```
args = parser.parse_args()
return args
if __name__ == '__main__':
args = get_args()
image_comparator = ImageComparator(
    args.image1,
    args.image2,
    args.save_to,
    args.min_color_diff,
    args.min_quad_size)
image_comparator.compare_images()
```

В роботі розглянуто приклад роботи програми при порівняні зображень супутникових знімків аеродрому з використанням послідовності кроків розбивки зображень, поки не буде досягнута задана точність, та порівнянь їх дерев квадрантів. Також наведена залежність часу виконання роботи програми, в залежності від площі мінімального вузла. В результаті порівняння зображень отримано третє результуюче з вмістом отриманих результатів. Цей метод дозволяє порівнюючи карти місцевості, отримані в результаті періодичної зйомки, виявляти об'єкти що з'являються або зникають у місцях проведення контролю місцевості, без участі людини.

Література

1. «Выглядит похоже». Как работает перцептивный хеш. – [Електронний ресурс]. – Режим доступу: https://habrahabr.ru/post/120562/.

2. Лукін В.Є. Аналіз використання технології штучних нейронних мереж в якості нового підходу до обробки сигналів // В.С. Лукін / Телекомунікаційні та інформаційні технології. – №3. – Київ, 2014. – С. 81-88.

3. Петин В. Микрокомпьютеры Raspberry Pi: Практическое руководство // В. Петин. – СПб: Питер, 2015. – 240 с.

4. Прохоренок Н.А. Python 3 и PyQt 5. Разработка приложений // Н.А. Прохоренок, В.А. Дронов. – СПб: БХВ-Петербург, 2016. – 812 с.

5. Квадродеревья и октодеревья – [Електронний ресурс] Режим доступу: http://loi.sscc.ru/gis/QuadTree/QuadTree.html.

Дослідження та класифікація основних типів загрозливих програм

Кушнерик О.О.
Науковий керівник – к.т.н., доц. Джулій В.М.
Хмельницький національний університет

Однією з ключових сучасних проблем забезпечення комп'ютерної безпеки є необхідність ефективної протидії загрозливим програмам. При цьому необхідно враховувати, що це можуть бути, як самостійні програми,

покликані здійснювати відповідні несанкціоновані дії, так і цілком легальні, санкціоновано використовувані додатки, що наділяються в процесі роботи загрозливими властивостями. У загальному випадку атаки подібних програм можуть бути націлені, як на розкрадання даних, так і на виведення з ладу комп'ютерних ресурсів, як наслідок, об'єктами захисту, стосовно до даних загроз, повинні бути, як інформаційні, так і системні комп'ютерні ресурси. Існуюча статистика зростання загрозливих програм дозволяє припустити про низьку ефективність методів вирішення найбільш актуальних сучасних завдань захисту інформації. Незалежно від типу, загрозливі програми здатні завдавати значної шкоди, реалізуючи будь-які загрози інформації - порушення цілісності, конфіденційності, доступності.

Загрозливі програми прийнято ділити на класи за такими основними ознаками: місце існування; обсяг завданої шкоди; особливості алгоритму роботи; операційна система.

Загрозливі програми (ЗП) по природному середовищі можна розділити на наступні типи: макро; завантажувальні; мережеві; файлові; скриптові. За обсягом заподіяної шкоди ЗП діляться на: безпечні - в результаті свого поширення обмежуються зменшенням вільної пам'яті на диску; небезпечні - можуть привести до серйозних збоїв в роботі комп'ютера або ОС; дуже небезпечні - можуть привести до втрати програм, конфіденційних даних, системних файлів і інших критичних файлів. При цьому не можна з повною впевненістю назвати програму незагрозливою, якщо в її коді, не знайдено команд, що завдають шкоди системі, так як її проникнення в комп'ютер-жертву може викликати непередбачувані наслідки. За алгоритмом роботи ЗП діляться на наступні типи: з використанням стелс-алгоритмів; з самошифруванням і поліморфічністю; з використанням нестандартних прийомів; резидентні; наділення санкціонованих програм шкідливими властивостями.

Використання стелс-алгоритмів дозволяє ЗП повністю або частково приховати себе в системі. Найбільш поширеним стелс-алгоритмом є перехоплення запитів операційної системи на читання/запис заражених об'єктів. Стелс ЗП при цьому заміняють собою незаражені ділянки інформації. Резидентна ЗП при інфікуванні комп'ютера-жертви залишає в оперативній пам'яті свою резидентну частину, яка після зараження перехоплює звернення операційної системи до об'єктів зараження і впроваджується в них. Резидентні ЗП знаходяться в пам'яті і є активними до перезавантаження операційної системи або вимкнення комп'ютера.

За способом зараження ЗП діляться на кілька груп: перезаписуючі; паразитичні; «компаньйон»; інші способи зараження. Перший спосіб зараження є найбільш простим: ЗП записує свій код замість коду в файли, які заражаються, знищуючи його вміст. Як правило перезаписуючі (overwriting) - програми швидше за все виявляються, так як рано чи пізно система починає працювати не коректно або повністю втрачає працездатність. Паразитичні програми (parasitic) додають свій код в заражений файл, після чого він

залишається повністю або частково працездатним. До категорії «компаньйони» відносяться програми, що не змінюють файли, які заражаються. Алгоритм роботи полягає в тому, що для файла, що заражається створюється файл-двійник і при запуску зараженого файла управління отримує саме цей двійник. До інших способів зараження відносяться загрозливі програми, які не пов'язують свою присутність з яким-небудь виконуваним файлом. При зараженні вони копіюють свій код або файл цілком в будь-які каталоги дисків, нові копії будуть коли-небудь запущені користувачем або прописуються в автозапуск.

На основі проведених досліджень всіх типів загрозливих програм пропонується провести їх класифікацію за способами виконання загрозливих файлів. У загальному вигляді загрозливі програми слід ділити на виконувані і макро-програми, в свою чергу виконувані діляться на бінарні, мережні загрозливі програми, класичні комп'ютерні віруси, троянські програми, комп'ютерні черв'яки, хакерські утиліти, потенційно небажане програмне забезпечення, і скриптові загрозливі програми.

Запропоновано загальний підхід до захисту від загрозливих програм, заснований на контролі доступу до ресурсів по розширенням і типам файлів. Дослідження актуальності захисту від загрозливих програм і ефективності існуючих методів захисту, показало, що навіть при такому підході до оцінювання можна зробити висновок, що завдання захисту від загрозливих програм актуальне, а ефективність існуючих засобів захисту низька.

В результаті проведених досліджень виникає необхідність кількісної оцінки актуальності завдання захисту від загрозливих програм і ефективності існуючих засобів захисту. Без вирішення цього завдання неможливо оцінити реальний стан справ в даній області.

Перш за все слід розглянути наскільки завдання захисту від загрозливих програм актуальне для інформаційної системи в цілому, з урахуванням безлічі інших загроз, так чи інакше експлуатованих атаками. Для оцінки актуальності загрози в інформаційній системі, в тому числі розглядаються загрози впровадження та запуску загрозливої програми, використаємо математичну модель, засновану на представленні атаки у вигляді реалізації послідовності загроз на орієнтованому графі (рис. 1). В результаті успішної атаки буде розкрадання (крадіжка) або модифікація інформації, відмова в доступі до інформаційної системи або відмови операційної системи. На рис. 1: *З* - зловмисник; *Зі*, де *і* від 1 до *n* - реалізація загрози; *Ц* - цілі: розкрадання (крадіжка інформації), модифікація інформації, відмова в доступі.

Отримуємо наступну розрахункову формулу побудованої моделі, що дозволяє оцінити ймовірність здійснення атаки:

$$p_{0здійсн} = \prod_{i=1}^{n} (1 - p_{0i}) \quad (1)$$

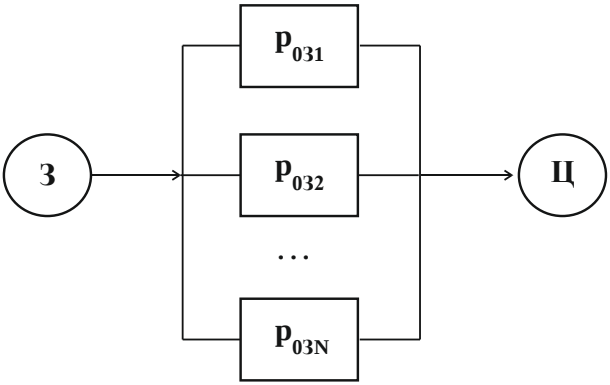

Рисунок 1 - Схема паралельного резервування

Проведено дослідження основних типів загрозливих програм, на підставі якого запропоновано класифікацію загрозливих програм за способом їх виконання. На підставі існуючої статистики зроблено висновок, що найбільш актуальними для захисту є виконувані бінарні і скриптові файли. Проведено дослідження способів впровадження загрозливих програм, в результаті якого дійшли висновку - класи загрозливих програм, що розглядаються передбачають обов'язкове збереження файлу на жорсткому диску перед виконанням (читанням). Для захисту від найбільш актуальних загрозливих програм потенційно може бути реалізований контроль доступу (розмежувальна політика доступу) до файлових об'єктів.

Література

1. Проскурин В. Г. Защита программ и данных: учебное пособие / В. Г. Проскурин, С. В. Крутов, И. В. Мацкевич. – М.: Академия, 2011. – 198 с.

2. Борисов М.А. Основы программно-аппаратной защиты информации. / М. А. Борисов, И. В. Заводцев, И.В. Чижов. – М.: УРСС: Либроком, 2013. – 370 с.

3. Михайлов А. В. Компьютерные вирусы и борьба с ними. / А.В. Михайлов. – М.: Диалог-МИФИ, 2012. – 148 с.

4. Касперский Е. В. «Компьютерное зловредство» / Е. В. Касперский. – Санкт-петербург: Питер, 2009. – 208 с.