Оглавление.

Введение.

Современное вредоносное программное обеспечение (*далее ВПО*) в общем случае представляет из себя исполняемые файлы, упакованные и зашифрованные сложнополиморфными алгоритмами. В отличие от полиморфных вирусов конца 90-х годов, современное ВПО в подавляющем большинстве случаев не содержит механизм размножения и не включает генератор полиморфного кода, который использовался для их маскировки. Соответственно, их маскировочные алгоритмы недоступны для анализа. Это т.н. offline полиморфизм, при котором после анализа и детектирования очередного образца ВПО немедленно в полуавтоматическом режиме создаётся и распространяется новый образец (обычно 15-30 образцов в сутки), и server-side полиморфизм, при котором новый шифрованный образец ВПО создаётся автоматически на стороне сервера ВПО при каждой очередной инсталляции.

Алгоритмы, разработанные против традиционных полиморфных вирусов, такие как эмуляция кода или попытки воспроизвести криптографический алгоритм в антивирусе, показали свою низкую эффективность применительно к подобным угрозам. Эмуляция кода снижает производительность антивирусного ПО, и в случае сложнополиморфных вирусов требует неприемлемых временных затрат. [**пример – RDA.Fighter, Idea и что-нибудь из нового**].Анализ криптографического алгоритма требует усилий высококвалифицированных специалистов, которые не в состоянии обработать файловый поток новых образцов ВПО.

В связи с эволюцией ВПО возникла необходимость разработки более рациональных методов предварительного анализа с целью детектирования новых образцов известного ВПО, прежде всего выявления характерных для каждого семейства ВПО признаков.  
Такими характерными признаками являются распределение информационной энтропии в исследуемом образце, характерный набор импортируемых функций, некоторые особенности формирования исполняемых файлов.

В данной работе была предпринята попытка анализа характеристик информационной энтропии исполняемых файлов. Для анализа был разработан адаптивный алгоритм на основе сигмоидальных нейросетей.

Обзор литературы.  
Эксмпериментальная часть.  
Заключение.  
Список литературы.

Приложения.