другой вредоносный код. Однако ни один пакет против шпионских программ не совершенен. Один продукт может быть, слишком тесно касаться программ, блокируя при малейшем подозрении, включая «вычищение» и полезные утилиты, которые регулярно используются.

В отличие от антивирусных пакетов, которые регулярно показывают,100% эффективность по обнаружению вирусов в профессиональном тестировании, проводимом такими экспертами, как «Virus Bulletin» (британский журнал, посвященный предотвращению, обнаружению и удалению вредоносного ПО и спама), никакой пакет против рекламных программ не получает больше 90%, а эффективность других продуктов определена между 70% и 80%.

Опыт показывает, что один пакет должен использоваться в качестве постоянного «блокировщика», который загружается каждый раз, при включении компьютера, в то время как другой пакет (или больше) должен запускаться, по крайней мере, один раз в неделю, чтобы обеспечить дополнительное сканирование. Таким образом, то, что пропустит один пакет, другой может обнаружить.

Библиографический список

1. Касперски, К. Техника сетевых атак. Приемы противодействия / К. Касперски. — М.: Солон-Р, 2001.— 397 с.

2. Сердюк, В.А. Перспективные технологии обнаружения информационных атак / В.А. Сердюк // Системы безопасности.— 2002.— № 5(47).— С. 96—97.
3. Точки входа вируса [Электронный ресурс]. - URL: http://www.viruslab.ru.
4. Что такое компьютерные вирусы, и как они работают [Электронный ресурс].— URL: http://www.frolov-lib.ru.

COUNTERACTION TO MALICIOUS APPLICATIONS

Umrikhina O. A.

Keywords: *malicious software, antivirus, scanning, imunizator.*

Now about thousands of malicious applications are reckoned. Considering the fact that each of them exists in several modifications, it is necessary to increase this number at 5-10 times the Majority extends one of two methods: infecting files or boot sectors.