Секция: Информатика
Университетский лицея №1511 предуниверситарий НИЯУ МИФИ
Пролетарский проспект д. 6, корп. 3, Москва, 115522
Тел.: +7 (495) 788-56-99, доб. 5808; +7 (499) 324-29-21, e-mail: info@1511.ru

Средство обхода сигнатурного анализа антивирусного ПО

Пустовит Владислав, Смирнов Владислав, Жеребятин Илья
Класс: 10

Научные руководители:

- Когос Константин Григорьевич - Доцент отделения интеллектуальных кибернетических систем офиса образовательных программ, ИИКС НИЯУ МИФИ, кафедра №42
- Пархомец Павел Петрович - студент 4-го курса, каф 42, лаборант ИИКС НИЯУ МИФИ

Цель проекта: показать, что статический анализ не является самодостаточным методом защиты как персональных ПК, так и отдельных сетевых сегментов, и продемонстрировать необходимость внедрения дополнительных методов защиты.

В настоящее время проблемы информационной безопасности стоят наиболее остро. Одной из главных причин данного вопроса является широкое распространение различного рода компьютерных вирусов, целью которых становится похищение пользовательских данных, нанесение вреда и тд. В процесс борьбы с вирусами вовлечены многие компании, например, Лаборатория Касперского, Microsoft, Dr. Web. Хоть их решения и считаются одними из лучших на рынке антивирусного ПО, но идеальными они не являются, поскольку в них широко используется статический анализ.
Статический (или сигнатурный) анализ вредоносного программного обеспечения - один из видов проверки файлов на наличие в них участков кода или инструкций, которые могут привести к нанесению определенного вреда пользователю или информационной системе. Недостатком данного метода является необходимость заранее подготовленной базы данных сигнатур вредоносного ПО, так называемых паттернов. Во время самого анализа осуществляется поиск данных паттернов в файле. Если такой паттерн был найден, то файл считается зараженным.

Логика функционирования разработанного ПО:

1. На сайт поступает файл и тип мутации.
2. Этот набор отправляется на мутатор (Мутатор - программа, которая изменяет вирус по выбранному шаблону, т.е. типу мутации).
   Алгоритм работы мутатора:
   1) пользователь загружает вирус и выбирает тип мутации;
   2) по выбранным типам мутации загруженный вирус изменяется.

3. После преобразования полученный файл с помощью API отправляется на проверку на virustotal.com.
4. От virustotal.com ответ через API отправляется в базу данных сайта.
5. Полученный результат сканирования отображается на сайте.
6. На основе результатов формируется рейтинг антивирусного ПО в соответствии с количеством обнаруженных вирусов.

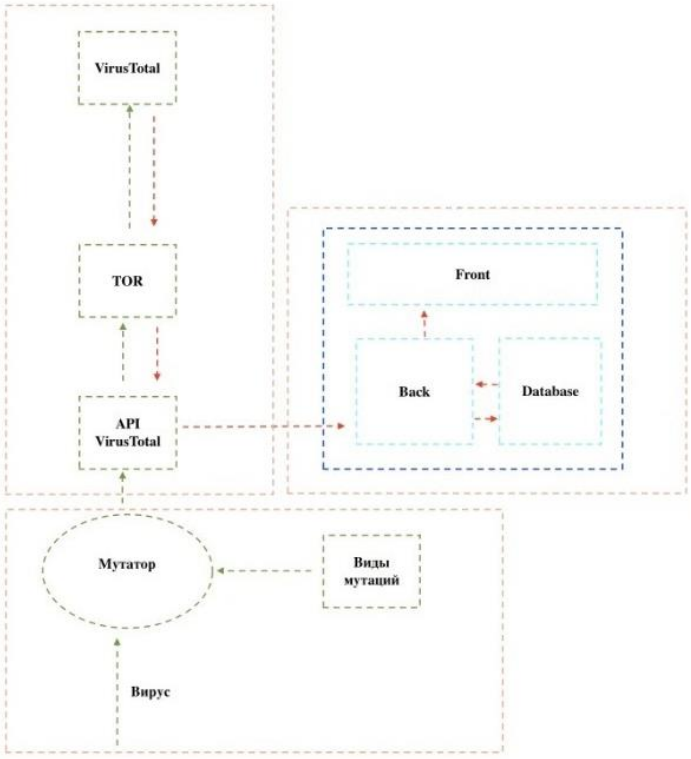

Рис. 1. Схема работы разработанного ПО

Актуальность:

1. Суммарный ежедневный рост различного вида ВПО.
2. Появление нового вида ВПО
3. Наличие большого количества антивирусных программ, которые не обеспечивают должной информационной безопасности;
4. Широкое распространение и появление новых информационных систем и технологий, требующих защиты.

Литература:

https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html
https://ru.wikipedia.org/wiki/%D0%A1%D0%B8%D0%B3%D0%BD%D0%B0%D1%82%D1%83%D1%80%D0%BD%D1%8B%D0%B9_%D0%B0%D0%BD%D0%B0%D0%BB%D0%B8%D0%B7