Средство обхода сигнатурного анализа антивирусного ПО

Всероссийский конкурс научных работ школьников «Юниор», 1 февраля 2020 года

Авторы проекта: Пустовит Владислав, Смирнов Владислав и Жеребятин Илья

Предуниверситарий НИЯУ МИФИ Университетский лицей 1511, Москва

Научные руководители: Когос Константин Григорьевич и Пархомец Павел Петрович

Цель работы

Показать, что статический анализ не является самодостаточным методом защиты как персональных компьютеров, так и отдельных сетевых сегментов, продемонстрировать необходимость внедрения дополнительных методов защиты.

Актуальность

1. 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.

Введение

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 т.д. 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 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.

Программное решение

Для того чтобы продемонстрировать недостаток статического анализа современного ВПО, разработано программное решение, с помощью которого его пользователь может преобразовать (мутировать) файл и отправить его на проверку на наличие ВПО. В результате антивирусное ПО, использующее такой метод обнаружения ВПО, как сигнатурный анализ, с большей вероятностью не сможет обнаружить вирус, который находится в файле.

Список используемой литературы

1. Доктрина информационной безопасности РФ
2. Документация Python, https://www.python.org/doc/
3. Документация Flask, http://flask.palletsprojects.com/en/1.1.x/

Логика функциональности 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.

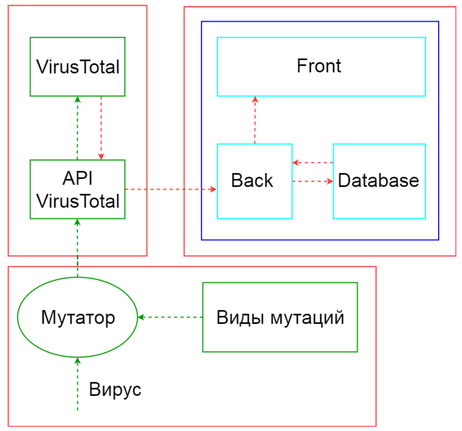


Рис. 1. Схема разработанного ПО

О сайте

- Для отправки файлов разработан сайт с специальной формой, с помощью которой пользователь может выбрать вирус и по определенному типу мутации его преобразовать, после чего отправить мутированный файл на проверку наличия в нем ВПО на сайт VirusTotal с помощью разработанного API . На созданном сайте есть страница с историей запросов пользователя, где есть ссылки на результат каждого из них. На главной странице сайта описаны цель проекта и функциональность программного решения.
- Веб-сайт разработан на языке программирования Python с помощью микрофреймворка Flask с использованием виртуального окружения. Базой данных была выбрана MongoDB.

О мутаторе

Мутатор создан на языке программирования Python. Для преобразования ВПО используется 3 вида мутации: "Joiner", "Cryptor", "WinRAR".

О вирусах

- **Trojan -** программы, осуществляющие различные неподтверждённые пользователем действия: сбор информации банковских карт и т.п. и её передачу злоумышленнику. Также троянские программы могут устанавливать рекламные модули, используются для блокировки обнаружения вирусов.
- **Stealer -** программа, ворующая с вашего компьютера пароли, куки, данные автозаполнения, кредитные карты.
- **Winlocker -** программа, полностью блокирующая ОС Windows от любого воздействия. Для разблокировки нужно ввести пароль. Чаще используется с целью вымогательства.
- **RAT -** программа удалённого управления. Расшифровывается как Remote Administration Tool.

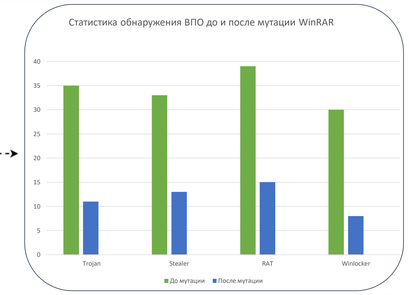
Результаты

В результате работы было получено программное решение, которое позволяет изменить структуру бинарного файла таким образом, что количество обнаружений ВПО уменьшается в разы. Подтверждено, что сигнатурный анализ файлов не является самодостаточным методом защиты от ВПО.

WinRAR

Порядок действий WinRAR состоит в нахождении повторяющихся последовательностей, которым назначается другое, более короткое, сочетание байт. К полученному материалу добавляется словарь - расшифровка коротких сочетаний.

Рис. 2. Схема работы мутации WinRar



Joiner

Джойнер (Joiner) – это некое программное обеспечение, которое позволяет объединять несколько файлов в один с возможностью присоединения к полученному файлу произвольной иконки. Джойнер нужен для того, чтобы склеить вирус с другим файлом.

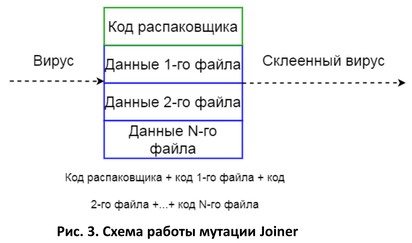
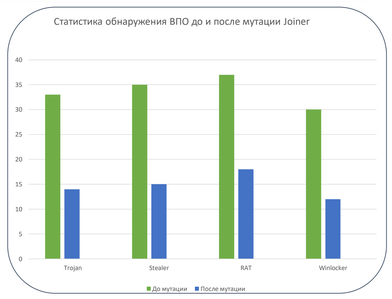


Рис. 3. Схема работы мутации Joiner



Cryptor

Cryptor (шифровщик) – это название одного из вида программных продуктов, которые используются программистами-вирусописателями для того, чтобы скрыть вредоносную сущность написанного ими программного обеспечения от антивирусных программ.
Суть их работы состоит в последовательных действиях стаб. Стаб в этом случае — это отдельная программа, к которой прикрепляется шифруемый файл. При запуске файл расшифровывается и запускается. Криптор, шифруя программу, обеспечивает защиту вредоносного программного кода от распространённых антивирусных методов поиска по сигнатурам.

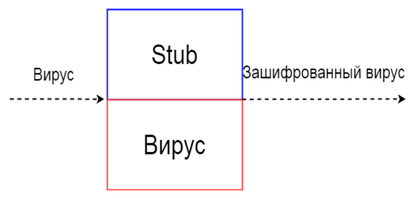


Рис. 4. Схема работы мутации Cryptor