МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Одеський національний технологічний університет
Університет Інформатики і прикладних знань, м.Лодзь, Польща
Національний технічний університет України «Київський політехнічний інститут»
Навчально-науковий інститут комп'ютерних систем і технологій «Індустрія 4.0» ім. П.М. Платонова

XXII Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів

«СТАН, ДОСЯГНЕННЯ ТА ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ»

Матеріали конференції

Одеса

21-22 квітня 2022 р.

Стан, досягнення та перспективи інформаційних систем і технологій / Матеріали XXII Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів. Одеса, 21-22 квітня 2022 р**.** - Одеса, Видавництво ОНТУ, 2022 р. – 251 с.

Збірник включає матеріали доповідей учасників конференції, які об'єднані за тематичними напрямками конференції.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Голова - д.т.н., проф., **Єгоров Б.В.**, ректор ОНТУ

Співголови:

Поварова Н.М. – к.т.н., доц., проректор з наукової роботи ОНТУ,
Котлик С.В. – к.т.н., доц., директор ННІКСіТ "Індустрія 4.0" ОНТУ,
Даріуш Долива, д.математичн.наук, уповноважений декана факультету Інформатики УІтаПЗ, м.Лодзь, Польща,
Ковалюк Т.В. - к.т.н., доц., Київський національний університет імені Тараса Шевченка

Члени оргкомітету:

Плотніков В. М. – д.т.н., проф., завідувач кафедри ІТтаКБ ОНТУ,
Артеменко С.В. – д.т.н., проф., завідувач кафедри КІ ОНТУ,
Хобін В.А. – д.т.н., проф., завідувач кафедри АТПтаРС ОНТУ,
Тарасенко В.П. – д.т.н., проф., завідувач кафедри СКС НТУУ «Київський політехнічний інститут»,
Невлюдов І.Ш. – д.т.н., проф., завідувач кафедри КІТАМ ХНУРЕ,
Мельник А.О. – д.т.н., проф., завідувач кафедри ЕОМ НУ “Львівська політехніка”,
Жуков І.А. – д.т.н., проф., завідувач кафедри КСтаМ НАУ.

Матеріали подано українською та англійською мовами.
Редактор збірника Котлик С.В.

УДК 004.49

АНАЛІЗ ТА КЛАСИФІКАЦІЯ ШКІДЛИВИХ ПРОГРАМ

БОНДАРЕНКО В.Г., КРУШЕЛЬНИЦЬКА М.О.
Одеський національний технологічний університет

Стаття присвячена короткому опису методів проникнення у систему найпоширеніших видів шкідливого програмного забезпечення, аналізуються загрози.

Шкідливе програмне забезпечення є реальною загрозою, здатною паралізувати роботу різних організацій та завдати багатомільярдних збитків. Дослідження шкідливих програм з метою знаходження ефективних способів протидії їх впливу на заражені системи є не просто одним із напрямків розвитку інформаційних технологій, а справжньою необхідністю, що має вкрай високий пріоритет, адже зі зростанням значення комп'ютерів у житті суспільства зростає і потенційна небезпека, яку несуть різні шкідливі програми.

Більшість існуючих у світі шкідливих програм розрахована на ОС сімейства Windows. Друге місце займає ОС Android, в якій кількість заражень щороку збільшується експоненційно (смартфони дозволяють зловмисникам розсилати платні SMS-повідомлення, здійснювати дзвінки на різні комерційні номери, купувати підписки на ті чи інші віртуальні послуги, а якщо власник використовує системи мобільного банкінгу, просто знімати гроші з його рахунку). Третю позицію щодо кількості відомих загроз займають операційні системи сімейства Linux (це пов'язано з активним використанням даних систем на різних «розумних» пристроях). Четверте місце за поширеністю займає шкідливе програмне забезпечення для операційної системи Apple macOS.

Інші системні платформи мають набагато меншу в абсолютних значеннях число відомих загроз. Наприклад, за даними на 2020 рік, кількість шкідливих програм, розроблених під Apple iOS, не перевищує десяти [2].

Шкідливій програмі для віднесення до класу вірусів необхідно відповідати двом основним критеріям: мати здатність до самореплікації та вміння інфікувати файлові об'єкти. Можливість самореплікуватися (поширюватися в автоматичному режимі шляхом створення власних копій без участі користувача) мають ще й комп'ютерні черв'яки, проте вміння заражати файли характерно насамперед для вірусів. Під зараженням розуміється процес впровадження вірусу у файл виконуваного додатка (програми), у якому порушуються основні функціональні можливості даного докладання. При запуску такої програми автоматично запускається вірус [4]. Поліморфні віруси - це різновид вірусів, представники якого здатні змінювати свій код безпосередньо у процесі його виконання. Процедура, що здійснює динамічне виправлення коду вірусу, також може самостійно змінюватися при переході від одного зараженого пристрою до іншого. Найпростішим способом модифікації структури вірусу без зміни його функціоналу є додавання до нього різного «сміттєвого коду», до якого відносяться порожні цикли, порожні рядки тощо. Такі модифікації призводять до значного ускладнення процесу виявлення подібної шкідливої програми, тому практично всі сучасні віруси використовують ті чи інші поліморфні технології [4].

Стелс-віруси – віруси, здатні частково або повністю приховувати свою присутність на зараженому пристрої шляхом перехоплення системних запитів до інфікованих файлових об'єктів, пам'яті або завантажувальних областей диска та повернення недостовірної інформації, яка не дозволяє комп'ютеру виявити загрозу. В даний час цей термін застарів і подібні програми прийнято називати "руткіт" [4]. Макровіруси - різновид вірусів, що створюються за допомогою макромов, вбудованих в різні програми пакета Microsoft Office, і змінюють або замінюють макроси, що є послідовністю команд [3]. Резидентні віруси - віруси, що здійснюють свою діяльність у пам'яті зараженого пристрою паралельно з іншими активними програмами. Після запуску ці віруси або видаляли вихідний файл, або переміщали його в місця, недоступні операційній системі та користувачеві. З моменту появи

операційних систем, що мають багатозадачність, поняття «резидентного вірусу» застаріло, а шкідливе програмне забезпечення, що діє в оперативній пам'яті комп'ютера, стали називати загальним терміном «безфайлові шкідливі програми» [4].

Комп'ютерні черв'яки - різновид шкідливих програм, що мають здатність до самореплікації без можливості зараження файлових об'єктів (з цього правила є деякі винятки). У наші дні широко поширені так звані поштові черв'яки, що розсилають свої копії на всі поштові адреси, що є у списку контактів на інфікованому комп'ютері. Багато хробаків розповсюджуються за допомогою знімних носіїв інформації. Вони можуть розміщувати в кореневій папці накопичувача файл, що часто носить назву autorun.inf, що забезпечує автоматичний запуск черв'яка при кожному зверненні до накопичувача, або переміщати весь вміст знімного носія в приховану папку, заміщаючи її власною копією з такими ж назвами директорій та файлів, при натисканні на які запуститься шкідлива програма [2]. Троянські програми (троянці або трояни) - це широко поширений і найчисленніший тип шкідливого програмного забезпечення. Особливостями троянських програм є їхня нездатність до самореплікації та зараження файлів, а також те, що «жертва» самостійно запускає їх на своєму комп'ютері. Це відбувається через те, що троянці вміло маскуються під різні корисні програми, антивіруси, ігри та навіть прості текстові документи. Існує величезна кількість хитромудрих схем, за допомогою яких зловмисники змушують людину завантажити шкідливу програму, проте найчастіше вони обмежуються масовим розсиланням троянців у вигляді вкладень у поштові повідомлення та включенням їх у піратські та зламані комерційні програми [3].

Бекдори – це шкідливі програми, які відкривають зловмисникам повний доступ до інфікованого пристрою. До них відносять деякі види вірусів та троянців [1]. Буткіти - це віруси або троянські програми, здатні шляхом зараження завантажувального запису на диску комп'ютера запускатися раніше антивірусного програмного забезпечення, одночасно із запуском ОС або навіть перед ним. Це дає можливість перехоплювати управління операційною системою, цим паралізуючи запуск і нормальну роботу антивірусів і блокуючи можливість видалити буткіт з комп'ютера. Невдала спроба видалення такої програми може призвести до пошкодження логічної структури диска, що спричинить повну непрацездатність пристрою. Особлива небезпека буткітів полягає ще й у їх можливості отримати в системі максимальні привілеї, що дають доступ до файлової системи, компонентів ОС, пам'яті та драйверів [2]. Руткіти – це шкідливе програмне забезпечення, що спеціалізується на приховуванні своєї присутності в інфікованій операційній системі та протидії спробам його виявлення та видалення. Деякі руткіти спеціально розробляють з метою приховування на інфікованому пристрої інших шкідливих програм, тим самим створюючи зв'язку з шкідливого ПЗ, що «впливає» і «прикриває» [2]. Біоскіти - це тип шкідливого ПЗ, що має здатність змінювати вміст мікросхем BIOS. Наприклад, кілька сотень тисяч комп'ютерів посилають запити з інтервалом у кілька мікросекунд, завантажуючи сервер вщент. Даний вид атак зветься «атака на відмову в обслуговуванні» — «Distributed Denial of Service» (DDoS-атака).

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. Масалков, А. С. Особливості кіберзлочинів: інструменти нападу та захисту інформації / А. С. Масалков. - М: ДМК Прес, 2018. - 226 с. - Текст: безпосередній.

2. Холмогоров, В. PRO Віруси/В. Холмогоров. - 4. - СПб.: Страта, 2020. - 224 с. - Текст: безпосередній.

3. Козлов, Д. А. Енциклопедія комп'ютерних вірусів / Д. А. Козлов, А. А. Парандовський, А. К. Парандовський. - М: СОЛОН-Р, 2001. - 464 с. - Текст: безпосередній.

4. Гошко, З. У. Технології боротьби з комп'ютерними вірусами. Практичний посібник. / С. В. Гошка. - М: СОЛОН-ПРЕС, 2009. - 352 с. - Текст: безпосередній.

XXII Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів

«СТАН, ДОСЯГНЕННЯ ТА ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ»

Одеса

21-22 квітня 2022 р

Збірник включає доповіді учасників конференції. Тези доповідей публікуються у вигляді, в якому вони були подані авторами.

Відповідальність за зміст і форму подачі матеріалу несуть автори статей.

Редакційна колегія: Котлик С.В., Корнієнко Ю.К.

Комп'ютерний набір і верстка: Соколова О.П.

Відповідальний за випуск: Котлик С.В.