**МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ**

**БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ**

**Факультет прикладной математики и информатики**

Кафедра технологий программирования

СЕЧКО МАРИНА ЮРЬЕВНА

**Визуализация данных о вредоносном ПО**

Курсовая проект

студента 3 курса 9 группы

|  |  |
| --- | --- |
| “Допустить к защите”  с предварительной оценкой\_\_\_\_\_  **Руководитель работы**  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  “\_\_\_“ \_­­\_\_\_\_\_\_\_\_\_\_­­\_\_\_\_\_ ­­2017 г. | “Допустить к защите”  **Руководитель**  *Мушко Вилена Владимировна*  доцент кафедры ТП |

**Минск 2017**

**МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ**

**БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ**

**ФАКУЛЬТЕТ ПРИКЛАДНОЙ МАТЕМАТИКИ И ИНФОРМАТИКИ**

**Кафедра технологий программирования**

**ВИЗУАЛИЗАЦИЯ ДАННЫХ О ВРЕДОНОСНОМ ПО**

Курсовой проект

|  |  |
| --- | --- |
|  | Сечко Марины Юрьевны  студента 3 курса,  специальность «компьютерная безопасность»  Научный руководитель:  доцент кафедры технологий программирования, Мушко Вилена Владимировна |

**МИНСК, 2017**

**РЕФЕРАТ**

Курсовой проект, ХХ стр., ХХ рис., ХХ источников.

**Визуализация данных о вредоносном ПО**

Ключевые слова:

Объект исследования –.

Цели работы –

Результат работы –

Область применения –

**СОДЕРЖАНИЕ**

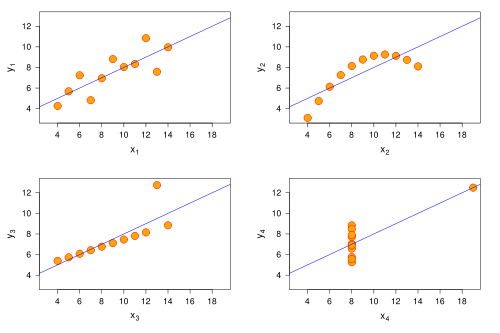
**ВВЕДЕНИЕ**

Визуализация данных - один из методов, используемых для передачи данных или информации путем их представления в виде визуальных объектов (например, точек или линий), содержащихся в графике.

Первичной целью визуализации данных является четкая и эффективная передача информации с помощью статистической графики, графиков и информационной графики (инфографики).

Визуализация данных – это и искусство, и наука. Как эстетичность и красота, так и функциональность должны идти рука об руку, обеспечивая понимание довольно разреженного и сложного набора данных, передавая его ключевые аспекты более интуитивно понятным способом.

Отличным примером важности визуализации данных является так называемый квартет Энскомба — четыре набора числовых данных, у которых простые статистические свойства (среднее значение, дисперсия, корреляция) идентичны, но их графики существенно отличаются.



Уже из этого можно сделать вывод, что при анализе данных визуализация данных не только желательно, а даже необходима.

Область применения визуализации достаточно велика – она используется в научных и статистических исследованиях (в частности, в прогнозировании, интеллектуальном анализе данных, бизнес-анализе), в педагогическом дизайне для обучения и тестирования, в новостных сводках и аналитических обзорах. Сфера анализа вредоносного программного обеспечения не стала исключением в потребности визуализации.

**1. АНАЛИЗ ВРЕДОНОСНОГО ПО**

Из-за растущей угрозы со стороны вредоносного программного обеспечения исследование уязвимых систем становится все более важным. Необходимость регистрации и анализа активности охватывает сети, отдельные компьютеры, а также мобильные устройства. Хотя существуют различные автоматические подходы и методы для обнаружения и идентификации вредоносных программ, фактический анализ постоянно растущего числа подозрительных образцов является трудоемким процессом для аналитиков вредоносного ПО. Использование визуализации может помочь поддержать этот процесс анализа в отношении исследования, сравнения и обобщения образцов вредоносных программ.

Существует два основных подхода к анализу вредоносного ПО: статический и динамический.

* Статический анализ описывает методы, которые не требуют фактического выполнения проверяемого образца. В зависимости от глубины анализа файл может быть проверен на его основные свойства (например, тип файла, контрольная сумма), легко извлекаемая информация (например, строки, информация об импортах DLL) или полностью разобран.
* Динамический анализ выполняет файл в главной системе, при этом различные инструменты контролируют выполнение проверяемого образца и записывают соответствующую информацию в лог выполнения. В зависимости от глубины анализа, это могут быть как простые операции файловой системы, так и целые инструкции, захваченные через отладчик.

Несмотря на то, что динамический анализ может показать больше при базисном (имеющем небольшую глубину) анализе, при более продвинутом анализе вредоносного ПО используют именно статический анализ – при помощи дизассемблеров, методов обратной разработки и так далее. Причиной этому является зависимость динамического анализа от среды анализа: данные, полученные при этом типе анализа, могут являться не полными в силу текущих свойств соответствующей системы. Однако, статический анализ проводится медленнее, так как аналитику приходится разбираться в структуре исполняемого файла.

Также существует несколько целей, для которых используется анализ вредоносных программ.

* Индивидуальный анализ используется для анализа отдельного образца вредоносного ПО, выявления целей его выполнения и пути их достижения.
* Классификация вредоносного ПО. Здесь анализ используется для определения семейства вредоносных программ, к которому относится заданный образец.
* Анализ выборки образцов. В этом случае анализ используется для выявления схожести в поведении большого количества образцов вредоносного ПО с целью получения какой-либо статистики.

**2. ПИКСЕЛЬНЫЕ МЕТОДЫ ВИЗУАЛИЗАЦИИ**

Методы визуализации приобретают все большее значение при изучении и анализе больших объемов многомерной информации. Одним из важных методов визуализации, который особенно интересен для визуализации таких больших и многомерных наборов данных, является класс пиксельных методов – dense pixel display. Основная идея пиксельных методов визуализации состоит в том, чтобы одновременно представлять как можно больше объектов данных на экране путем сопоставления каждого значения данных с пикселем экрана, учитывая его цвет и расположение.

**СПИСОК ЛИТЕРАТУРЫ**