УДК 004.056.57

Горбунова Т. В.

МОДИФІКАЦІЯ МЕТОДУ КЛАСИФІКАЦІЇ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НА ОСНОВІ ПОВЕДІНКОВОГО АНАЛІЗУ

Вінницький національний технічний університет

Анотація

Дана робота присвячена вивченню та аналізу існуючих методів класифікації шкідливого програмного забезпечення, а також модифікації методу класифікації на основі поведінкового аналізу. Новизна даного меоду полягає у вибірковосі сисемних викликів, що аналізуюься.

Ключові слова: програмне забезпечення, методи антивірусного захисту, динамічний аналіз, евристичний метод, машинне навчання, безпека інформаційних і комунікаційних систем.

Abstract

This paper is devoted to the study and analysis of existing methods for the classification of malicious software, as well as the modification of the classification method by behavioral analysis. The novelty of this method is the selectivity of the systemic calls that are analyzed.

Keywords: software, methods of antivirus protection, dynamic analysis, heuristic method, machine learning, information and communication systems security.

Вступ

На сучасному етапі динамічного розвитку й застосування інформаційних технологій виникає проблема підтримки належного рівня захищеності інформаційних середовищ від різноманітних видів атак та шкідливого програмного забезпечення. Особливо актуальним є питання виявлення та протидії найновішим, ще невідомим типам та методам зламу. вірусам, шкідливому програмному забезпеченню та іншій зловмисній діяльності.

У даній роботі розглядається розробка прототипу програми, що покликана класифікувати ПЗ, щляхом присвоєння ймовірнісного коефіцієнту належності ПЗ до множини шкідливих додатків.

Основна частина

У роботі розглянуті проблеми розпізнавання шкідливих програм, існуючі методи класифікації та знаходження шкідливого ПЗ. Поставлено задачу аналізу переваг та недоліків досліджених методів.

Було виявлено, що шкідливі програми еволюціонували від невеликих програмних блоків, вбудованих в виконувані файли інших програм, до складних самостійних багаторівневих систем, які складаються з декількох компонентів, кожна з яких має своє особливе призначення: інсталятори, завантажувачі, програми-маскувальники.

Видалення шкідливого коду з системи користувача є нетривіальним завданням. Для цього розробляються і застосовуються досить складні технології, що використовують методи приховування від антивірусів, засновані на знайдених в ОС вразливості (Rootkit технології). Застосування таких технологій робить задачу розпізнавання і видалення вірусу із системи дуже складною.

Проведений аналіз існуючих класів вірусів показав, що сучасне шкідливе ПЗ містить широкий спектр вірусів, тому необхідно розробити методи і моделі розпізнавання як старих, так і нових модифікацій ШП, які дозволяли б їх відносити до відповідному родини вірусів.

Серед існуючих методів і моделей розпізнавання шкідливих програм було обрано метод, базований на викликах API ОС, що дозволяє знаходити всі типи вірусів:

1. Віруси захищені криптуванням
2. Обфусковані віруси
3. Нащадків метаморфних вірусів

Завдяки тому, що незалежно від зміни виконуваного коду загальна семантика ПЗ залишається сталою, стає можливим застосування динамічного аналізу. А оскільки більшість викликів є загальними, що не залежать від семантики програми, виникла необхідність сформувати список

основних API функцій. Одним із основних критеріїв віднесення ПЗ до шкідливого буде частота викликів даних функцій.

Після видалення зайвих API викликів із логу, було знайдено статистичну міру шкідливого ПЗ. Застосовуючи набутий математичний апарат стало очевидно, що найкраще буде використовувати Хі-квадрат розподіл, який дав найкращу статистичну характеристику побудовіаній послідовності. У результаті було визначено, що оцінювання ПЗ відбуватиметься по двом чинникам:

1. Хі -квадрат тест для різниці основних API
2. Порівняння загального об'єму зразків.

Формула статистичної вибірки

$$x^2 = \sum_i (V_i - B_i)^2 / B_i$$

де V_i - це кількість основних API викликів ПЗ, що тестується;

B_i - це кількість цих же викликів у шаблонному файлі.

Даний метод застосовується в системах антивірусного захисту або системах попередження вторгнень.

Результати та висновки

Дана модель написана мовою програмування C++. Для її випробування були обрані реальні зразки вірусного ПЗ з порталу "virustotal.com". Для чистоти експерименту не було порведено попередніх та послідуючих обробок результату. Більшість шкідливого ПЗ може виявляти факт запуску у пісочниці, не завдаючи шкоди коректній роботі ОС. Такі зразки, котрі не виявляли цього, розпізнавалися з високою точністю: 5/7 вірусних зразків було успішно виявлено. Звісно, результати тесту є дещо синтетичними – аналіз проводився на основі семплу, котрий є схожим на них самих. Проте цей метод знаходить своє застосування в співпраці з сучасними напрацюваннями в області антивірусного захисту. Це дозволить значно збільшити ефективність модифікованого методу.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. A Tutorial on Principal Component Analysis [Електронний ресурс] // Center for Neural Science, New York University. – 2009. – Режим доступу до ресурсу: http://ic.unicamp.br/~rocha/teaching/2011s2/mc906/aulas/pca-tutorial-01.pdf.
2. Christodorescu M. Mining Specifications of Malicious Behavior [Електронний ресурс] /M. Christodorescu, S. Jha, C. Kruegel. – 2007. – Режим доступу до ресурсу: https://pdfs.semanticscholar.org/f1de/136249e1322bb95bc17611a844d207ad93a8.pdf
3. Sai S. Signature Generation and Detection of Malware Families [Електронний ресурс] / S.Sai, K. Pankaj, B. Bezawada // Centre for Security, Theory and Algorithmic Research (C-STAR) International Institute of Information Technology Hyderabad - 500032, India. – 2008. – Режим доступу до ресурсу: https://vxheaven.org/lib/pdf/Signature%20Generation%20and%20Detection%20of%20Malware%20Families.pdf
4. Новіков О. М. Безпека Інформаційно-Комунікаційних Систем / О. М. Новіков, М. В. Грайворонський. – Київ: BHV, 2009. – 608 с. – (Підручник).
5. Sun H. API Monitoring System for Defeating Worms and Exploits in MS-Windows System/ H. Sun, Y. Lin, M. Wu. – Hsinchu Taiwan: Department of Computer Science National Tsing-Hua University, 2006. – 4058 c.
6. Analysis of Computer Intrusions Using Sequences of Function Calls [Електронний ресурс]/ P.Sean, B. Matt, K. Sidney, M. Keith. – 2007. – Режим доступу до ресурсу: http://web.cs.ucdavis.edu/~peisert/research/PBKM-IEEETDSC-FunctionCalls.pdf

Тамара Валеріївна Горбунова – студентка групи УБ-14б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: tamaragorbunova97@gmail.com

Науковий керівник: ***Поплавський Анатолій Вацлавович*** - кандидат технічних наук, доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця.

Tamara Valeriivna Horbunova - student of UB-14b group, faculty of management and information security, Vinnytsia national technical university, Vinnytsia, e-mail: tamaragorbunova97@gmail.com

Supervisor: ***Poplavskii Anatolii Vatslavovich*** - candidate of technichal Sciences, associate Professor of management and security of information systems, Vinnytsia national technical University, Vinnytsia.