2. И.И. Пилецкий и др. Виртуальная ИТ среда БГУИР для исследования Big Data и VCL, с. 21-32, BIG DATA and Predictive Analytics. Использование BIG DATA для оптимизации бизнеса и информационных технологий : сборник материалов междунар. науч.-практ. конф. / редкол. : М.П. Батура [и др.]. – Минск : БГУИР, 2015. – 220 с. ISBN 978-985-543-146-7. - С. 21-32.
3. What is the IBM Cloud platform? [Электронный ресурс] / IBM developerWorks. – 2017-2018. – Режим доступа: https://console.bluemix.net/docs/overview/ibm-cloud-platform.html#whatis. – Дата доступа: 19.03.2019.
4. IBM RCIS Watson Cloud Cognitive University [Электронный ресурс] / IBM Developer Works. – 2016-2019. – Режим доступа: https://www.ibm.com/developerworks/community/groups/service/html/communitystart?communityUuid=bc004137-b64a-4378-ac02-2caf59c56c2a. – Дата доступа: 19.03.2019.

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОС WINDOWS

Андреюк Д. С., Кадушко А. А., Малиновская Е. Д.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Стройникова Е. Д. – ассистент кафедры информатики

В процессе изучения предметной области была собрана и систематизирована информация о вредоносном программном обеспечении и информационных атаках. В результате была смоделирована и протестирована вредоносная программа, сокрытая в обыденном для обычного пользователя приложении.

В работе были изучены уязвимости ОС Windows относительно сохранности конфиденциальных и личных данных. Основной акцент был сделан на деятельности вредоносного программного обеспечения на примере вирусов, червей и троянов. Была приведена статистическая информация о деятельности вредоносного программного обеспечения с момента их возникновения. Продемонстрированы прецеденты наиболее масштабных и результативных вирусных атак за XX – XXI вв., таких как WannaCrypt0r, Jerusalem, CIH и подобных. Выведены критерии сравнения и классификации разного рода атак, изучаются их предпосылки, реализация, результаты и специфика. Рассмотрены особые беспрецедентные случаи осуществления атак (например, с использованием «умной» бытовой техники). Изучена также возможность осуществления DDoS-атак в социально-приемлемых целях. В процессе рассмотрения деятельности вредоносного программного обеспечения сделан упор на механизмы шифрования и распространения в прогностических интересах. Изучены способы сокрытия признаков деятельности вредоносного программного обеспечения (встраивание в код полезной программы, маскировка под неё и др.) с целью выявления специфики вредоносного программного обеспечения и планирования контрмер в виде разработки антивирусного программного обеспечения. В целом подход к изучению вредоносного ПО в данной работе использует концепцию «Знай врага в лицо».

В практической части продемонстрирована работа искусственно созданной программы, деятельность которой в не тестовом случае однозначно нежелательна. Пример представляет собой игру, запуск которой приводит к шифрованию файлов на жестком диске шифром Цезаря. Продемонстрирован механизм сокрытия, проникновения и шифрования самодельного трояна. Рассмотрены различные шифры (Цезаря, Виженера, многоалфавитная замена и др.), методы поиска ключей и дешифрования (на основе шифротекста, открытого текста и др.). Произведена классификация шифров, их сравнение, рассмотрено их использование в предметной деятельности. Изучены возможные исходы деятельности вредоносного программного обеспечения, способы восстановить утраченные или поврежденные данные. Предложены возможные меры профилактики утраты конфиденциальных данных. Спрогнозирована дальнейшая деятельность вредоносного программного обеспечения. Осуществлена рефлексия последующих цифровых эпидемий и их возможного исхода.

Список использованных источников:

1. WannaCry 2.0: наглядное подтверждение того, что вам обязательно нужно правильное решение для надежного бэкапа [Электронный ресурс]. – 2017. – Режим доступа: https://habr.com/ru/company/acronis/blog/328796/.
2. Холодильник атакует: как киберпреступники используют бытовую технику [Электронный ресурс]. – 2016. – Режим доступа: https://www.rbc.ru/technology_and_media/13/11/2016/5825cf889a79475b671ff971/.
3. Вредоносное ПО, вошедшее в историю. Часть II [Электронный ресурс]. – 2017. – Режим доступа: https://habr.com/ru/company/ua-hosting/blog/407621/.
4. Азбука безопасности [Электронный ресурс]. – 1998. – Режим доступа: https://kaspersky.antivirus.lv/rus/threats/safetyabc/.
5. Вирусы XXI века [Электронный ресурс]. – 2016. – Режим доступа: https://geekbrains.ru/posts/xxi_viruses/.
6. Самые разрушительные компьютерные вирусы начала XXI века [Электронный ресурс]. – 2018. – Режим доступа: https://www.iguides.ru/main/other/samye_razrushitelnye_kompyuternye_virusy_nachala_xxi_veka/.

7. Самые опасные вирусы за всю историю существования компьютеров [Электронный ресурс]. – 2013. – Режим доступа: https://www.osp.ru/pcworld/2014/01/13038813/.

8. Десять самых громких хакерских атак в истории интернета [Электронный ресурс]. – 2014. – Режим доступа: https://republic.ru/posts/l/1139636/.

9. Вирусы, статистика и немного всего [Электронный ресурс]. – 2017. – Режим доступа: https://habr.com/ru/post/357426/.

10. Новая работа для графических процессоров: GPU защитит от вирусных атак [Электронный ресурс]. – 2018. – Режим доступа: https://habr.com/ru/company/1cloud/blog/354526/.

11. «Разрубить Гордиев узел», или преодоление проблем шифрования информации в ОС Windows [Электронный ресурс]. – 2016. – Режим доступа: https://habr.com/ru/company/aladdinrd/blog/304024/.

12. Уязвимости SSD с аппаратным шифрованием позволяют злоумышленникам легко обходить защитные меры [Электронный ресурс]. – 2016. – Режим доступа: https://habr.com/ru/post/428964/.

13. Прозрачное шифрование: преимущества и недостатки [Электронный ресурс]. – 2015. – Режим доступа: https://habr.com/ru/company/cybersafe/blog/251041/3/.

14. Срыв масштабной хакерской атаки на пользователей Windows в России: часть 2 [Электронный ресурс]. – 2018. – Режим доступа: https://habr.com/ru/company/microsoft/blog/351692/.

СРАВНЕНИЕ АЛГОРИТМОВ РЕШЕНИЯ ЗАДАЧИ КОММИВОЯЖЁРА

Астрашаб В. В., Бондарев И. М., Клебанов Д. А.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Стройникова Е. Д. — ассистент кафедры информатики

В докладе рассматривается одна из ключевых задач комбинаторной оптимизации — задача коммивояжёра. Формулируется суть задачи, рассматриваются различные алгоритмы её решения, а также анализируются и сравниваются результаты выполнения алгоритмов при различных наборах входных данных.

Задача коммивояжёра — одна из самых известных задач в комбинаторной оптимизации. Она заключается в следующем: «Зная список городов и их координаты, найдите самый короткий путь, проходящий через все города один раз и возвращающийся в исходный город».

Данная задача была впервые сформулирована в 1930 г. и до сих пор является одной из наиболее интенсивно изучаемых задач оптимизации. Ричард Карп в 1972 г. доказал NP-полноту задачи поиска гамильтоновых путей, из чего, благодаря полиномиальной сводимости, вытекала NP-трудность задачи коммивояжёра. На основе этих свойств им было приведено теоретическое обоснование сложности поиска решений задачи на практике.

Задача коммивояжёра используется в логистике, транспорте, проектировании различных коммуникационных сетей и трубопроводов, а также в других сферах.

Вместе с простотой определения и сравнительной простотой нахождения хороших решений задача коммивояжёра отличается тем, что поиск действительно оптимального пути является достаточно сложной задачей.

Существует множество различных способов решения данной задачи, которые можно разделить на несколько групп:

1. Точные алгоритмы — алгоритмы, которые находят гарантированно верное решение.

Примеры:

A. Полный перебор всех возможных путей. Сложность алгоритма $O(N!)$.
B. Алгоритм Хелда — Карпа — алгоритм динамического программирования. Сложность алгоритма $O(N^2 * 2^n)$.
C. Метод ветвей и границ — вариация полного перебора с отсевом подмножества заведомо неоптимальных решений.

Ключевое преимущество алгоритмов данной группы заключается в том, что они гарантированно находят верное решение, чего не позволяют сделать алгоритмы из других групп. Однако на практике эти алгоритмы почти никогда не применяются ввиду огромных временных затрат даже при небольших значениях N.

2. Эвристические алгоритмы — алгоритмы, которые не гарантируют точного решения, однако достаточны для решения поставленной задачи.

Примеры:

A. Деревянный алгоритм — алгоритм решения через построение кратчайшего остовного дерева. Сложность $O(N^2)$.
B. Алгоритм ближайшего соседа — жадный алгоритм, который строит путь, находя самую ближнюю к данной вершину. Сложность $O(N^2)$.
C. 2-opt алгоритм — алгоритм, сводящийся к удалению двух пересекающихся рёбер и вставке новых рёбер, не нарушающих корректности решения. Сложность $O(N^2)$.