УДК 002.513

Л. М. Ткачук
А. В. Ніколаєнко

МЕТАМОРФІЗМ ВІРУСІВ, ПРИНЦИП ЇХ РОБОТИ ТА БОРОТЬБИ З НИМИ

Вінницький національний технічний університет;

Анотація

Досліджено будову та принцип роботи метаморфічних вірусів. Проаналізовано розповсюдження та можливі наслідки діяльності таких вірусів. Розглянуто актуальні методи боротьби.

Ключові слова: *інформація, інформаційна безпека, національна безпека, кіберпростір, віруси, метаморфізм.*

Abstract

The structure and principle of operation of metamorphic viruses have been studied. The spread and possible consequences of such viruses are analyzed. Current methods of struggle are considered.

Keywords: *information, information security, national security, cyberspace, viruses, metamorphism.*

Вступ

У наш час антивірусні програми захищають від більшості вірусного забезпечення, тому механізми маскування з кожним роком стають все більш досконалішими. Одним із найскладніших у розробці та найкращим для маскування є технологія метаморфізму. Метаморфічні віруси на сьогоднішній день найскладніші для знаходження. Це досягається завдяки їх будові. Також, чим більше копій такого вірусу було створено, тим складніше побороти його та знищити усі копії на інфікованому пристрої.

Результати дослідження

Метаморфізм – це технологія маскування, що у своїй основі тримає ідею перебудови усього тіла вірусу в кожному поколінні, при цьому не змінюючи свого функціоналу. Фактично – для кожного покоління генерується новий код. Це дозволяє кожній копії вірусу бути унікальним набором команд, що ускладнює їх пошук та створення сигнатур, по яким можна було б виявити наступні покоління даного вірусу. Метаморфічний вірус у собі має так званий метаморфний генератор, він лежить у тілі вірусу. У свою чергу цей генератор і перебудовує з кожним поколінням сам вірус. Також генератор не тільки переписує вірус, використовуючи несхожі між собою патерни ассемблерних команд, а і додає у простір між основним кодом вірусу так зване «сміття». Сміттєві команди або блоки таких команд ніяк не впливають на роботу вірусу, і в свою чергу вірус ніяк не використовує даний код – це досягається завдяки розмежуванню регістрів. Тобто вірус використовує деякий набір регістрів для роботи, в той час як усі інші регістри використовуються для роботи сміттєвих команд, при цьому сміттєві команди не змінюють прапори або повертають їх у початкові положення. Також, слід зауважити, що набір регістрів змінюється у кожному новому поколінні.

Тепер потрібно розібратися як має працювати детектор для того щоб виявити вірус. Детектору потрібно вміти розрізняти сміттєві команди та блоки таких команд, мати у собі велику базу різних патернів ассемблерного коду для виявлення вірусної логіки, слідкувати за змінами регістрів та прапорів. У свою чергу, для максимально ускладнення і збільшення роботи для детектору, метаморфний генератор має створювати код по наступним критеріям: містити ходові цілочисельні інструкції з регулярними регістрами, не використовувати інструкції збереження-відновлення контексту для відділення сміттєвого коду від істинного, набори регістрів як в сміттєвих блоках та і у інструкціях декриптора у кожному поколінні повинні бути різні, базові інструкції декриптора повинні перетворюватися у блоки інструкцій різної довжини, байт-структура мутованих інструкцій має мати максимальні варіативність[1].

Щоб написати детектор для виявлення та створення оптимальних сигнатур для пошуку вірусу, потрібно мати багато часу та ресурсів. Але є інший метод виявлення таких вірусів – їх емуляція. Дескриптор вірусу перед початком роботи повинен повернути вказівник стеку на його початкове положення. З великою долею вірогідності, коли він відновить стек після виконання коду, ми можемо припускати, що вірус виконав свою основну роботу або її частину, і наразі у пам’яті ми маємо розшифрований дискриптор вірусу, у якому містяться данні, що можна використати для створення постійної сигнатури. Також можна відслідковувати небезпечні дії або підозрілі виклики API та за

допомогою них визначати дискриптор вірусу. Тому наш детектор-емулятор має віртуально емулювати роботу вірусу та слідкувати за стеком, щоб піймати момент його відновлення до початкового значення і в цей момент отримати розшифровані дані з пам'яті на основі яких і буде створена постійна сигнатура. Таким чином ми зможемо виявляти віруси одного покоління та аналізувати віруси інших поколінь для пошуку сигнатур.

Що ж можуть зробити такі віруси? Даний тип вірусів може зробити все що завгодно, при цьому не будучи знайденим. Але таких вірусів на даний час дуже мало. Це пов'язано з тим, що не кожен ентузіаст, звичайний програміст, крекер та навіть спеціаліст з кібербезпеки може написати даний тип вірусів, а ті люди які можуть це зробити і мають потрібний багаж знань зазвичай займаються більш прибутковими справами, таких спеціалістів дуже цінять у IT сфері. Написання метаморфічного генератора – досить кропіткий, складний та довгий процес.

Висновок

Метаморфічні віруси дуже складні в будові та у виявленні. Для їх ефективного пошуку та знешкодження потрібно багато ресурсів та часу. Цей процес можна назвати битвою розумів, як і написання будь якого вірусу або детектору.

Недолік метаморфізму в його складності, але це одночасно і його перевага. Через цей недолік на сьогоднішній день таких вірусів дуже мало і усі вони безпрецедентно є унікальними витворами мистецтва.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Прилуцкий С. Вирусы. Вирусы? Вирусы! Часть 2 [Електронний ресурс] / Сергей Прилуцкий. – 2014. – Режим доступу до ресурсу: https://habr.com/ru/company/mailru/blog/240655/.

2. Збицкий П. В. МОДЕЛЬ МЕТАМОРФНОГО ПРЕОБРАЗОВАНИЯ ИСПОЛНЯЕМОГО КОДА / П. В. Збицкий. // Серия «Компьютерные технологии, управление, радиоэлектроника». – 2009. – С. 57–61.

3. Клементьев К. Е. Компьютерные вирусы и антивирусы: взгляд программиста / К. Е. Клементьев. – Москва, 2013. – 656 с. – (ДМК Пресс).

4. Что такое метаморфный вирус? [Електронний ресурс] – Режим доступу до ресурсу: https://www.kaspersky.ru/resource-center/definitions/metamorphic-virus.

Ткачук Людмила Миколаївна – доцент кафедри менеджменту та безпеки інформаційних систем, кандидат економічних наук, заступник декана з навчально-методичної роботи Факультету менеджменту та інформаційної безпеки ВНТУ, e-mail: ludatkachuk2017@gmail.com.

Ніколаєнко Андрій Володимирович — студент групи КІТС-18б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: andrey.nikolaienko.0@gmail.com

Tkachuk Lyudmyla Mykolayivna – associate professor of Department of Management and Security of Information Systems, candidate in economics, deputy dean for educational and methodological work of the Faculty of Management and Information Security of VNTU, e-mail: ludatkachuk2017@gmail.com.

Nikolaienko Andrii V. - department of Management and Information Security, Vinnitsa National Technical University, Vinnytsia**, e-mail:** andrey.nikolaienko.0@gmail.com