Міністерство освіти і науки України
Кам'янець-Подільський національний університет імені Івана
Огієнка Фізико-математичний факультет
Кафедра комп'ютерних наук

Кваліфікаційна робота магістра

з теми: **«Дослідження адаптивного методу приховування даних для забезпечення кібернетичного протиборства в інфокомунікаційних мережах профільних структур»**

Виконав: здобувач вищої освіти групи KN1-M24

спеціальності 122 Комп'ютерні науки
Потапчук Артур Сергійович

Керівник: Бараннік Володимир Вікторович, доктор технічних наук, професор

Рецензент: Оптасюк Сергій Васильович, завідувач кафедри фізики, кандидат фіз-мат наук, доцент

м. Кам'янець-Подільський – 2025р.

ЗМІСТ

Вступ

Розділ 1. АНАЛІЗ МЕТОДІВ ПОШИРЕННЯ КІБЕРНЕТИЧНИХ ВІРУСНИХ АТАК В ІНФОРМАЦІЙНО-МЕРЕЖНОМУ ПРОСТОРІ ПРОФІЛЬНИХ СТРУКТУР……6

1.1. Аналіз та класифікація вірусних потоків телекомунікаційних мережах профільного призначення…….....8

1.2. Дослідження підходів поширення вірусних потоків в інформаційно-мережному просторі профільних структур……..15

Висновок за розділом 1……17

Розділ 2. ОЦІНКА СУЧАСНИХ ПІДХОДІВ ДО ПРОТИДІЇ ВІРУСНИМ АТАКАМ В ІНФОРМАЦІЙНО-МЕРЕЖЕВОМУ ПРОСТОРІ ПРОФІЛЬНИХ СТРУКТУР……18

2.1. Оцінка сучасних методів маскування вірусних потоків в інформаційній мережі профільних структур…….....21

2.2. Дослідження підходів для захисту автоматизованого робочого місця від вірусного ураження в інформаційно-мережевому просторі……25

2.3. Оцінка ефективності функціонування антивірусних заходів у мережах профільних структур……...31

2.4. Дослідження недоліків антивірусних заходів з врахуванням досвіду протидії для профільних структур……...34

Висновок до розділу 2……...35

Розділ 3. РОЗРОБКА АДАПТИВНОГО МЕТОДУ ПРОТИДІЇ ПРИХОВАНИМ ВІРУСНИМ АТАКАМ В ІНФОРМАЦІЙНО-МЕРЕЖЕВОМУ ПРОСТОРІ ПРОФІЛЬНИХ СТРУКТУР

3.1. Створення адаптивного методу маскування даних з врахуванням особливостей виконання завдань в інтересах профільних стру-

ктур……...35
3.2. Розробка комбінованого методу маскування вірусних атак в інформаційно-мережевому просторі профільних структур…….44
3.3 Розробка адаптивного методу забезпечення кібернетичного захисту в інформаційно-мережевому просторі профільних структур…….46
Висновки до розділу 3……..50
Висновки……50
ПЕРЕЛІК ПОСИЛАНЬ……51

АНОТАЦІЯ

Пояснювальна записка містить 52 сторінки, 7 рисунків, 2 додатки, 24 літературних джерел

Наукове завдання – підвищення ефективності систем забезпечення кібернетичного протиборства в інфокомунікаційних мережах профільних структур.

Мета роботи – розробка адаптивного методу виявлення та приховування даних в системах забезпечення кібернетичного протиборства в інфокомунікаційних мережах профільних структур на основі виявлення прихованих вірусних атак

Об'єкт дослідження – процеси забезпечення кібернетичної протидії на основі виявлення прихованих вірусних атак в інформаційно-мережному просторі профільних структур

Предмет дослідження – методи виявлення та приховування інформації в системах кібернетичної протидії з врахуванням технологій маскування вірусного коду.

Методи дослідження – методи маскування, методи цифрової стеганографії, методи криптографічного шифрування даних, методи впровадження повідомлень до цифрових контейнерів аналогової природи, методи протидії вірусним атакам, методи аналізу двійкових потоків даних.

Для надання відомостей про підвищення безпеки в інформаційно-мережному просторі використовуються програмне забезпечення що є у телекомунікаційному обладнані, серверне обладнання, стійкі шифрування. Завдяки досвіду інформаційних операцій досягається можливість підвищення захисту інформаційних систем та ресурсів інформації. Захист інформації створює умови для приховування спеціальної інформації. Використовується технологія виявлення прихованих вірусних атак. Розробляється адаптивний ме-

тод виявлення прихованих вірусів на основі апарату стеганографічного аналізу та вбудовування даних. Підвищується ефективність протидії вірусним атакам в інформаційно-мережному просторі профільних структур.

Розглянуті способи адаптивного захисту в інформаційно-мережному просторі, на основі реалізації програмного модуля в алгоритм стиснення відеоданих, з використанням шифрування та модифікації заміною останніх двох бітів інформації. Пропонується використовувати розроблений алгоритм для адаптивного захисту інформації в інформаційно-мережному просторі профільних структур.

Ключові слова: КІБЕРНЕТИЧНЕ ПРОТИБОРСТВО, АНТИВІРУСНІЙ ЗАХИСТ, МЕРЕЖНЕ ОБЛАДНАННЯ, ПРИХОВУВАННЯ ДАНИХ, КІБЕРНЕТИЧНІ АТАКИ, ВІРУСНІ ПРОГРАМИ

ВСТУП

Організація кібернетичної безпеки інфокомунікаційного простору від кібер-загроз та вірусних атак, пов'язаних зі шкідливими інформаційно-технічними впливами є надзвичайно значимим завданням в умовах збройної агресії РФ проти України. Важливим є організація захисту суспільства від негативного кібернетичного впливу з боку протиборчої сторони. Та, навпаки потреба в організації проведення захисник кібернетичних атак на інфраструктуру протиборчої сторони.

Аналіз останніх подій свідчить про широке застосування РФ комплексних атак з використанням збройних ударів та кібер-інформаційних впливів. Це руйнує критичну інфраструктуру держави, впливає на дестабілізацію обстановки у суспільстві. Оказує ймовірний негативний вплив на особовий склад безпілотних систем, руйнує мережі передачі даних у Збройних Сил України, пошкоджує інформаційні системи, втрачаються якісні характеристики щодо процесів обробки та передачі інформації.

Можливість доступу до важливих видів інформації, в тому числі з порушенням умов конфіденційного захисту зумовлює необхідність аналізу, прогнозування та протидії кібернетичним та вірусним атакам. Це зумовлює необхідність використання фільтрів шкідливих впливів із забезпеченням інформаційної безпеки держави, суспільства, особистості.

Важливо враховувати потребу у захисту змісту інформаційних потоків. Особливо це стосується інформації, яка передається по інформаційним мережам, та має вагомий внесок для здійснення інформаційного протиборства та впливу на важливу інфраструктуру, особовий склад, підрозділи профільних структур.

З метою підвищення захисту та кібербезпеки інфо-мережного простору від зовнішніх кібернетичних та вірусних атак, що здійснюються на підрозділи профільних структур та населення, для організації захисних кібернетич-

них атак необхідно розробити метод протидії вірусним атакам в інфо-мережному простору профільних структур.

Аналіз результатів розроблених методів здійснюється шляхом використання створених програмних модулів. Це є варіантом для побудови системи адаптивної протидії вірусним атакам в інформаційно-мережній компоненти профільних структур.

1 АНАЛІЗ МЕТОДІВ ПОШИРЕННЯ КІБЕРНЕТИЧНИХ ВІРУСНИХ АТАК В ІНФОРМАЦІЙНО-МЕРЕЖНОМУ ПРОСТОРІ ПРОФІЛЬНИХ СТРУКТУР

1.1 Аналіз та класифікація вірусних потоків телекомунікаційних мережах профільного призначення

Сучасні комп'ютерні вірусу або КП-віруси являють собою цифрові вірусні цифрові потоки. В тому числі це бітові потоки з властивістю комп'ютерних кодів (програма), що мають потенціал до прихованого само поширення або компонентного підключення інших модулів. Цифрові вірусні потоки (КП-віруси) можуть одночасно поширюватись, підключати інші модулі. При цьому може бути створено різні втрати та пошкодження. До них відносяться:

- властивість знищувати інформаційні бази даних;
- властивість нанесення пошкоджень якісному змісту інформації;
- властивість створення умов для викрадання та несанкціонованого доступу до секторів інформаційних баз даних;
- блокувати або зменшувати продуктивність щодо працездатності інформаційних систем, серверних комплексів, сховищ даних;
- блокувати або унеможливлювати передачу даних в інформаційно-мережному просторі.

На теперішній час відомими є порядку 10^4 цифрових (КП-вірусних) реалізацій. Вони є цифровими та зачасти мають макро-структуру або комплексну модульну топологію та будуються за комбінацією вірусного пакету.

Найбільш поширеним методом їх розповсюдження (масштабування у просторі) є телекомунікаційні мережі, Інтернет-простір, супутникові мережі.

Розробники цифрових вірусних модулів (програм, файлів) зачасти застосовують:

1) протоколи зберігання та обміну для соціо-технічних просторів;

2) наявні відомості щодо вразливостей різних рівнів багатоярусного програмного забезпечення в масштабі: кінцевого обладнання систем окремих користувачів (комп'ютер, смартфон); локальних мереж користувачів; сховищ даних.

Потрібно сказати, що рівень шкоди від дії таких комплексних вірусних модулів та КП-вірусів залежіть від рівня користувачів, рівня виконання завдань та рівня впливу завдань на забезпечення національної безпеки держави, соціуму та особистості. Найбільш потужні шкоди та втрати відбуваються у разі прояву вірусних атак в системах профільних структур. Особливо це стосується сучасного періоду – збройної агресії РФ проти України.

Варіант класифікації вірусів можна навести на рисунку 1.1. Потрібно сказати, що подалі вірусні модулі стають більш комплексними та набирають ознаку прихованості. Відповідно шкода від дії таких вірусних атак значно збільшується.

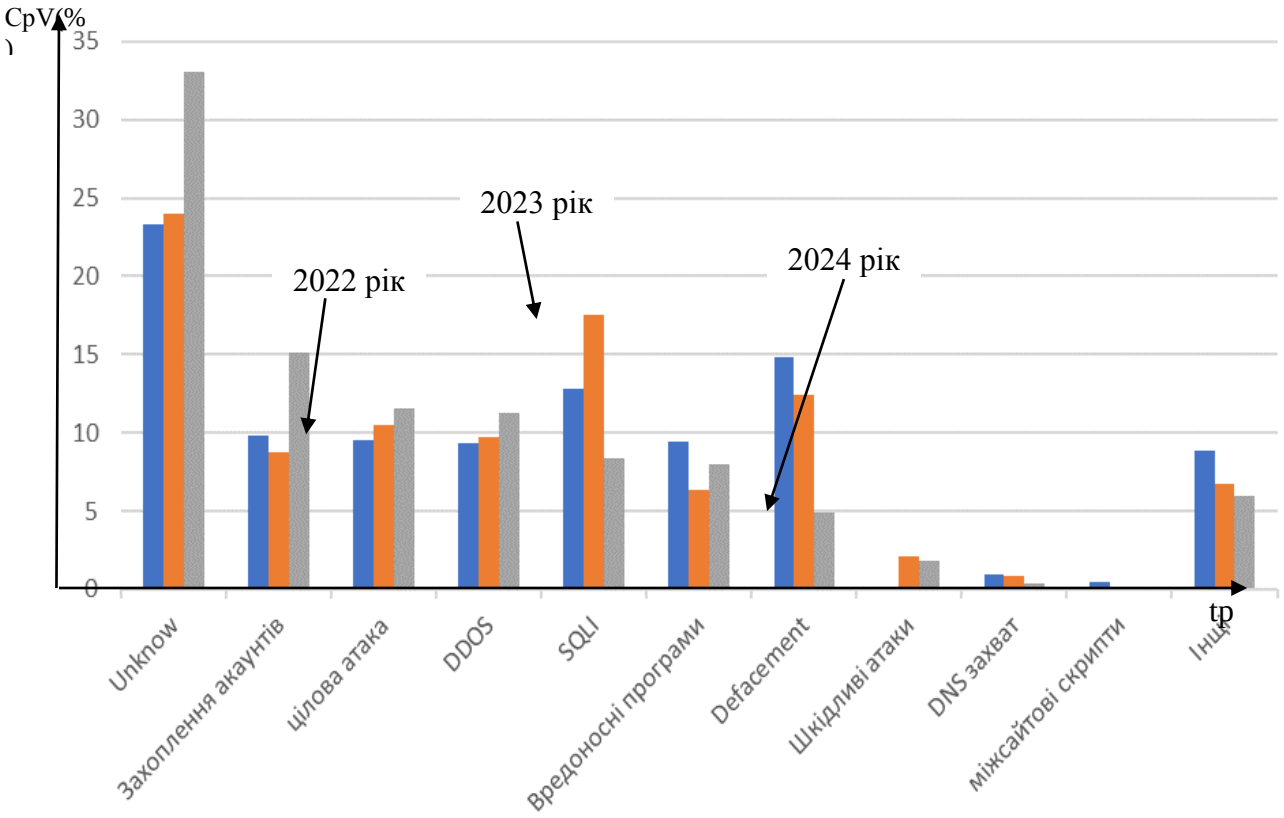


Рисунок 1.1 - Діаграма типів кібернетичних вірусних атак з кількістю їх використання за роками

Віруси-невидимки - це файлові цифрові вірусні модулі, з обмеженою можливістю свого знаходження з боку програм-антивірусів. Таке можливо в тому числі шляхом модифікації або фальсифікують перевірочних синдромів під час скан-перевірки.

Квазівірусні, або «троянські» цифрові програми-модулі. До них слід віднести віруси, які не здатні до «розмноження». Троянська програма маскується під корисну або цікаву програму, виконуючи під час свого функціонування ще й руйнівну роботу (наприклад, стирає file allocation table(FAT)-таблицю) або збирає на комп'ютері яка не підлягає розголошенню інформацію. На відміну від вірусів троянські програми не мають властивість самовідтворення.

Вірусні платформи або «черв'яки». Тут слід вказати, що вони є найпоширенішими для інфо-мереж та віртуальних комп'ютерних просторів. На відміну деяких типів вони володіють властивістю до швидкого «розмноження» - масштабування по мережі. Можуть формуватися різні типові копії таких вірусів. Наприклад, під час копіювального розповсюдження виникають файли з іменами «install.exe».

Цифрові бомби або закладки за логікою переходу. Це такі програмні пакети, що мають властивість своєї активації (запуску) за певних часових; інформаційних; комплексних; логічних умовах. Реалізації таких типів вірусних атак проходить з нанесенням шкоди шляхом несанкціонованого доступу до інформаційних баз, спотворення або знищення даних, в тому числі з накладенням крипто-гами. Крипто-гама може також використовуватись під час форматування сховищ даних та дисків для зберігання інформації. Це призводить до знищення даних або до обмеження доступу до неї.

Companion-вірусні модулі. Реалізація атаки таких типів вірусів можлива через формування для executable(EXE) - файлів нових файлів-супутників (дублікатів). Такі файли матимуть те ж саме ім'я. Однак з розширенням component object model (COM). Наприклад, для файлу XCOPY.EXE створюється файл XCOPY.COM. Вірус записуємо в COM - файл і ніяк не змінює однойменний EXE - файл. При запуску такого файлу disk operating system (DOS) першим виявить і виконає COM - файл, тобто вірус, який потім запустить і EXE - файл.

Паразитичні віруси при розповсюдженні своїх копій обов'язково змінюють вміст дискових секторів або файлів. У цю групу можна адресувати віруси, які не є «хробаками» або «компаньйонами».

Вірусні модульні програми – черв'яки (worm). Характерним для них є поширення в інфомережному просторі з властивостями схожості на типи компаньйон-вірусів. Так само не змінюють файли або сектори на дисках. Відмінним таких типів вірусів є проникнення в системи зберігання даних, наприклад кінцевого обладнання (комп'ютер, смартфон). Таке проникнення реалізується через телекомунікаційну мережу. Далі дія вірусу проходить шляхом обчислення мережних адрес інших комп'ютерів, наприклад користу-

вачів в локальній мережі. Потім проходить розсилка за цими адресами своєї копії. Зрозумілим наслідком таких вірусних атак є зменшення пропускної здатності телекомунікаційного простору. Втрачається рівень доступності до даних інформаційних серверів та сховищ даних.

Реплікатори. Такі типи вірусів можуть розмножуватися без впровадження в інші програми і мати «начинку» з комп'ютерних вірусів.

Окремо слід відмітити віруси з властивістю невидимки. Або так звані Stealth-віруси. Тут застосовується пакет цифрових засобів для здійснення маскування вірусної наявності або присутності вірусів в цифровому просторі, просторі інформаційної мережі. Характерним тут є властивість обмеженості виявлення таких вірусів, тобто обмеженості локації (фільтрації) наявності таких вірусів під час сканування інформаційного середовища. В тому числі це забезпечується шляхом перехоплення звернень скан-процесу операційної системи до уражених файлів або секторів дисків. Після чого проходить «підставляння» незаражені ділянки файлів для скан-перевірки.

Віруси, які шифрують власне тіло різними способами, називаються поліморфними. Поліморфні віруси (або віруси - примари, віруси - мутанти, Полиморфик) досить важко виявити, тому що їх копії практично не містять повністю збігаються ділянок коду. Це досягається тим, що в програми вірусів додаються порожні команди (сміття), які не змінюють алгоритм роботи вірусу, але ускладнюють їх виявлення.

Типи вирусів - макро-віруси. Вони використовують можливості макромов. Такі модулі вбудовані або впроваджені до засобів обробки даних. Наприклад, текстові редактори (редактор Word) та електронні таблиці (середа Excel).

Цифрові віруси або віруси в цифровому просторі мереж зберігання даних або систем передачі даних можуть мати топологію:

1) монолітного вірусного цифрового модуля, що являє собою єдиний цифровий кодовий-блок;

2) розподіленого вірусного за декількома модулями в мережному просторі. Такі компоненти (частини) можуть містити програмні інструкції або адреси-переходу до знаходження інших частин спрут-вірусу. Зачасти програмні інструкції (команди) надають обчислювальній системі певний набір команд для збирання монолітного вірусу. Після чого проходить його активація (запуск). Вірус в цьому випадку ніби відтворюється. Такий тип вірусних атак має властивість прихованості, у просторі системи зберігання даних та за часом щодо функціонування інформаційної системи. Лише на обмежений час – час активації такий вірус компонується до монолітного стану, що дозволяє його реалізацію, тобто реалізацію відповідної вірусної або кібернетичної атаки.

За ступенем впливу віруси можна класифікувати, як:

- безпечні віруси - також займають частину ресурсів комп'ютера, але про

їхню присутність користувач знає добре. Зазвичай вони проявляються у вигляді візуальних і звукових ефектів і не шкодять даними користувача.

- нешкідливі віруси - мають незначний вплив на роботу ПК, займаючи частину системних ресурсів. Нерідко користувачі навіть не підозрюють про їх присутність;

- небезпечні віруси - програми, які порушують нормальну роботу користувальницьких додатків або всієї системи;

- дуже небезпечні віруси - програми, завдання яких полягає у знищенні файлів, виведення з ладу програм і операційна система (ОС) або розсекречення конфіденційних даних;

За способом зараження середовища перебування віруси діляться на:

- резидентні віруси - являють собою програми, присутні в оперативній пам'яті, або зберігають там свою активну частину, які потім перехоплюють звернення неінфікованих програм до операційної системи, і впроваджуються в них, постійно заражаючи ті чи інші об'єкти операційної системи. Свої деструктивні дії і зараження інших файлів, резидентні віруси можуть виконувати багаторазово;

- не резидентні віруси не заражають оперативну пам'ять комп'ютера і проявляють свою активність одноразово при запуску інфікованої програми;

Значно небезпечніше наслідки дії вірусу, який знищує частину файлів на диску.

Як нескладно здогадатися, найбільшу небезпеку становлять резидентні віруси, так як час їх активної роботи обмежується тільки вимиканням або перезавантаженням всієї системи, а не окремого додатка.

За середовищі перебування віруси поділяються на: мережеві, файлові, завантажувальні, системні, файлово-завантажувальні.

Мережеві віруси в якості середовища проживання використовують глобальну або локальні комп'ютерні мережі. Вони не зберігають свій код на жорсткому диску комп'ютера, а проникають безпосередньо в оперативну пам'ять ПК. Віруси цього типу за здатність обчислювати мережеві адреси інших машин, перебуваючи в пам'яті комп'ютера, і самостійно розсилати за цими адресами свої копії називають мережними хробаками. Такий вірус може знаходитися одночасно в пам'яті кількох комп'ютерів. Мережеві віруси виявити складніше, ніж файлові. Мережеві віруси поширюються з великою швидкістю і можуть сильно уповільнити роботу апаратного забезпечення комп'ютерної мережі.

Файлові віруси - це програми, які вражають виконувані файли операційної системи і користувальницьких додатків. Найчастіше вони впроваджуються в файли з розширеннями com, exe, bat, sys, dll. Такі віруси виявити і знешкодити найпростіше. Радує також, що проявити свою шкідливу активність вони можуть тільки після запуску зараженої програми.

Навколишнє середовище завантажувальних вірусів - спеціальні області жорстких і гнучких дисків, які служать для завантаження операційної системи. Завантажувальні віруси впроваджуються в завантажувальний сектор дис-

ка (Boot - сектор) або в сектор, що містить програму завантаження системного диска (Master Boot Record (MBR)). Деякі віруси записують своє тіло в вільні сектора диска, позначаючи їх в FAT - таблиці як «погані» (Bad cluster). Завантажувальний вірус підміняє оригінальний запис і перехоплює управління системою. Такі віруси виявити і видалити найскладніше, оскільки вони починають свою роботу ще до завантаження антивірусних програм. Вони ж становлять найбільшу небезпеку.

Файлово-завантажувальні віруси вражають завантажувальні сектори дисків і файли прикладних програм.

Системні віруси проникають в системні модулі і драйвери периферійних пристроїв, файлів і таблиці розділів.

Тип вірусів - мережевий черв'як. Характерним для таких типів є їх використання в інформаційно-мережевих просторах. Зачасти таки типи вірусів володіють:

1) можливостями проникнення до локальних мереж, подалання в автономному режимі систем захисту автоматизованих інформаційних систем (АСУ);

2) можливостями створення і масштабування з поширенням своїх копій;

3) можливістю змінювати характер нанесення шкоди для створених копій відносно базового прототипу.

Так само як для вірусів, життєвий цикл хробаків можна розділити на певні етапи або реліз-стадії:

- перша реліз-стадія, це етап проникнення в систему або мережевий простір;

- друга реліз-стадія, це базовий етап активація вірусу;

- третя реліз-стадія, це етап пошук вразливостей та знаходження цільових секторів шкідливої дії;

- четверта реліз-стадія, це етап підготовки копій;

- п’ята реліз-стадія, це етап масштабування вірусної атаки шляхом поширення відповідних вірусних копій.

Можливо вказати на попередню реліз-стадію, яка пов’язана зі зборкою монолітного вірусу у разі режиму розподіленого його зберігання.

Під час проходження реліз-стадії на проникнення до інформаційно-мережевого простору або подалання системи захисту вірус-черви діляться переважно за типами використовуваних протоколів:

- мережеві вірус-черві. Це віруси, що поширюються завдяки телекомунікаційним протоколам. Тут може використовуватись набір порушення під час обробки з використанням протоколів tcp / ip на певних рівнях відкритої моделі OSI;

- поштові вірус-черв'яки. Віруси, що мають своє розповсюдження шляхом масштабування у цифрових форматах зберігання даних електронної пошти;

- IRIC-черв'яки. Віруси, які масштабуються шляхом поширення в телекомунікаційних мережах;

- peer-to-peer (P_2P)-черв'яки. Віруси, яка мають напрямок масшатабування завдяки піринговвих інформаційно-мережевих технологій обміну даними;

- instant Messenger-черв'яки. Віруси, які застосвують свою передачу через канали миттєвого обміну інформацією;

Троян. Такий вірус володіє властивістю часової прихованості та подалання систем захисту локальних мереж. Подалі проходить зараження компонент такої мережі. У загальному випадку, троян-вірус проникає до мережі разом з хробаком в автономному режимі.

В силу відсутності у троянів функцій розмноження і поширення, їх життєвий цикл вкрай короткий - всього три реліз-стадії:

Перша реліз-стадія, це подалання захисних фільтрів мережі.

Друга реліз-стадія, це етап запуску або активації програми-вірусу.

Третя реліз-стадія, це проведення етапу щодо реалізації шкідливих цільових вірусних функцій.

При цьому враховувати властивість троян-вірусу до тривалої непомітності. Такий тип вірусів може зберігатися у пам'яті комп'ютера за умов властивості маскувати свою присутність.

Хробаки і віруси можуть здійснювати всі ті ж дії, що і трояни. На рівні реалізації це можуть бути як окремі троянські компоненти, так і вбудовані функції. Крім цього, за рахунок масовості, для вірусів і черв'яків характерні також інші форми шкідливих дій:

- перевантаження каналів зв'язку.
- distribute denial of service (DDoS) атаки.
- втрата даних.
- порушення роботи.
- завантаження ресурсів комп'ютера.

Наявність деструктивних дій зовсім не є обов'язковим критерієм для класифікації програмного коду як вірусного. Слід також зазначити, що одним тільки процесом саморозмноження вірус здатний завдати колосальної шкоди.

Проаналізувавши звіти у компаніях Kaspersky, AVAST, AVG, NOD32 зробив статистику використання кібернетичних атак (вірусів) за період 2022-2024 який продемонстровано на рисунку 1.1, де «а» - це відношення кількості всіх запитів з кількістю відомим типом загрози запитів.

А також графік кількості кібернетичних атак з 2022-2024 років по місячно продемонстровано на рисунку 1.2, де $kil(10^3)$ – кількість вірусних атак,t -місяць.

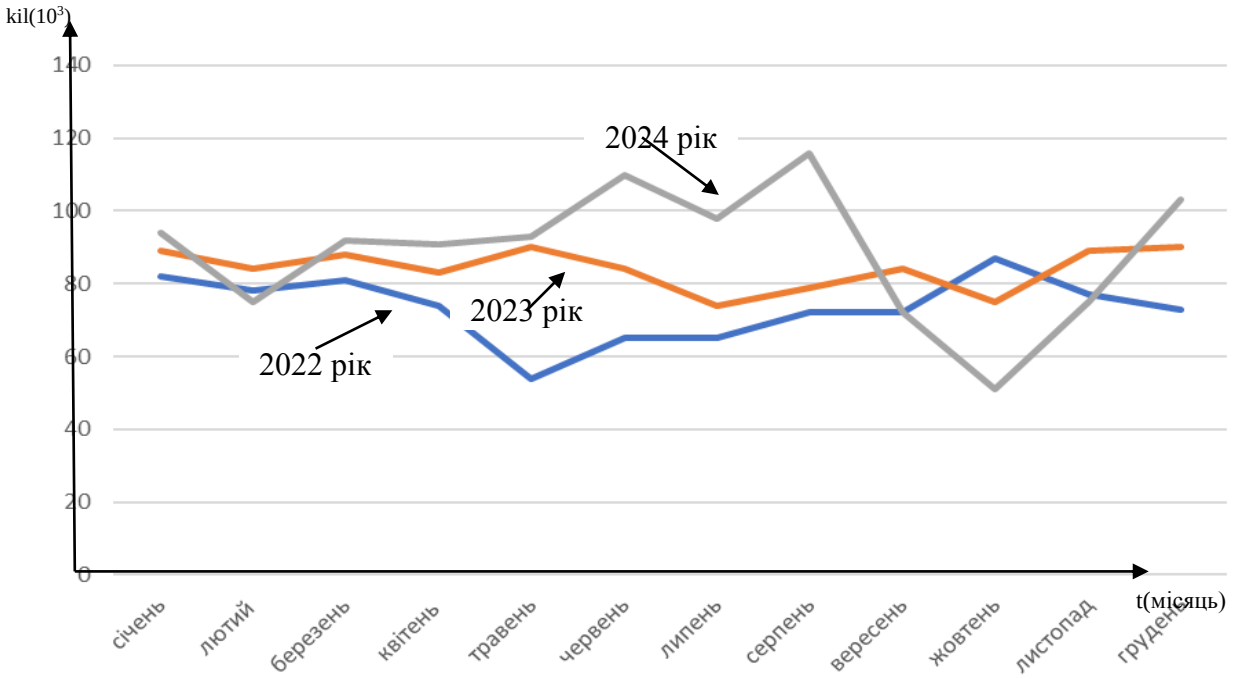


Рисунок 1.2 – Графік кібернетичних атак

1.2 Дослідження підходів поширення вірусних потоків в інформаційно-мережному просторі профільних структур

В даний час епідемії комп'ютерних вірусів та інших шкідливих програм завдають величезної шкоди різним організаціям і окремим користувачам комп'ютерів. За останні 10-15 років поширення шкідливого коду, що носило локальний характер, перетворилося на глобальні епідемії мережевих черв'яків, які не потребують для поширення участі користувач. Робота і функціонування багатьох структур і організацій тісно пов'язана або повністю залежить від глобальних мереж. Мережеві черв'яки, розмножуються в необмеженій кількості, забивають канали передачі інформації, тим самим завдаючи величезних збитків, не кажучи вже про те, що код хробака може містити деструктивні функції, що може призвести до втрати або витоку важливої та конфіденційної інформації. Сучасна шкідлива програма може інфікувати більшу частину вразливих комп'ютерів всього за кілька годин, завдяки масштабам глобальної мережі Інтернет і величезним пропускним здібностям сучасних каналів передачі інформації. Багато дослідників епідемій комп'ютерних вірусів відзначають, що сучасні шкідливі пр грами використовують далеко не самі оптимальні стратегії пошуку нових комп'ютерів для зараження. В майбутньому можлива поява шкідливого коду, здатного поширюватися за лічені секунди, завдяки використанню вдосконалених стратегій поширення. Моделювання епідемій шкідливих програм показує, що більшу частину часу,

за який частка інфікованих комп'ютерів досягає свого максимального значення, шкідлива програма витрачає на зараження невеликого, в масштабах епідемії, числа комп'ютерів. Таким чином, в майбутньому можливий прискорений розвиток епідемій шкідливих програм завдяки попередньому аналізу стану мережі передачі даних, тобто складання списку вразливих комп'ютерів, який буде використовуватися для того щоб захопити деякий "критичне" число вразливих комп'ютерів. Якщо це «критичне» число комп'ютерів буде захоплено, подальше поширення відбуватиметься лавиноподібно. Нові уразливості в різних програмах знаходять практично кожен день, виробники програмного забезпечення не завжди оперативно їх усувають, а готові латки встановлюються дуже повільно. Деякі користувачі і технічний персонал мереж ніяк не дбають про безпеку власних комп'ютерів. Певну роль в поширенні вірусів відіграє і людський фактор: Три недосвідчені користувачі, не замислюючись, відкривають всі поштові вкладення, через які поширюються багато шкідливих програм. Таким чином, в даний час існують безліч факторів, сприяють появі масових епідемій шкідливих програм. До того ж, сучасні мережеві черв'яки, згідно з багатьма роботами в області комп'ютерної безпеки, використовують далеко не весь свій потенціал; можлива поява шкідливого коду поширюється за лічені хвилини. Завдання протидії поширенню шкідливих програм вкрай актуальний. Всі організації, робота яких так чи інакше, пов'язана з використанням мереж передачі даних, зазнають збитків від постійних спалахів епідемій мережевих черв'яків, нові модифікації яких з'являються щодня. Протидія поширенню і створенню шкідливих програм-дуже складне завдання, яке має безліч аспектів, одним з яких є моделювання та методи передбачення поширення шкідливих програм. За допомогою математичних моделей можна оцінити масштаби можливої епідемії, вивчити динаміку зміни числа заражених комп'ютерів і так далі.

Моделювання також може бути використано для того щоб оцінити ефективність тих чи інших заходів протидії поширенню, наприклад лікування вже заражених комп'ютерів або попередньому усуненні вразливостей в ПЗ, використовуваних шкідливим кодом для інфікування. Таким чином, епідеміологічні моделі є необхідним інструментом для вивчення та протидії поширенню вірусних атак.

Найпростішим підходом є використання класичних епідеміологічних моделей, розроблених ще в XIX столітті для вивчення епідемій інфекційних захворювань і заснованих на системах диференціальних рівнянь. Однак ці моделі досить примітивні і не враховують деяких особливостей поширення комп'ютерних вірусів . Характер епідемії, передбачених за допомогою традиційних моделей досить часто не збігається зі статистичними даними, тому актуальна задача створення нових, більш відповідних математична модель. Крім класичних моделей, існують моделі поширення епідемій, спеціально розроблені для вивчення комп'ютерних шкідливих програм. Багато з них базується на змінених системах диференціальних рівнянь, сформульованих у класичних епідеміологічних моделях. Більшість моделей не вносить істотних

змін в традиційні моделі, а деякі з них призначені тільки для конкретних видів шкідливих програм.

Проаналізувавши методи поширення вірусів у системах телекомунікаційного обладнання та інформаційної мережі світу, сформувалася класифікація способів поширення вірусів у спеціальних телекомунікаційних системах.

Сервіси електронної пошти. В цьому разі вірусу мають можливість мАскуватися або приховуватися у електронних даних, в тому числі текстові файли, текстові повідомлення, аудіо-файли, відеоданні. Однак треба пам'ятати, що в електронних ресурсах само тело вірусу може бути відсутнім. Навпаки, може міститься посилання на адрес, де знаходиться головний модуль програми-вірус. Наприклад, за таким посиланням буде проведено перехід на спеціальну сторінку веб-сайту. Саме за місцем знаходження вірусної програми. Багато вірусів через електронні ресурси використовують адресну книгу з поштових клієнтів типу Outlook. Після проводиться етап розповсюдження самого вірусу.

Електронний ресурс веб сторінки. Здійснення вірусного ураження можливо проводиться завдяки ресурсів Інтернет-мережі. Наприклад з використанням: скриптів та ActiveX-компонент. Тоді застосовуються множина вразливостей програмно-системних компонент.

Спеціалізовані мережі, Інтернет-ресурси та ресурси локальних інформаційно-мережевих компонент. Такі типи вірусів можуть потрапляти та проникати до інформаційних систем, до АСУ спеціального призначення. Вірусні модулі використовують вразливості у системі захисту на доступність або «дірки» у системі забезпечення конфіденційності, системи аутентифікації та ідентифікації користувачів та/або авторизованих процесів. Також можуть застосовуватись закладки, вразливості в операційних системах. З такої точки зору вразливість, як поняття можна класифікувати помилкою або неякісною розробкою програмному продукті. Саме такі вразливості зачасти дозволяють дистанційно завантажити та активувати програмний код. Після чого вірус-програма отримує доступ до операційної програмної системи. Також може проводиться активація процесу ураження та нанесення шкідливих дій через опосредовані компоненти інформаційно-мережевих систем. Зловмисники виможуть таких застосовувати заражені комп'ютери користувачів для розсилки спаму та організації DDoS-атак.

Висновок за розділом 1

Віруси є великою проблемою для військових мереж в спеціальних телекомунікаційних системах в умовах інформаційної війни тим що віруси е адаптивними, а також гнучкими за для більш ефективного маскування. Віруси по переду від антивірусних програм на пару кроків. Як ми бачили раніше продемонстрованих графіках, кібернетичних атак стає все більше. Все більше людей користуються не ліцензійною продукцією, тим самим більшість випадків кібернетичного злочину саме із за провини людей.

2. ОЦІНКА СУЧАСНИХ ПІДХОДІВ ДО ПРОТИДІЇ ВІРУСНИМ АТАКАМ В ІНФОРМАЦІЙНО-МЕРЕЖЕВОМУ ПРОСТОРІ ПРОФІЛЬНИХ СТРУКТУР

Протидія вірусним атакам в профільних структурах організується шляхом використання комплексних засобів. В тому числі з задією антивірусних програмних заходів. Базовими функціями таких заходів є: детектування з діагностуванням типового класу вірусу; блокування або ліквідування вірусів; усунення вразливостей. Однак слід вказати, що не існує універсальних антивірусних заходів з гарантованою ефективністю протидії. Це зумовлено також тим, що вірусні операційні дії постійно удосконалюються. При цьому зрозуміло, що враховуються особливості нових антивірусних заходів з виявленням їх слабких вразливих місць. Отже формується система протидії «вірус – атака – антівірус – захист». При цьома така система зачасту находиться в дисбалансу в напрямку збільшення ефективності вірусних атака. Тут потрібно сказати, що неможливість існування абсолютного антивірусу була доведена математично на основі теорії кінцевих автоматів, автор доказу - Фред Коэн.

В загальному випадку ефективність антивірусних заходів оцінюється за набором показників. Тут визначаються такі:

1. Надійність, простота та зручність функціонування та інтерфейсу користувача. Важливим є забезпечення усунення набору технічних складнощів. В іншому випадку це потребує спеціальних знань та додаткової підготовки користувача. Даний показник є основним. Це пояснюється тим, що ефективність антивірусних функцій буде унеможливлена у разі виникнення затримок або припннення сканування інформаційного простору, тобто у разі незапланованої зупинки процесу скан-пошуку вірусів. У разі складного інтерфейсу з користувачем може виникнути ситуація, коли буде проігноровано вадливі опції для виявлення вірусних потоків.

2. Часові затримки для функціонування антівірусних заходів. Наприклад, у разі використання надто складних математичних перетворень для

сканування та виявдення вірусних компонент. Наприклад, це може деструктивно впливати на загальний процес обробки інформації в інтересах профільних структур.

3. Показник типованості виявлення вірусів. Це впливає на якість детектування вірусів різних найбільш розповсюджених типів або таких типів, що мають найбільше нанесення шкоди. Тут важливо забезпечити додаткову можливість для сканування файлових структур включно текстових ресурсів, таблиць (MS Word, Excel, Office), архівіруваних документів.

4. Показник ймовірності прийняття помилкового рішення щодо наявності вірусних уражень в окремих файлових сегментах. Це може призвести до блокування корисних даних та програм користувачем.

5. Показник щодо наявності властивостей не лише виявлення наявності вірусних уражень але й можливості лікування з блокуванням уражених інформаційних об'єктів. Отже значимим також є показник якості скан-детектування вірусних уражень.

6. Многоплатформність або масштабованість до різних операційних платформ (систем) антивірусних заходів. В іншому випадку антивірусний захід матиме обмежену можливість щодо використання функцій операційних платформ. Наприклад, антівірусна програма може виявиться непрацездатною для конкретної системи.

7. Показник однопроходності або попередньої перевірки зі скануванням інформаційного простору. Це дозволяє використовувати скан-перевірку в режимі швидкого детектування. Такий режим можна використовувати для побудови стратегії примусової перевірки у разі, наприклад, наявності високої ймовірності потенційних загроз з боку протиборчої сторони.

8. Показник, що характеризує модульність або багато функціональністьНаявність таких функцій можуть покращити практичність використання антівірусних програм.

Виходя чи з цього можна вказати на такі програмні антівірусні заходи:

- антивірусний компонент - програми-детектори (сканери). Вони дозволяють детектувати певний набір вірусних уражень. В їх основі лежить функціє спеціального співвідношення та порівняльне оцінювання характерної двійкової послідовності (сигнатур або масок вірусів). Такі послідовності обираються на основі наявних тестових вірусних еталонів, з двійковими послідовностями потоків або програмних кодів, що підвергаються скануванню. Особливістю тут є потреба у постійному оновленню набору тестових або еталонних послідовностей відомих вірусів (сигнатур). Зрозуміло, що в цьому разі збільшується ймовірність помилки першого роду, тобто коли уражена програма буде ідентифіковано, як «чиста».

- антивірусний компонент - програми-лікарі (фаги, дезінфектори). Особливістю тут е можливість додатково блокувати або усувати насідки ураження програмних кодів або двійкових потоків. Отже може бути вилучено вірус з корисного потоку інформації. Прикладами тут може бути: AVP; Aidstest ; Doctor Web.

- антивірусний компонент - програми-ревізори. Особливість тут полягає у оцінюванні змісту еталонного інформаційного поля з скан-варіантом шляхом порівняння їх синтаксису. Це може проводиться також на основі функціональних апроксимацій, що зменшує час перевірки. Еталону версіє зміст інформаційного пля позначають, як файл-ревізор. Оцінюванню підвергаються зміст Boot-Сектору, FAT та їх службові та маркерні атрибути (параметри). Прикладом такого типу антивірусний компонент може бути програма Adin f.

- антивірусний компонент - програми-фільтри (сторожачи, монітори). Особливість тут стосується виконання функцій прогнозу та опередження щодо наявності певних загроз. Відповідний пакет фільтрів здійснює контроль за такими операційними функціями: реконструкція файлів, інформаційних полів, системної області дисків; форматування дискового простору; резидентне розміщення програм оперативній пам’яті. Приклад таких антивірусний компонент програма Vsafe.

- антивірусний компонент - програми-іммунізатори. Особливість тут полягає проведені маркування шляхом фіксації у вакційну програму відповідної ознаки конкретного вірусу. Тоді даний тип вірусу буде сприймати окреслене інформаційне поле, як попередньо ураженим. Відповідно вакційне інформаційне поле буде уминатися з боку вірусних дій.

2.1. Оцінка сучасних методів маскування вірусних потоків в інформаційній мережі профільних структур

Маскування вірусних атак стає майже най актуальнішою проблемою на даний час, с кожним днем все частіше знаходять віруси, постійно створюють нові алгоритми пошуку вірусу. Як ми знаємо, що віруси йдуть на два кроки по переду від антивірусних програм. Люди які створюють віруси, це люди які досить великі програмісти, вони вміють дуже добре читати коди програм. Далі продовжемо говорити про маскування вірусних атак, на даний час можливо класифікувати маскування вірусів як продемонстровано на рисунку 2.1

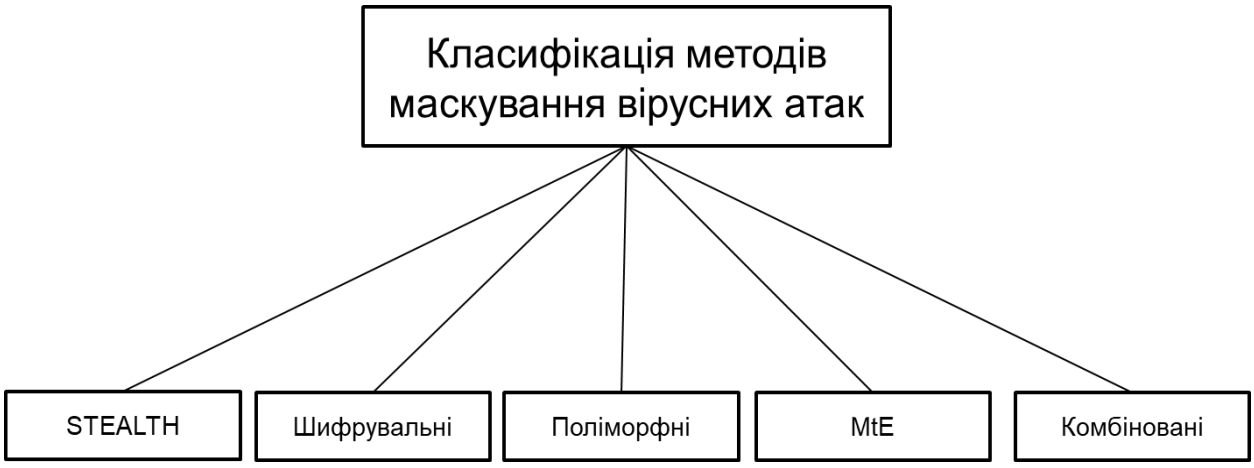


Рисунок 2.1 – Класифікація методів маскування

STEALTH – віруси, віруси в яких автори замінюють деякі компоненти операційної системи, наприклад, переривання, драйвери так, що програма-вірус стає невидимою для інших програм. Такі віруси називаються вірусами-невидимками, або стелс-вірусами (Stealth - невидимка).

Stealth-віруси завжди резидентны. Резидентний модуль перехоплює звернення операційної системи до уражених файлів і секторів дисків і "підставляє" замість них початкові об'єкти.

Так Stealth-віруси ховаються від досвідченого користувача і багатьох антивірусних засобів, які здійснюють ранній пошук вірусів щодо змін довжин файли контрольних сум і вмісту завантажувальних секторів.

Шифрувальні віруси, це віруси які шифрують свій код. З поняттям комп'ютерного вірусу тісно пов'язане інше поняття - сигнатура. Сигнатура - це фрагмент коду, що зустрічається у всіх копіях вірусу і тільки в них. Сигнатура однозначно визначає наявність або відсутність вірусу.

Найпростіша техніка шифрування виглядає наступним чином: кожен раз, коли вірус заражає нову програму, він зашифровує свій власний код, використовуючи новий ключ. Ключ шифрування залежить від цільового файлу (наприклад, його імені або довжини). В результаті два примірники одного і того ж вірусу можуть значно відрізнятися один від одного, і навіть мати різну довжину! Це ускладнює виявлення вірусу за допомогою сигнатурного пошуку. Адже зашифрований код вже не має тієї ж сигнатури.

Шифрувальний віруси при отриманні управління насамперед розшифровують свій код за допомогою процедури розшифрування, а потім виконують всі інші дії. Шифрувальний віруси називають іноді вірусами - "примарами".

Поліморфні віруси – це всі подальші удосконалення алгоритмів вірусів вже продиктовані виживанням вірусів при роботі під всілякими антивірусними засобами.

Шифрувальний віруси приховують сигнатуру свого коду. Але ж зашифрований код повинен бути розшифрований перед виконанням, отже, не-

обхідна процедура-дешифрування , яка сама не може бути зашифрована, так як виконується перед основним кодом вірусу. Дешифрувальник містить специфічний код і має достатній розмір для того, щоб служити сигнатурою. Цим і користуються антивірусні програми, які застосовують в якості сигнатури код процедури розшифрування. Автори вірусів на такий підхід відповіли поліморфними вірусами. Ці віруси для шифрування використовують не тільки різні ключі, але і різні процедури шифрування (відповідно, дешифрування). Два примірники такого вірусу не мають ні одного збігається послідовності коду!

Віруси, які завдяки використанню різних дешифрувальник, можуть повністю змінювати свій код, називаються поліморфними вірусами (polymorphic).

Ці віруси доповнені генераторами дешифрування. Такий генератор створює для кожної нової копії вірусу свій власний розшифровувача, відмінний від всіх інших, але виконує ту ж функцію. Це досить складно. Такі задачі відносяться вже до автоматизації програмування.

Метаморфізм. В комп'ютерній вірусології метаморфний код — це код, здатний до самоперепрограмування. Найчастіше він це робить шляхом переведення свого коду в яке-небудь тимчасове представлення, редагування цього представлення, а потім переведення його назад в двійковий код. Ця процедура застосовується до всього вірусу, включаючи механізм метаморфізму. Вона запускається тоді, коли вірус збирається заразити нові файлі, тому вірус-нащадок ніколи не виглядатиме так, як його батько.

Mutant engine (MtE) віруси. У 1991 р. в Болгарії найвідомішим автором вірусів, які іменують себе Dark Avenger (Чорний Месник), був розроблений алгоритм створення поліморфних вірусів. Це дуже складний алгоритм, який породжує дешифрувальники, абсолютно несхожі один на одного. Їх розмір коливається в діапазоні від 0 до 512 байт, а в тілі можуть зустрічатися практично всі команди процесора. Цей алгоритм його автор назвав Mutation

Engine (машина мутацій), скорочено він називається MtE або DAME (Dark Angel MuTation Engine).

Віруси з підключеним до них молулем MtE для породження дешіфровщіков, називають MtE-вірусами. Це напівавтоматичні віруси.

Слідом за Mutation Engine з'явилося ще кілька засобів розробки поліморфних вірусів. У Казані був створений AWME (Anti WEB Mutation Engine). А ось назви зарубіжних розробок поліморфних вірусів:

- Crazy Lord Mutation Engine (CLME);
- Dark Slayer Confusion Engine (DSCE);
- Golden Cicada Abnormal Engine (GCAE);
- NUKE Encription Device (NED);
- Simulated Metamorfic Encription Generator (SMEG);
- Trident Polymorfic Engine (TPE);
- Virogen's Irreguar Code Engine (VICE);

Навіть за кількістю автоматизованих розробок для створення поліморфних вірусів стає очевидним широке поширення поліморфних вірусів.

- період прихованості (латентності). Це активація вірусу через певний інтервал часових затримок та певних функціональних умов. Прикладом є вірус („Чорнобиль”), написаний Chen Ing Hau.

- КОМБІНОВАНІ ВІРУСИ - в сучасних умовах виживають і поширюються тільки складні віруси, які використовують всі відомі можливості для впровадження в комп'ютерні системи і для того, щоб приховати свою присутність.

Зазвичай такі віруси не обмежуються зараженням файлів одного типу. Файлово-завантажувальні віруси поширюються як через здійснимі файли, так і завантажувальні сектори дискет і жорстких дисків, одночасно вражаючи файли і сектори. При цьому вони, як правило, розміщують резидентний модуль оперативної пам'яті.

А для того, щоб досягти найбільшої невразливості, віруси комбінують і всі відомі методи маскування: від менш досвідчених користувачів і одного

виду антивірусних засобів ховаються, використовуючи Stealth-технологію, від більш досвідчених користувачів і більш потужних антивірусних засобів - реалізовуючи поліморфні механізми.

При цьому іноді виникають такі складні комбінації всіх цих способів, що результатом є потужний вірус, який виробляє масове зараження.

2.2. Дослідження підходів для захисту автоматизованого робочого місця від вірусного ураження в інформаційно-мережевому просторі

Раз вже мова зайшла про заходи щодо захисту від поширення шкідливого коду, то її можна і потрібно розглядати як викорінення причин, що роблять можливою реалізацію DDoS-атак. Якщо структурувати сучасні технології виявлення і захисту від шкідливого коду, то можна виділити три різновиди таких технологій: сигнатурну, поведінкову і репутаційну. Тільки однією з них вже недостатньо для ефективного захисту від вірусів. А от комбінація цих методів, реалізована на різних рівнях мережевої взаємодії, дозволяє побудувати ешелоновану систему захисту, вирішальну проблему поширення шкідливого коду. Один з найбільш ефективних підходів – застосування сигнатурної і поведінкової технології на рівні хоста і репутаційної технології-на рівні e-mail і Webшлюзов. Перші дві технології, реалізовані у формі антивірусного ПО і системи Host IPS (прикладна система виявлення і запобігання вторгнень) відповідно, органічно доповнюють один одного. Сигнатурні методи виявлення працюють за принципом " все, що в явному вигляді не заборонено, то дозволено». Заборона в явному вигляді означає заборону об'єктів, описаних сигнатурами конкретних примірників вірусів. У цьому принципі закладено реактивність, адже вірус спочатку з'являється, потім починає поширюватися, потім його починають аналізувати антивірусні компанії, після чого створюють сигнатуру цього вірусу, і, нарешті, антивірусне ПЗ отримує цю сигнатуру з черговим оновленням. За часом така ланцюжок дій займає кі-

лька годин, протягом яких антивіруси беззахисні перед новою формою загрози. Багато сучасні антивіруси мають так звані фільтри запобігання вірусних епідемій, що дозволяють скоротити час очікування виходу сигнатури. Але ці фільтри також є реакцією на появу нового зразка шкідливого коду, і проблему реактивності антивірусів вони в цілому не вирішують. Другий підхід, поведінковий, позбавлений даного недоліку, так як діє від зворотного – «все, що в явному вигляді не дозволено, то заборонено». Але для того щоб реалізувати такий принцип, система Host IPS повинна знати, що таке «нормальна» поведінка системи і, щоб на підставі цього знання виявляти «ненормальне». Для створення шаблону нормальної поведінки деякий час доведеться витратити на навчання і налаштування системи. І, нарешті, репутаційна технологія безпосередньо адресує новий метод поширення шкідливого коду в Web-трафіку. Реалізована на рівні Web-шлюзу система аналізу репутації перевіряє кожен запитуваний користувачем ресурс в мережі Інтернет на предмет того, наскільки безпечним буде його відвідування. Наприклад, якщо Web-сайт був зареєстрований кілька днів тому, і в якийсь момент на цей сайт почався великий потік запитів, чого раніше не спостерігалося, то це є ніщо інше, як один з найпопулярніших на сьогодні способів поширення шкідливого ПЗ. Така яскраво виражена аномалія в трафіку не може залишитися непоміченою для спеціалізованих систем, які займаються моніторингом Web-трафіку і оцінкою репутації, таких як мережа SenderBase (www.senderbase.org), використовувана в рішеннях Cisco IronPort. Однак, незважаючи на достаток технологій і рішень, націлених на запобігання вірусних заражень, нові вірусні епідемії не перестають вражати своїми масштабами. Причин тому кілька-це і зростання числа користувачів Інтернету, і висока швидкість поширення нових примірників шкідливого коду, що робить все менш і менш ефективним захист, засновану тільки на наявності антивірусного ПЗ на комп'ютері користувача.

Також крім технологій по захисту від поширення шкідливого коду є ще одна технологія, що дозволяє запобігти створення ботнету в той момент, коли поїзд, здавалося б, вже наполовину пішов, а саме, коли вірус вже потрапив

на комп'ютер користувача і намагається вийти на зв'язок з контролером ботнету для отримання подальших інструкцій. У спеціалізованих лабораторіях спіймані екземпляри вірусів аналізуються, визначаються не тільки безпосередньо сигнатури вірусу, але і ресурси, з якими він намагається вийти на зв'язок. Таким чином формуються списки контролерів ботнетів, які служать основою для протидії ботнету на другій фазі його життєвого циклу. Функціональність з моніторингу та блокування з використанням таких списків може бути реалізована в різних мережевих пристроях. Зокрема, в рішеннях Cisco вона присутня в міжмережевих екранах Cisco ASA і Web-шлюзах IronPort Web Security. Но зловмисники теж не стоять на місці і реалізують в ботнетах нові методи комунікацій. Все частіше замість звичного IRC-каналу зв'язку вірусів з контролером ботнету застосовуються P2P-комунікації, ті самі, на основі яких побудовані файлообмінні мережі. P2P-комунікації дозволяють позбутися від необхідності кожному зараженому комп'ютера безпосередньо спілкуватися з єдиним сервером управління ботнету. Керуюча команда може бути введена в будь-який із заражених вузлів і далі може поширюватися вже між учасниками ботнету. Вельми цікавий метод реалізований творцями вірусу Conficker. Вірус щодня генерує за заданим алгоритмом 50 тис. DNS-адрес, з якими він намагається вийти на зв'язок. Творцеві ботнету, ймовірно, заздалегідь відомо, які адреси в який день будуть згенеровані, і досить буде заздалегідь зареєструвати будь-який з цих адрес в DNS і розмістити за цією адресою керуючий сервер. В результаті сервер може постійно переїжджати з адреси на адресу, що досить надійно захищає ботнет від нейтралізації керуючого каналу. При даному підході, що поєднується з P2P-технологією, намагатися виявити і заблокувати канал зв'язку з контролером ботнету – все одно, що шукати голку в копиці сіна. Теоретично при комбінації з 10 млн учасників ботнету і 50 тис. адрес керуючого сервера ботнету для продовження своєї діяльності досить здійснювати кожен день все одне успішне з'єднання з 500 млрд можливих. Сама по собі технологія блокування за заздалегідь відомим списком контролерів ботнетів також не може дати 100%-ний результат. Але вона

може використовуватися в поєднанні з перерахованими вище способами боротьби з поширенням шкідливого коду, і не тільки як механізм блокування, але і як засіб виявлення заражених сайтів в мережі. Адже якщо користувач раптом наполегливо намагається зв'язатися з контролером ботнету, то навряд чи він робить це з доброї волі. Перераховані заходи з протидії створенню ботнету можна розглядати як спосіб запобігання вихідних атак. Це важливо для організацій і операторів зв'язку, так як вихідні від ботнету явища, такі як спам і DDoS, не кращим чином впливають на ділову і технологічну репутацію оператора. Але, на жаль, далеко не всі організації здатні запобігти утворенню ботнетів у своїх мережах, тому доводиться мати справу з вхідними в мережі DDoS-атаками і боротися з величезними потоками шкідливого трафіку.

розвитку ботнету, то багато давно відомі методи нанесення DDoS-атак як і раніше залишаються актуальними. За способом виведення з ладу інформаційної системи жертви розрізняють два класи DDoSатак: атака на переповнення смуги пропускання каналу зв'язку: складається з мережевих пакетів великого розміру (як правило, UDP Flood с довільними номерами портів, рідше ICMP Flood); атака на вичерпання обчислювальних ресурсів кінцевого вузла: застосовуються такі методи, як TCP SYN Flood, DNS Query Flood і HTTP GET Flood. Якщо подивитися на шлях трафіку атаки, то він буде виглядати наступним чином: Заражений комп'ютер – Оператор доступу – Магістральні оператори – Оператор доступу – Жертва. Вплив DDoS-атаки (рис. 2) посилюється в міру акумуляції потоків шкідливого трафіку у напрямку до жертви. Для власника зараженого комп'ютера і його оператора зв'язку атака може бути практично непомітна, якщо, звичайно, у оператора немає рішень, що дозволяють виявляти вихідний флуд від окремих абонентів. Для магістральних операторів атаки середнього розміру також можуть залишитися непоміченими на тлі величезних потоків переданого трафіку. А ось для оператора жертви атака буде виражатися як мінімум в підвищеному навантаженні на мережу. Ну а для незахищеної жертви це явище буде рівносильно відклю-

чення від Інтернету. На прикладі наведеного ланцюжка проходження трафіку зручно розглянути застосовність різних методів придушення DDoS-атак. Користувач зараженого комп'ютера може боротися з вірусним зараженням методами, які ми вже розглянули в раніше. Оператор зв'язку, до якого підключені заражені вузли, може виявляти шкідливі потоки трафіку і таким чином ідентифікувати заражених абонентів у своїй мережі. Вихідний DDoS видає себе за аномальною кількістю одночасних мережевих з'єднань від окремих абонентів. Для моніторингу таких сполук від кожного абонента застосовні рішення DPI (deep packet inspection), що виконують глибоку перевірку трафіку і аналіз даних Netflow. Наприклад, DPI-рішення операторського класу Cisco Service Control Engine (Cisco SCE) може виявляти спроби розсилки спаму, вихідний DDoS, спроби сканування і поширення черв'яків. Все це характерні ознаки для учасника ботнету. Після того, як виявлено заражений сайт, рішення Cisco SCE дозволяє заблокувати шкідливі потоки трафіку і помістити абонента в карантинну мережу. Магістральні оператори зв'язку і оператор, до якого підключений атакований ресурс, можуть безпосередньо захистити жертву від DDoS-атаки. Високошвидкісні канали зв'язку, якими вони мають, дозволяють прийняти весь потік трафіку, що йде у напрямку до жертви, і заблокувати його шкідливу складову за допомогою спеціалізованих рішень по захисту від DDoS. Чому потрібні саме спеціалізовані рішення? Справа в тому, що з точки зору окремих мережевих пакетів, шкідливий трафік складно відрізнити від легітимного. Одні й ті ж пакети TCP SYN, DNS Query і HTTP GET присутні і в рамках легітимних сесій. Але ключовий момент полягає в тому, що трафік DDoS-атаки, як правило, складається виключно з перерахованих вище первинних протокольних запитів, і продовження мережевої взаємодії для трафіку DDoS-атаки не характерно. На цій ключовій особливості DDoSатак і побудовані різні механізми блокування шкідливого трафіку в рішенні Cisco Guard. Ідея полягає в тому, щоб у відповідь на прийшов запит послати відповідну відповідь, що вимагає обов'язкової реакції від запитувача. Якщо він реагує і від нього приходить адекватну відповідь, то ві-

дразу можна зрозуміти, що це не спуфинг IP-адрес джерела і не односторонній потік протокольних запитів. Саме ці дві важливі характеристики відрізняють легітимний трафік від трафіку DDoS-атаки. Наприклад, для захисту від атаки TCP SYN Flood в Cisco Guard застосовується відомий механізм SYN Cookie, який втручається в процес встановлення TCP-з'єднання з метою переконатися, що цей процес пройде коректно. Для захисту від атак на Webсайти за допомогою завалу запитами HTTP GET в рішенні застосовується HTTP Redirect, по реакції на який можна відрізнити трафік ботнета, що складається тільки з запитів HTTP GET без какоголибо продовження, від трафіку легітимних користувачів. У пристрої Cisco Guard такі перевірочні механізми реалізовані для захисту від самих різних варіантів протокольних DDoS-атак, причому є кілька послідовно застосовуваних рівнів перевірок – від м'яких до більш жорстких, аж до блокування трафіку з атакуючих вузлів. Поряд зі старими методами реалізації DDoS, які застосовуються в ході переважної більшості атак, іноді зустрічаються і нові методи. Один з таких недавно помічених методів-здатність ботнету реагувати на HTTP Redirect в ході атаки на Webсайт, що дозволяє обходити цей механізм захисту. Гарна новина полягає в тому, що рішення Cisco Guard оцінює трафік після всіх етапів обробки як на вході, так і на виході, і якщо поточні активні механізми не допомагають, то до трафіку атаки будуть застосовані ще більш жорсткі методи. Цей приклад ще раз підтверджує сучасну тенденцію: спеціалізовані засоби захисту від DDoS отримують все більшу поширеність в мережах операторів зв'язку, і творці ботнетів вивчають застосовуються механізми захисту і намагаються реалізувати способи їх обходу. Що може зробити жертва? Не так вже й мало, як може здатися. Жертва може не тільки чекати якнайшвидшого закінчення DDoS-атаки, але і вживати ефективних заходів з профілактики: опрацьовувати питання взаємодії з оператором зв'язку на випадок можливих атак; застосовувати рекомендації щодо захисту на рівні ОС і додатків для публічно доступних серверів, таких як Web і DNS. А при наявності спеціалізованого рішення організація-жертва може самостійно впоратися з DDoSатакой, але

тільки поки не будуть повністю забиті трафіком атаки канали зв'язку з оператором. Ось чому захист від атак на вичерпання пропускної здатності – обов'язок виключно оператора зв'язку. Ефективно вирішити проблему DDoS-атак цілком можливо, але старий підхід «одна проблема – одна технологія захисту» вже давно не працює. Необхідно приймати заходи для захисту, причому як на виході атак, так і на вході, і реалізовувати ці заходи і на рівні операторів зв'язку, і в корпоративних мережах.

2.3 Оцінка ефективності функціонування антивірусних заходів у мережах профільних структур

Реалізація антивірусний компонент потребує постійного моніторингу та оновлення баз антивірусів. Бази антивірусний компонент містять відомості щодо певних вірусів та алгоритм їх ліквідації. Відповідно для цього проводиться безперервний моніторинг. Аналізується вірусна активність інформаційного простору. Для цього застосовуються спеціальні мережі, які збирають відповідну інформацію. Наступним кроком є аналіз зібраної інформації за результатами антівірусного моніторингу. В процесі аналіз встановлюється: характер шкідливості вірусу; типовий код вірусу; характер нанесення можливої шкоди. Кінцевим кроком є відпрацювання напрямку дії щодо блокування та вилучення вірусних уражень.

Проблема боротьби з вірусними атаками є те, що нові віруси майже не можливо знайти, із за того що кожного разу знаходять нові способи замаскувати вірус, про це і поговоримо. Віруси приховують свою присутність порізному.

Одні віруси виявляються не відразу, а через деякий час, даючи можливість самому собі якомога більше розмножитися. Під проявом вірусу в даному випадку маються на увазі дії вірусу, з яким навіть недосвідчений користувач може відчути щось недобре. Це, наприклад, такі явні прояви вірусу, як

виконання якої-небудь мелодії або виведення на екран монітора будь-які повідомлення або малюнка. Від форматувати диск або зіпсувати завантажувальний сектор відразу ж при першому зараженні також "невигідно" вірусу, адже на цьому закінчується і його "життя". Тому багато віруси ставлять такі свої деструктивні дії у залежність від якихось певних умов. Наприклад:

а) багато віруси виявляються в один або деякі певні дні;

б) інші віруси ставлять свій прояв у залежність від випадковостей всілякого роду. Наприклад, якщо значення хвилин таймера менше N; чи перевіряє відсутність вводу з клавіатури протягом N хвилин; ,більшість завантажувальних вірусів люблять нищити сектори дисків, обчислюючи ймовірність (1/8 або 1/16);

в) іноді автори вірусів ставлять лічильники на кількість натискань на клавіші, на кількість заражених файлів, секторів і в залежності від їх значень виявляють свої віруси.

Тепер кілька слів про те, як працює будь-який сучасний антивірус. Це процес, який включає в себе стадії сканування на вимогу, попередження вторгнення загроз на основі декількох типів аналізу потенційно небезпечних файлів або ресурсів в інтернеті і ізоляція або повне знищення загрози. В якості інструментів визначення вірусів використовується два типа аналізу: сигнатурний і імовірнісний.

Сигнатурний аналіз - цей тип аналізу базується безпосередньо на зверненні до спеціальних баз даних, в яких є відомості про вже відомі віруси. При сканування потенційно небезпечного об'єкта програма порівнює його структуру з вже відомими структурами інших виявлених загроз. Саме тому можна сміливо стверджувати, що сучасний антивірус – це програма, для якого такі бази потрібно періодично оновлювати, оскільки нова інформація в них заноситься мало не щодня. Як вже було сказано, віруси еволюціонують набагато швидше, ніж антивірусне ПО. Таким чином, і версія антивіруса теж підлягає оновленню, оскільки вбудовані модулі старіють і з часом можуть не справлятися з покладеними на них функціями.

Імовірнісний аналіз - цей тип перевірки складається з трьох підтипів: евристичний і поведінковий аналіз, плюс метод порівняння контрольних сум. Кожен з цих трьох типів можна було б виділити в незалежні категорії, але в світовій практиці вони об'єднані в один тип у вигляді підрозділів. Розглянемо кожен з них:

- евристичний аналіз - по суті своїй дуже схожий на сигнатурний, оскільки заснований на порівнянні структури загрози на основі вже відомих ізольованих загроз. Різниця тільки в тому, що тут передбачено ще і визначення вбудованих в вірус алгоритмів, на основі яких виявляється можливий спосіб можливого впливу шкідливого коду на комп'ютерну систему;

- поведінковий аналіз - виходячи з назви цього типу тестування, неважко здогадатися, що він пов'язаний з евристичним аналізом і дозволяє зробити прогноз того, як вплив загрози позначиться на стані системи. Однак ця методика задіється більше стосовно до різного роду макросів і скриптів;

- аналіз контрольних сум - ще один взаємопов'язаний компонент, що дозволяє визначити наявність вірусу – порівняння контрольних сум файлів. Вся інформація про структуру будь-якого файлу, присутнього в системі, записується в кеш, а при спробі зміни об'єктів відбувається порівняння початкової і кінцевої сум, відповідних одного і того ж файлу. Коли зміни в якійсь файл вносить користувач або системний процес, зараз в розрахунок не беремо. Але от у випадку, коли починається масове або одночасне зміна контрольних сум, це якраз і може свідчити про те, що вплив шкідливого коду вже активувалося;

Також антивірусні програми стали працювати хитріше, вони стали використовувати штучний інтелект, та Верифікацію, що позволило працювати антивірусним програмам швидше, та знаходити в зловмисні функції у програмному коді.

2.4. Дослідження недоліків антивірусних заходів з врахуванням досвіду протидії для профільних структур

Як ми не хочемо буди в певними в антивірусних програмах в них є недоліки які продемонстровано на рисунку 2.2. Основними недоліками є те що антивірусні програми працюють по вже створеними базами даних та знань. Вони не можуть розшифровувати файли та не можуть залазити у зображення та відео потоки для перевірки даних. Не проводиться перевірка по причинам того що антивірусній програмі не вистачає розрахункових можливостей для перевірки усіх елементів. Для більш менш адекватного пошуку вірусних програм починають використовувати нейроін мережі, але вони теж потребують великої кількості розрахункової можливості а ще і час.

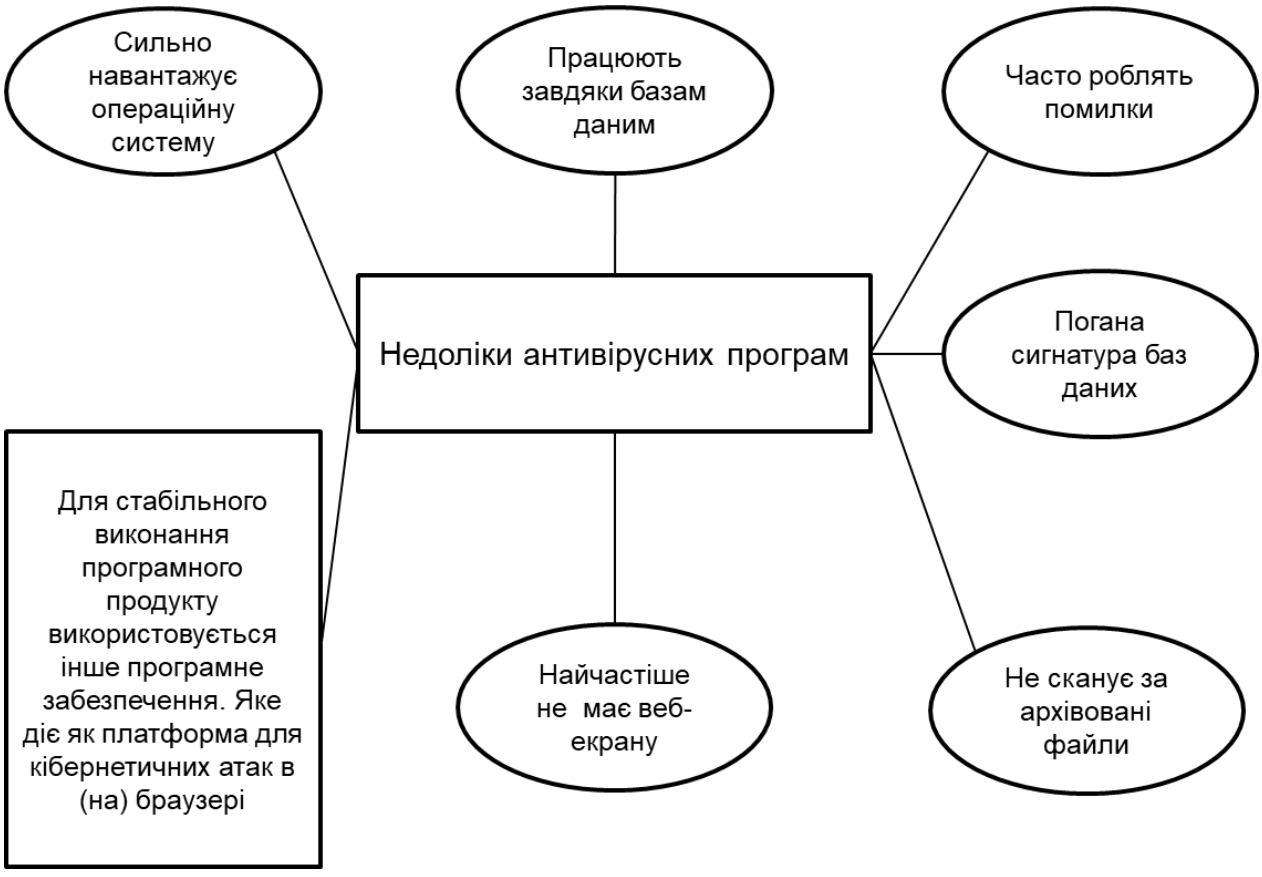


Рисунок 2.2 – Типові недоліки властиві антивірусним програмам

Висновок до розділу 2

Дослідивши принципи маскування вірусних атак а також роботу антивірусних програм, визначив що антивірусні програми почали дуже швидко нарощувати свою сили проти вірусів. Сучасні антивірусні програми почали використовувати нейрону мережу, за для гнучкого пристосування антивірусної програми в залежності від середовищ використання їх. Що дня антивірусні компанії нарощують свої бази даних, але це не достатньо для ефективної протидії вірусним програмам а також кібернетичним атакам.

3 РОЗРОБКА АДАПТИВНОГО МЕТОДУ ПРОТИДІЇ ПРИХОВАНИМ ВІРУСНИМ АТАКАМ В ІНФОРМАЦІЙНО-МЕРЕЖЕВОМУ ПРОСТОРІ ПРОФІЛЬНИХ СТРУКТУР

3.1 Створення адаптивного методу маскування даних з врахуванням особливостей виконання завдань в інтересах профільних структур

Серед даних методів маскування вірусних атак ми для дослідження обираємо комбінований метод, який складається з трьох етапів:

Перший етап - шифрування вірусу методом Advanced Encryption Standard

Другий етап - використання поліморфізму

Третій етап - запис коду програми у відео потік завдяки водяним знакам

Advanced Encryption Standard (AES), також відомий під назвою Rijndael — симетричний алгоритм блочного шифрування (розмір блока 128 біт, ключ 128/192/256 біт)

Шифрування вірусного коду проходить за алгоритмом продемонстрованого нижче на рисунку 3.1, та включає в себе такі функції:

ExpandKey — функція для обчислення усіх раундових ключів;

SubBytes — Функція для підстановки байтів, використовуючи таблицю підстановки;

ShiftRows — Функція, забезпечує циклічний зсув у форму на різні величини ;

MixColumns — Функція, яка змішує дані всередині кожного стовпця форми;

AddRoundKey — Додавання ключа раунду з формою;

Також в алгоритмі використовується скорочень Nr що означає в свою чергу кількість раундів. Даний принцип шифрування вірусної атаки в спеціальних телекомунікаційних системах є дуже простим, водночас його дуже важко розшифрувати, не знаючи ключа це може зайняти кілка років. За цей час поки будуть розшифрувати вірус зможе нанести великі втрати як інформаційні так і зможе нанести шкоду техніці.

Розшифрування відбувається аналогічним чином, тільки в зворотному порядку.

Наступним кроком буде використання поліморфізму. Поліморфізм - висококласна техніка, що дозволяє вірусу бути непоміченим за стандартною сигнатурі (або, просто, масці). Зазвичай детектори визначають вірус з характерним шматках його коду. У випадку з поліморфним вірусом таке не пройде. Два файли, заражені одним і тим же вірусом, завжди будуть мати різний розмір. Засікти такий вірус дуже складно.

Всі поліморфні віруси обов'язково забезпечуються расшифровщиком коду, який за певним принципом перетворює переданий йому код, викликаючи при цьому стандартні функції та процедури операційної системи. Самі методи шифрування можуть бути різними, але, як правило, кожна операція має свою дзеркальну пару. В асемблері це реалізується дуже просто, і таких пар може бути багато - ADD/SUB, XOR/XOR, ROL/ROR і т. п.

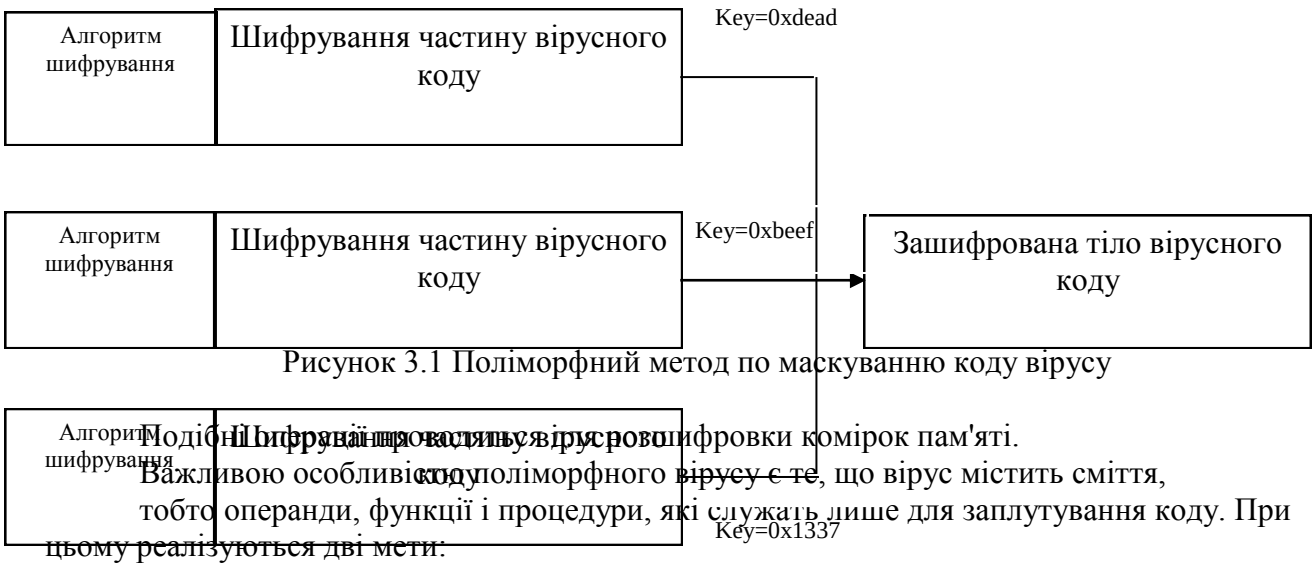


Рисунок 3.1 Поліморфний метод по маскуванню коду вірусу

Подібні операції використовуються для розшифровки комірок пам'яті.

Важливою особливістю поліморфного вірусу є те, що вірус містить сміття, тобто операнди, функції і процедури, які служать лише для заплутування коду. При цьому реалізуються дві мети:

Перша мета - складність вивчення коду при трасуванні файлу. Ця мета актуальна лише для новачка, професіонал, який вивченням вірусів займався багато років, одразу у всьому розбереться.

Друга мета - збільшення елементу випадковості в розшифровці. Місце їх вставки має величезний вплив на розмір коду. З сміттям з'являються нові варіанти компонування коду. Розмір при кожному з них буде різним.

Асемблер дає безмежні можливості по вставці сміття, тому вставки можуть бути різними. Ось деякі їх види:

- регістрові операції. Як правило, арифметичні і логічні. Прикладом можуть служити наступні команди: inc ax; mov ax,[si+bx-04]; add ax,1234h;
- дзеркальні команди. Такі, як add/sub, inc/dec та інші;
- помилкові переходи, а також виклик підпрограм, що містять сміття;
- Простий сміття з одиночних операндів (daa; nop; cld тощо);

Виділяють кілька рівнів поліморфізму, використовуваних у вірусі. Кожен з них по-різному реалізує неоднаковий розмір файлів, які були заражені.

Рівень 1. Найпростіші поліморфні віруси. Вони використовують постійні значення для своїх дешифрувальних, тому легко визначаються антивірусами. Із за цього такі віруси прозвали "не дуже поліморфними".

Рівень 2. Віруси, що мають одну або дві постійні інструкції, які використовуються в дешифрувальнику. Також визначаються по сигнатурі, але мають більш складну будову, ніж представники першого рівня. Приклади: ABC, DM, Flip, Jerusalem, Ontario, PC-Flu, Phoenix, Seat, Stasi, Suomi.

Рівень 3. Віруси, що використовують у своєму коді команди-сміття. Це, у своєму роді, пастка від детектування, допомагає заплутати власний код. Але такий вірус може бути помічений з допомогою попереднього відсіювання сміття антивірусом. Віруси Tequila, StarShip, V2Px, DrWhite належать до третього рівня поліморфізму.

Рівень 4. Використання взаємозамінних інструкцій з перемішуванням в коді, без додаткового зміни алгоритму дешифрування, допомагає повністю заплутати антивірус. При цьому неможливо "зловити" вірус за стандартною масці. Доводиться виконувати перебір, після якого потрібна сигнатура буде знайдена. Так були написані віруси Uruguay, CLME, APE.

Рівень 5. Реалізація всіх вищевикладених рівнів з підтримкою різних алгоритмів в дешифраторів допомагає досягти високого рівня поліморфізму. При цьому може існувати кілька паралельних процесів дешифрування , коли один буде перетворювати код іншого або навпаки. Розпізнавання таких вірусів - дуже складний процес. Для цього необхідно провести ретельний аналіз коду самого дешифрувальника. З лікуванням складніше - доводиться трасувати не тільки генератор, але і тіло самого вірусу для виявлення повної інформації про зараженому файлі. Ця процедура займає досить тривалий час і може закінчитися невдало. Лікувати віруси цього рівня може лише DrWeb, в інших програмах це просто не реалізовано. До представників рівня відносяться DAME та ін.

Рівень 6 (невиліковний). Існують віруси, які складаються з програмних одиниць-частин. Вони постійно змінюються в тілі і переміщують свої підпрограми. Лікування таких вірусів поки не проводиться, але і для написання потрібно дуже добре розбиратися в асемблері. Характерною особливістю такої зарази є плями. При цьому в різні місця файлу записується кілька блоків коду, що обумовлює назву методу. Такі плями в цілому утворюють поліморфний розшифровувача, який працює з кодом в кінці файлу. Для реалізації методу навіть не потрібно використовувати команди-сміття - підібрати сигнатуру буде все одно неможливо. Такий алгоритм використовують віруси BadBoy, CommanderBomber, Витоків і т. п.

При формальному поданні генерації ЦВЗ у вигляді математичної моделі скористаємося загальноприйнятою записом: $\varphi: X \to Y$ де ϕ –відображення (функція); X – область визначення; Y – область значень. Введемо наступні позначення: $Y_{ЦВЗ}$ – безліч ЦВЗ; $X_{КЛЮЧ}$ – безліч ключів, $X_{КОНТЕЙНЕР}$ - безліч контейнерів; $X_{повідомлень}$ - безліч прихованих повідомлень. Тоді генерація ЦВЗ може бути представлена у вигляді:

$$F: X_{контейнер} * X_{Ключ} * X_{повідомлення} \to Y_{ЦВЗ} \quad (3.1)$$

Або

$$y_{ЦВЗ} = F(x_{контейнер}, x_{ключ}, x_{повідомленя}) \quad (3.2)$$

Функція F (відображення) може бути довільною, але на практиці вимоги робастності ЦВЗ накладають на неї певні обмеження. Формально це можна записати так

$$y_{\text{ЦВЗ}} = F(x_{\text{контейнер}}, x_{\text{ключ}}, x_{\text{повідомленя}}) \approx F(x_{\text{контейнер}} + \varepsilon, x_{\text{ключ}}, x_{\text{повідомленя}}) \quad (3.3)$$

тобто незначно змінений контейнер не призводить до зміни ЦВЗ. Крім того, функція F часто є складовою:

$$F = T \cdot G \quad (3.4)$$

де $G: X_{\text{ключ}} * X_{\text{повідомленя}} \rightarrow X_{\text{код}}$ та $T: X_{\text{контейнер}} * X_{\text{код}} \rightarrow Y_{\text{ЦВЗ}}$; - привілейований

Функція G може бути реалізована за допомогою криптографически безпечного генератора псевдовипадкових послідовностей з $X_{\text{ключ}}$ в якості початкового значення. Відлік ЦВЗ приймають зазвичай значення з множини {-1, 1}, при цьому для відображення {0,1} → {-1, 1} можна застосувати двійкову відносну фазову модуляцію ФМн-2 (Binary Phase Shift Keying (BPSK)). Даний вид модуляції знайшов дуже широке застосування через високу завадостійкості і простоти модулятора і демодулятора. Оператор T модифікує кодові слова $X_{\text{код}}$ в результаті чого виходить ЦВЗ - $Y_{\text{ЦВЗ}}$. На цей оператор не накладають умова існування у нього зворотного, так як відповідний вибір G вже гарантує незворотність F. Функція T повинна бути обрана так, щоб незаповнений контейнер $x_{\text{контейнер}} \in X_{\text{контейнер}}$, заповнений контейнер $x_{\text{контейнер}_{\text{заповнений}}} \in X_{\text{контейнер}}$ продовжував би один той самий ЦВЗ.

$$T(X_{\text{контейнер}_0}, x_{\text{код}}) = T(X_{\text{контейнер}_{\text{заповнений}}}, x_{\text{код}}) = T(x'_{\text{контейнер}_{\text{заповнений}}}, x_{\text{код}}) \quad (3.5)$$

тобто вона повинна бути стійкою до малих змін контейнера.

Процес вбудовування ЦВЗ $y_{\text{ЦВЗ}}(i,j)$ в вихідне зображення $x_{\text{ЦВЗ}}(i,j)$можна описати як суперпозицію двох сигналів:

$$x_{\text{Контейнер заповнений}}(i,j) = x_{\text{контейнер}_0}(i,j) \oplus x_{\text{Маска}} y_{\text{ЦВЗ}}(i,j) p(i,j) \quad (3.6)$$

Тепер проаналізуємо алгоритм роботи вірусу, який зображений на рисунку 3.3.

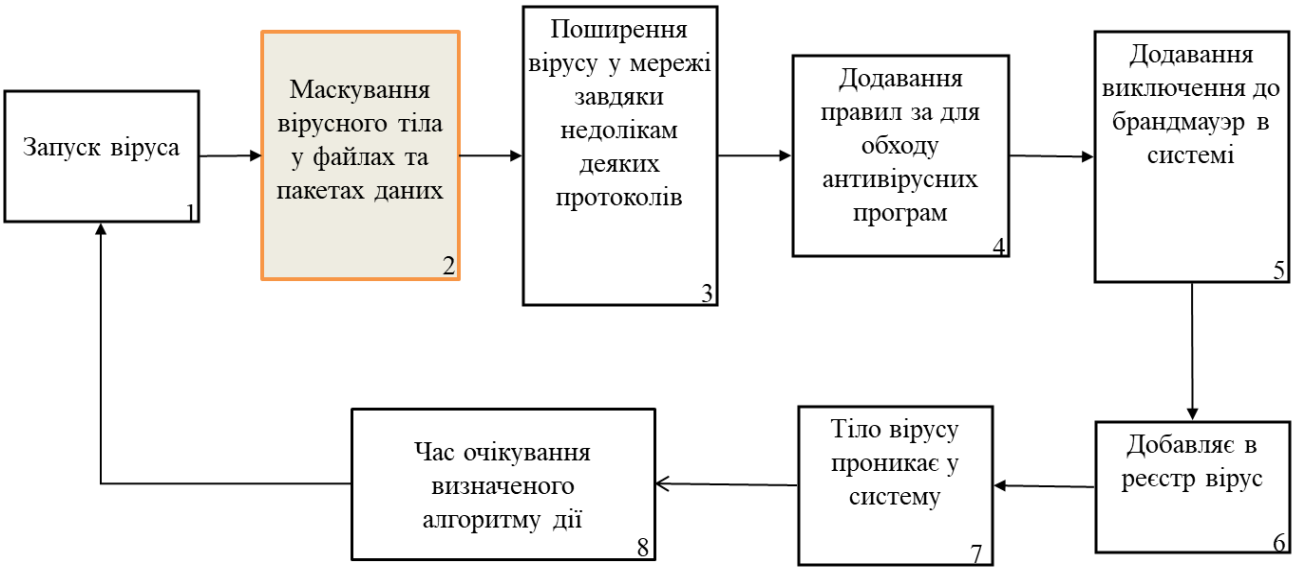


Рисунок 3.2 - Алгоритм роботи вірусу

Перший етап, один з найпростіших. Запуск вірусу проводиться на комп'ютері, який був заражений раніше. Запуск вірусу може проводитись віддалено, а також безпосередньо з самого зараженого комп'ютера. На даному етапі , найскладніше є те щоб програма (вірус) не була помічена антивірусними програмами.

Другий етап маскує вірус у зображеннях, відео файлах а також у пакетах при передачі тіла вірусу у мережі.

Третій етап, один з найважливіших етапів вірусу. Поширення вірусів в тимчасових, централізованих і комбінованих мережах відбувається по різному, однак результат практично завжди один і той же - програми, розташовані на робочих станціях і дисках сервера виявляються зараженими. Розглянемо способи поширення вірусу у різних мережах:

Віруси в однорангових мережах

Поширення вірусів в однорангових мережах можливо завдяки тому, що користувачі надають доступ на запис до дисків робочих станцій.

Рано чи пізно один з користувачів приносить флешку, заражену завантажувальним або файловим вірусом. При активізації вірус переглядає всі диски, доступні на запис, і заражає розташовані там програми.

Деякі завантажувальні віруси, які поширюються тільки через завантажувальні сектори локальних дисків, не можуть перейти через мережу на диски іншої робочої станції, навіть якщо до цього диску є доступ на запис. Справа тут в тому, що для запису в завантажувальні сектори необхідно використовувати систему введення-виведення, розташовану в basic input/output system (BIOS), а ця система "не вміє" працювати з секторами мережевих дисків. Спосіб запису вірусу в завантажувальні сектори, заснований на безпосередній роботі з дисковим контролером, також не підходить для мережевого диска, так як контро-

лер підключений до іншої станції та його порти введення-виведення абсолютно недоступні.

Проте об'єднані файлово-завантажувальні віруси закріплюються в завантажувальних секторах локального диску робочої станції і заражає файли, розташовані на всіх дисках, доступних для запису. У тому числі, зрозуміло, і файли, розташовані на мережевих дисках, що належать іншим робочим станціям.

Якщо користувач надав до своїх дисків доступ тільки на читання, але на них записані заражені програми, то інші користувачі зможуть запустити таку програму. В результаті цього їх локальні диски виявляться зараженими.

Віруси в централізованих мережах

Незважаючи на те, що в централізованих мережах користувачі не мають доступу до ресурсів інших робочих станцій, є принаймні дві можливості для поширення вірусів.

По-перше, вірус може потрапити з однієї з робочих станцій на диски сервера доступні для запису, заразивши записані там програми. Коли користувач робочої станції запустить заражену програму безпосередньо з диска сервера або спочатку перепише її на локальний диск і потім запустить її там, робоча станція виявиться зараженою. Таким чином, через якийсь, можливо дуже невеликий час, вірус потрапить з сервера на вс робочі станції, мережі та їх заразить.

По-друге, існує принципова можливість створення такого вірусу, який зуміє підібрати пароль системного адміністратора і записати себе навіть на диски, захищені від запису. І все це незважаючи на те, що современые мережеві операційні системи мають досить потужну і надійну систему розмежування доступу. Однак відомо: що один чоловік зробив, інший може зламати.

Незважаючи на те, що система паролів потенційно володіє високою стійкістю, зусилля користувачів можуть звести нанівець весь захист. Наприклад, для того щоб полегшити собі життя, вони не задають паролі взагалі або вказують в якості пароля своє ім'я або прізвище, рік народження і т. п.

Між тим існує список найбільш поширених паролів, який доступний через електронні дошки оголошень і, звичайно ж, є у розпорядженні розробників вірусів. Таким чином, при підборі пароля вірусу не потрібно перебирати величезна кількість випадково вибраних комбінацій символів, а досить

пройтися по зазначеному списку. Імовірність успіху при цьому досить велика.

Правильно налаштувавши права доступу користувачів і саму систему управління доступом, системний адміністратор може значно зменшити небезпеку ураження вірусами дисків сервера. Істотну допомогу в захисті сервера можуть надати спеціальні антивірусні програми та апаратні засоби захисту, які ми розглянемо в нашій книзі.

Віруси в комбінованих мережах

Як і слід було очікувати, у комбінованих мережах віруси можуть поширюватися як безпосередньо між робочими станціями, так і через диски серверів. При цьому віруси можуть потрапляти на диски, доступні для запису або ж вони можуть робити спроби підбору паролів для отримання доступу до дисків, захищених від запису.

Взявши на себе відповідальність за супроводу комбінованої мережі, для запобігання виникнення вірусної епідемії системний адміністратор повинен захищати від вірусів не тільки сервер, але і робочі станції.

Вірус в оперативній пам'яті сервера

Так як вірус є програмою, для активізації він повинен бути завантажений в оперативну пам'ять, після чого вірусу повинно бути передано управління.

Коли вірус "живе" на робочої станції, так і відбувається. Користувач запускає заражену програму або завантажує операційну систему з дискети, заражена завантажувальним вірусом, в результату чого вірус тим чи іншим способом виявляється в оперативній пам'яті робочої станції.

Якщо ж користувач запускає заражену програму безпосередньо з диска сервера, вірус знову-таки потрапляє в оперативну пам'ять робочої станції, з якої був виконаний запуск.

Таким чином, звичайний вірус, не розрахований спеціально для роботи під управлінням мережевої операційної системи, може змінити тільки вміст файлів, розташованих на доступних для запису дисків. Але він не може змі-

нити завантажувальні сектори на дисках сервера, так як для цього вірус повинен потрапити в оперативну пам'ять сервера, програма і отримати управління.

Тим не менш, можливо створення таких вірусів, які запускають себе як процес у середовищі мережевої операційної системи. Такі віруси найбільш небезпечні, так як їм доступні всі ресурси сервера.

Наприклад, зламавши тим чи іншим способом пароль супервізора, вірус може записати себе в системний каталог сервера Novell NetWare у вигляді nlm-програми і вказати її ім'я в файлі автоматичного конфігурування startup.ncf. При цьому вірусна nlm-програма буде отримувати управління кожен раз при завантаженні сервера.

Сучасні мережні операційні системи, такі, наприклад, як Windows NT, допускають віддалений запуск процедур. Ця можливість може бути використана спеціалізованими мережевими вірусами для поширення або для нанесення ушкоджень.

Особливості цього етапу полягає у тому що вірус додає правила у систему, тим самим дозволяючи системі завантажувати іншу частину вірусу у фоновому режимі. Завдяки цьому, вірус потрапляє у систему, оминаючи антивірусні програми.

Вірус вносить себе у виключення брандмауера, дозволяючи запуски свого тіла програми, а також прилеглих частин вірусного коду без відома користувача, та встановлювати інші програми.

Додає програму у автозавантаження, що дозволяє програмі поширюватись після перезавантаження системи, а також дає можливість поширення вірусного коду у інших мережах.

Після того як вірус виконав попередні шість етапів, він завантажує у весь код програми. Після цього всі ці етапи повторюють.

Межа у питаннях кібербезпеки між персональною, корпоративною і державною екосистемами стирається. Це зумовлено появою Bring Your Own Device, інтернету речей і соцмереж, в яких бізнес-дані у вигляді корпоративних сторінок і реклами поєднані з особистими профілями цільової аудиторії і

навпаки. Тому в кібербезпеці немає головних і другорядних завдань, усі головні. Згадайте вірус Petya.A, який нещодавно вразив чимало систем по всій Україні.

Кількість кібератак зростає, змінюються їхні цілі, це може бути як промислове шпигунство і блокування систем з метою шантажу, так і завдання репутаційного збитку і організація техногенних катастроф.

Раніше процес зараження був простий: програма – вірус – атака. Тепер такі спрощені ланцюжки не працюють, адже виробники систем захисту теж не сидять склавши руки. Нині використовують ланцюжки подій (вразливість – часткове інфікування – завантаження основного тіла вірусу з зовнішнього ресурсу – розпакування – атака – знищення слідів), які засновані на невиконанні базових дисциплін інформаційної безпеки у компаніях і слабостях людини.

Саме тому йдеться не про захист бізнесу від вірусів, а про комплексний підхід щодо захисту компанії від зловмисників. Це означає роботу за трьома напрямками, а саме: люди, процеси, системи.

Можна порадити десятки варіантів захисту, проте існують основні правила поведінки, які убезпечать військовий кібернетичний захист .

Системи:

- розділіть персональні та військові системи;
- завжди встановлюйте останні версії оновлень операційних систем;
- налаштуйте системи таким чином, щоб паролі користувачів і адміністраторів змінювалися не рідше одного разу на 60 днів і були складними.

Люди:

- використовуйте привілеї адміністраторів у системах за потреби, а не коли зручно;
- не користуйтеся знайденими або чужими флешками і не відкривайте підозрілі листи;
- дотримуйтеся інформаційної гігієни у соцмережах.

Процеси:

- резервуйте дані і регулярно тестуйте їх на відновлення;
- розробіть альтернативні процедури роботи компанії;

Традиційних підходів кібербезпеки уже недостатньо для повноцінного захисту від загроз, тому варто не лише забезпечувати якісний захист, а й швидке відновлення систем і їхніх даних.

Значні потужні за обсягом відеозображення, велика кількість кольорових компонент та глибина цифрового опису пікселей критично перевищує

потенціал з його передачі в телекомунікаційних мережах. Для передачі відеоданих в доступні часових межах проводиться його стиснення.

Стиснення є знаючим та впливає на обґрунтування стратегії стеганореалізації. Стиснення з втратами в результаті дає менший розмір файлу. Однак така обробка збільшує ймовірність того, що вбудоване повідомлення може бути частково втрачено. На це впливає процес усунення надлишковості в тому числі надлишковості візуального характеру. Навпаки стиснення без втрат дозволяє зберегти досторвінсть цифрового відео-зображення. Але в такому разі рівень зменшення обсягу буде незначним. Процес стиснення за схемою JPEG включає ряд етапів :

- Перетворення зображення в оптимальний колірний простір. - Децимація компонентів кольоровості усередненням груп пікселів. - Застосування дискретних косинус-перетворень (ДКП) для зменшення надлишковості даних зображення.

- Квантування кожного блоку коефіцієнтів ДКП із застосуванням вагових функцій, оптимізованих з урахуванням візуального сприйняття людиною. - Кодування результуючих коефіцієнтів (даних зображення) із застосуванням алгоритму Хаффмена для видалення надмірності інформації. При цьому хотілося б звернути увагу на те, що декодування JPEG здійснюється у зворотному порядку.

3.2 Розробка комбінованого методу маскування вірусних атак в інформаційно-мережевому просторі профільних структур

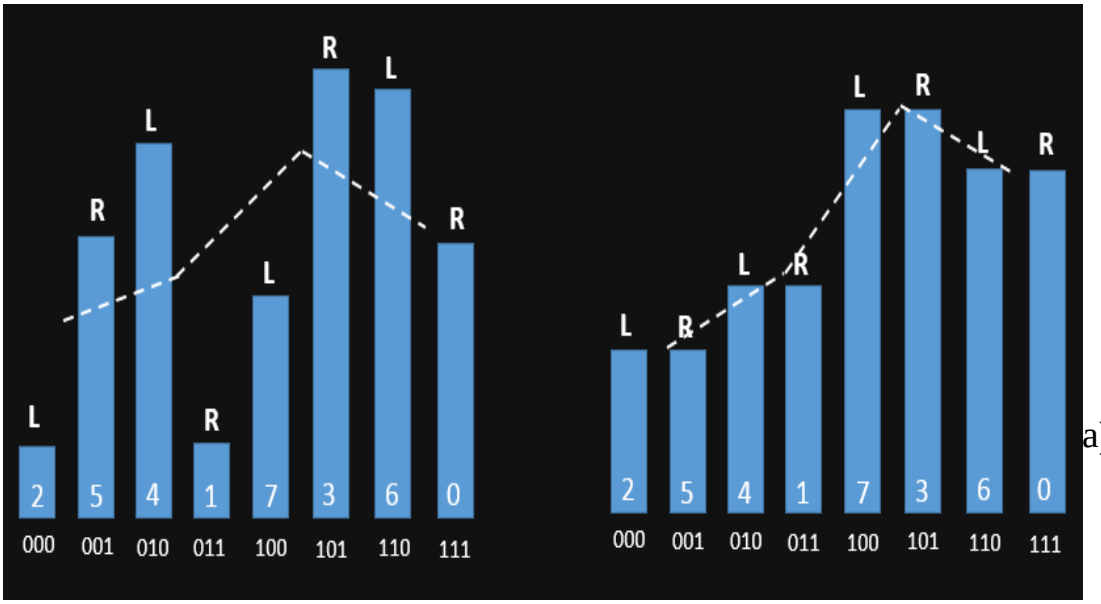
Математичні основи шифру. Для опису алгоритму GF використовується кінцеве поле Галуа ногочленами форми

$$b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0 \qquad (3.7)$$

Ступінь менше 8, а коефіцієнти. Операції в полі виконуються за модулем m (x). Всього , в поле GF(2^8) читає $2^8 = 2562^8 = 256$поліноми .

Другий спосіб, який я використовую, це криптографічне шифрування MD5, оскільки воно більш стиснуто.

Весь растр аналізується , для кожного кольору це кількість точок цього кольору в растре (для простоти ми говоримо про зображення, яке має одну кольорову площину). Метод передбачає, що кількість точок двох сусідніх кольорів суттєво відрізняється для нормального, нормального зображення (порожній контейнер) (рис. 3.3 а). І кількість пікселів таких кольорів приблизно однакова для заповненого контейнера



а) пустий контейнер

б) заповнений контейнер

Рисунок 3.3 – Графіки використання пам’яті у контейнері

На рисунку 3.3 було продемонстровано граф де вказується як змінюється контейнер якщо в нього вписати інформацію, як видно з рисунку пустий контейнер більш хаотичний коли заповнений контейнер вже більш лінійний.

- Теоретично очікувана частота пікселів кольору і після введення повідомлення розраховується наступним чином :

$$n_i^* = \frac{\left|\{colour | sortedIndexOf(colour) \in \{2i, 2i+1\}\}\right|}{2} \quad (3.8)$$

- Виміряна частота виникнення символу певного кольору визначається як:

$$n_i = |\{colour | sortedIndexOf(colour) = 2i\}| \quad (3.9)$$

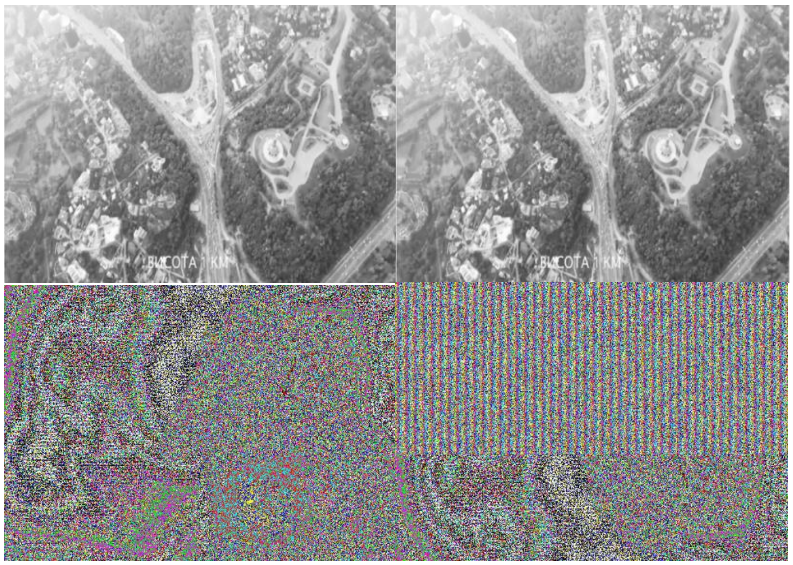
Критерій квадрату за кількістю ступенів свободи k-1 обчислюється наступним чином:

$$x_{k-1}^2 = \sum_{i=1}^{k} \frac{(n_i - n_i^*)^2}{n_i^*} \quad (3.10)$$

Пороги розподілу Чи-квадрати для p = 0,95 і p = 0,99 складають 101,9705929 та 92,88655838, відповідно. Таким чином, для зон, де розраховане значення Чі-квадрата є меншим, ніж порогове значення, ми можемо

прийняти початкову гіпотезу "розподіл частот сусідніх кольорів однаковий, тому він є заповненим стерегоконтами".

Дійсно, якщо ви дивитеся на зображення для візуальної атаки, легко помітити, що ці області містять вбудоване повідомлення. Таким чином, для вбудованих повідомлень з високою ентропією метод працює. Щоб боротися з цією загрозою, можна скористатись стисненням зображення, а точніше скористатися тим, що змінює код програми, для цього я використовую алгоритм стиснення Deflate. Алгоритм даних використовується для стиснення файлів PNG.



Оригінальне зображення Візуальна атака

Рис. 3.4 – Зображення до впровадження інформації (зверху) і після (знизу)

3.3 Розробка адаптивного методу забезпечення кібернетичного захисту в інформаційно-мережевому просторі профільних структур

Для ефективної боротьби з вірусами у зображеннях та у відео-потоці треба спочатку зрозуміти як завантажуйтеся інформація туди. Інформацію записують у останні 2 біта кольору (в кольорі Jpeg використовуються 8 біт), як ви можете бачити а точніше ви не бачите різниці між даними зображеннями, на рисунку 1а зображений квадрат к якому значення кольору 255, на рисунку 1б зображений це же квадрат але зі значенням кольору 254, на рисунку 1в зображено зі значенням 253.

а) б) в)

Рис. 3.5 – Кольори в інтервалі від 253 до 255 біт

Тим самим завдяки одному пікселю ми можемо перенести 2 біта інформації не змінюючи картинку. В сучасному світі ця наука називатися стеганографіею, її почали використовувати для переносів комп'ютерних вірусів. Щоб побороти дану систему пропонується використовувати наступну формулу :

$$n^* = \frac{1+(-1)^{n-a}}{2} \quad (3.11)$$

n^*= біт інформації

n = номер кроку

a = одиниця (1) чи нуль (0) в останніх 3 бітах інформації кольору

Дана методика дає змогу захиститись від вірусів але є і недоліки, наприклад ми не зможемо приймати таємне повідомлення завдяки стеганографії. Після проходження циклів з застосуванням цієї формули майже не можливо відновити повідомлення.

В якості інформаційної середовища існуючі інформаційних систем (ІС), як правило, використовують глобальні телекомунікаційні мережі (наприклад, Інтернет), що об'єднують інформаційні мережі локального і корпоративного рівня [1, Оліфер В. Р., Оліфер Н. А. Основи мереж передачі даних. Інтернет-університет інформаційних технологій.] Аналогія в архітектурі ІС найбільш повно проявляється в наявності ієрархічної організації рівнів глобальних інформаційних середовищ.

Біосистема аналогія в структурі захисту ІВ базується на ієрархії засобів забезпечення інформаційної безпеки (ІБ), вбудованих механізмах імунного захисту с накопиченням досвіду.

Відомі засоби захисту, як правило, обмежуються реалізацією функцій нижнього рівня системи інформаційної безпеки (СІБ) і антивірусної спрямованістю засобів імунного захисту. Згідно [3] , близько 70 % вірусних атак здійснюється ззовні через точку входу в захищається мережу і тільки близько 30% - зсередини. Перші можна віднести до зовнішніх загроз життєзабезпеченню системи, другі — до внутрішніх.

Засоби захисту рівня поштових шлюзів і міжмережевих екранів більшою мірою орієнтовані на виявлення зовнішніх атак, а засоби захисту серверного рівня — на нейтралізацію внутрішніх загроз в корпоративній системі. Відомі інтелектуальні засоби захисту, як правило, реалізують тільки механізми оперативної реакції і нейтралізації загроз, практично не приділяючи уваги координуючої ролі, яку відіграє нервова система — верхній рівень ієрархії захисту біологічних систем у реалізації еволюційного процесу накопичення життєвого досвіду системи (довготривалого запам'ятовування системної інформації). В біосистемах мають місце процеси поступової адаптації ієрархіч-

ної системи життєзабезпечення та захисту з використанням усього арсеналу засобів еволюційних процесів.

В ІС крім імунного рівня засобів захисту необхідно наявність ієрархії рівнів захисту, і насамперед — верхніх (наприклад, рецепторного рівня захисту), які виконують функції нервової системи організму з накопичення життєвого досвіду, координації та встановлення асоціативних (довготривалих) зв'язків між процесами, що відбуваються на нижніх рівнях засобів захисту, — атаками і зміною безлічі загроз. Таким чином, необхідний ієрархічний рівень накопичення життєвого досвіду з нейтралізації атак, представленого у формі структурованих інформаційних полів, зручних для успадкування в наступних реалізаціях системи.

Біосистемна аналогія в програмуванні ІС реалізується шляхом формування і корекції розподілених надлишкових інформаційних полів НС, що відносяться до ієрархічної системи засобів захисту. Структурована програма, подібно потоковим машин [8] описує топологію взаємопов'язаних компонентів, що забезпечує:

— універсальний характер опису взаємозв'язку безлічі відомих загроз і використовуваних механізмів захисту (МЗ) у вигляді системи предикатних правил та інформаційних полів НС;

— автоматичну корекцію інформаційних полів НС в процесі адаптації ІВ до зміни безлічі загроз або умов експлуатації;

— успадкування досвіду щодо нейтралізації загроз шляхом перенесення структурованих інформаційних полів НС в наступні модифікації ІС.

Метод проектування адаптивних засобів захисту ІВ базується на основних властивостях НС та нечітких систем, пов'язаних з адаптивністю, можливістю представлення досвіду фахівців ІБ у вигляді системи нечітких правил.

Можливість навчання розглядається як одна з найбільш важливих якостей нейромережевих систем, яка дозволяє адаптуватися до зміни вхідної інформації. Навчальними факторами є надмірність інформації і приховані закономірності, які видозмінюють інформаційне поле НС в процесі адаптації. НС, зменшуючи ступінь надлишковості вхідної інформації, що дозволяє виділяти в даних істотні ознаки, а змагальні методи навчання — класифікувати інформацію, що надходить з допомогою механізму кластеризації: подібні вектори вхідних даних групуються нейронною мережею в окремий кластер і представляються конкретним формальним нейроном. НС, здійснюючи кластеризацію даних, знаходить такі усереднені по кластеру значення функціональних параметрів, які мінімізують помилку подання згрупованих у кластер даних.

Модель адаптивного захисту і етапи життєвого циклу ІС. Метою етапів проектування з урахуванням життєвого циклу ІВ є формування коректної (без несанкціонованих можливостей) безпечної ІС. На початковому етапі життєвого циклу відповідно до вимог специфікації на проектування ІВ здійснюється формування ІВ та засобів захисту із заданою сукупністю властивос-

тей. Для реалізації функцій засобів захисту, що відповідають системі нечітких предикатних правил (наприклад, для класифікації механізмів захисту), формуються адаптивні інформаційні поля адаптивних рівнів захисту прикладної ІС. Проводиться перед експлуатаційне навчання нейро-нечітких нейромережевих класифікаторів і кластеризаторов із застосуванням коректних алгоритмів, тобто виконується адаптація інформаційних полів НС під завдання інформаційного захисту.

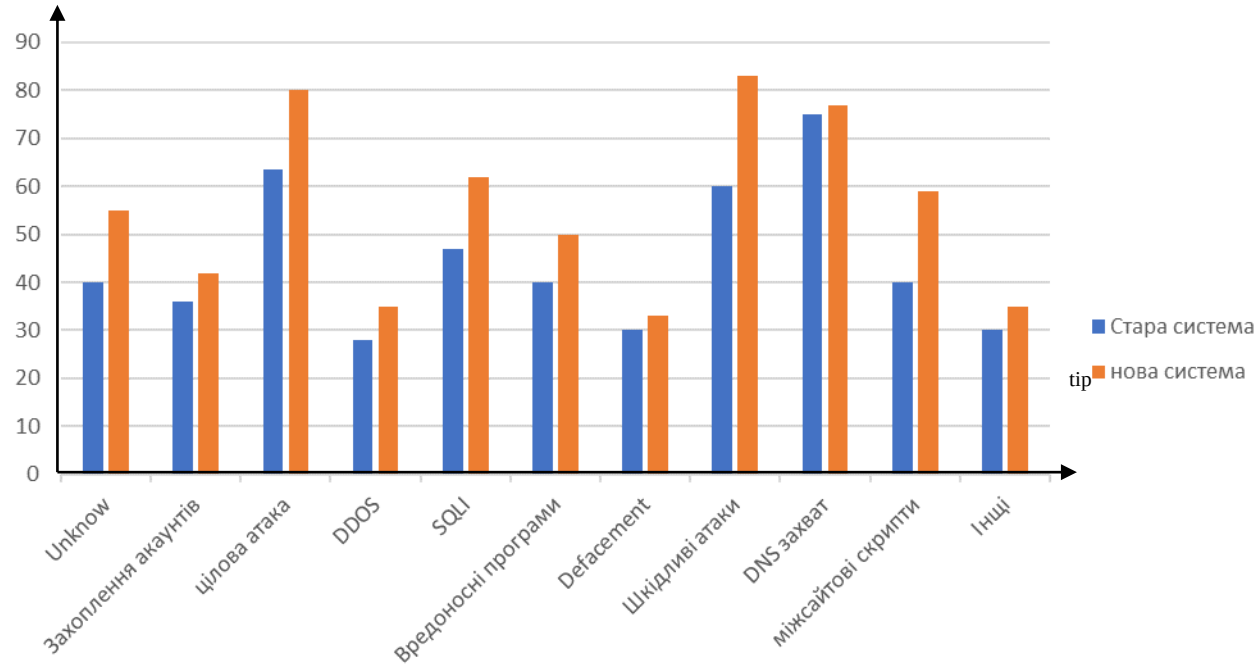


Рисунок 3.6 – Гістограма ефективності старої і нового методу захисту інформації в інформаційно-телекомунікаційної мережі світу

Процеси налаштування (навчання) відбуваються в режимі адаптації системи при безпосередній участі і під контролем довірених осіб, зокрема, адміністратора ІВ. Процес налаштування завершується блокуванням режиму адаптації і перекладом сформованої системи в режим роботи. Як можливо побачити на рисунку 3.8 в середньому піднялась ефективність боротьби з вірусними атаками в інформаційно-телекомунікаційної мережі різного типу на 15 %, найбільш захищена система від цільових атак та шкідливих атак на систему, що позволить бути біль спокійним за безпеку інформації що зберігаються на серверах

Багаторівнева модель інформаційної безпеки системи на першому етапі відповідає мінімальній активації потенційних механізмів захисту та повноти інформаційного безлічі відомих загроз. Метою етапу експлуатації життєвого циклу системи є коректне виконання системою заданих функцій. Передбачений режим адаптації функцій системи захисту інформації, який використовує механізм адаптації для реагування на зміну зовнішніх факторів відбуваються подальше зростання, самонавчання системи і зміна інформаційних полів засобів захисту. Як і на попередньому етапі, процеси корекції функцій засобів захисту відбуваються в режимі адаптації системи при безпосередній участі

адміністратора ІС. Процес налаштування завершується блокуванням режиму адаптації і переведенням системи в режим роботи. Багаторівнева модель адаптивної засобів захисту на другому етапі динамічно поповнюється шляхом переведення механізмів захисту зі статусу „потенційний“ в статус „активований“ і прив'язки активованого механізму до відповідного ешелону моделі засобів захисту. Збільшується число елементів на підмножині заданих загроз як за рахунок включення елементів з множини відомих загроз, так і за рахунок поповнення самого безлічі відомих загроз раніше невідомими погрозами.

Метою етапу виведення системи з експлуатації є поступове згортання прикладних функцій системи при коректній роботі засобів захисту і збереження основних системних функцій.

Багаторівневої моделі інформаційної безпеки ІС притаманні наявність максимальної кількості механізмів захисту і повнота інформаційного поля відомих загроз. Накопичений досвід засобів захисту підлягає аналізу і використанню (спадкування) в створюваних прикладних системах.

Висновки до розділу 3

В розділі 3 було розглянуто адаптивний та комбінований метод маскування даних за для того щоб потім протидіяти вірусним атакам у спеціальних телекомунікаційних системах. Створено новий метод протидії зашифровуваним та замаскованим тілам вірусів у відео-потоці завдяки зміні останніх бітів інформації кольору. Запропоновано створення єдиної системи антивірусної протидії та створення нейронної мережі за для швидкої та адаптивної протидії вірусним атакам в умовах реального часу.

ПЕРЕЛІК ПОСИЛАНЬ

1. Коваленко М. М. Комп"ютерні віруси і захист інформації.- К: Наукова думка, 2010.- 268с.
2. Жигун Т.Ю. Законодавчі та нормативні документи України у сфері інформації, видавничої та бібліотечної справи: Тематична добірка: У 2-х ч. Ч. 1. Правове регулювання у сфері інформації/ У- 2-ге вид., доп.- К.: Книжкова палата України, 2012.- 124с.
3. Кулик А. Я. Адаптивні алгоритми передавання інформації: Монографія.- Вінниця: Універсум, 2013.- 214с.
4. Безруков Н.Н. Компьютерная вирусология: Справ. руководство. К.: УРЕ, 2015. 416 с.
5. Бакаревич Ю.Б., Антивірусні програми для комп'ютерів. Пушкіна Н.В. — К.: 2012. — 295с.
6. Венц К., Як уберегти комп'ютер від вірусів Хаузер Т. – К.: Пресс, 2011. – 230с.
7. Девид Хеллер, Сучасний самовчитель професійної роботи на комп'ютері. Дороті Хеллер — К.: BHV, 2010. — 550с.
8. Дьяконов В. Домашній комп'ютер: Комп'ютерні віруси і антивірусні програми. — К.: 2010. — 275с.
9. Екслер А. Антивірусні програми для вашого ПК. – К.: Пресс, 2017. – 265с.
10. Каратигін С.А. Антивірусні програми для вашого ПК. — К.: Кн. компанія, 2013. — 298с.
11. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. — К.: “МК-Пресс”, 2012. — 288 с.
12. Мао В. Современная криптография. Теория и практика. - К.: «Вильямс», 2009. - 768с.
13. Бараннік В.В. Теоретичні основи створення технологій протидії прихованим інформаційним атакам в сучасній гібридній війні [Текст]/ В.В.Бараннік, Т.В.

Белікова, С.О. Сідченко. – Х. : ХНУПС Наука і техніка Повітряних Сил Збройних Сил України, 2017. – 133 с.

14. Беликова Т.В. Методы выявления деструктивных суггестивных информационно-психологических операций в информационно-социальном пространстве [Текст]/ Т.В. Беликова // Радиоэлектроника и информатика. – 2016. – № 3. – С. 62-68.
15. Белікова Т.В. Технологія маскування сугестивних інформаційно-психологічних операцій в інфокомунікаційному просторі // Наукові технології. 36, с. 267-271, лип.
16. Ю.О. Кулаков, Г.М. Луцький Комп'ютерні мережі. Підручник за ред. Ю.С. Ковтанюка – К.: Юніор, 2013. – 400 с.
17. В.Д. Руденко, О.М. Макарчук, М.О. Патланжоглу Практичний курс інформатики / За ред. Мадзігона В.М. – К.: Фенікс, 2011. – 370 с.