УДК 004.9

КЛАСИФІКАЦІЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ОСНОВНІ МЕТОДИ ЗАХИСТУ

Б. М. Гавриш[1], О. В. Тимченко[2,3,] Ю. О.Борзов[4], А. Т. Кобевко[2]
[1] Національний університет «Львівська Політехніка»
[2] Українська академія друкарства
[3] Університет Вармінсько-Мазурський в Ольштині
[4] Львівський державний університет безпеки життєдіяльності

У статті описуються способи проникнення та впливу на комп'ютерну систему найпоширеніших видів шкідливого програмного забезпечення, розглядається кілька підходів до класифікації загроз, зокрема щодо шкідливості програмного забезпечення та рівня небезпеки. Дано приклади нанесення шкоди окремих видів вірусів та нанесених втрат. Проведена формальна класифікація шкідливих програм. Зазначено, що більшість існуючих у світі шкідливих програм розрахована на ОС сімейства Windows, наступне місце посідає ОС Android. Мінімальна кількість шкідливих програм, а значить і найвища захищеність, існує для Apple iOS Запропонована ієрархія шкідливого програмного забезпечення за ступенем небезпеки. Також розглядається основні методи боротьби, які використовуються сучасними антивірусними програмами: сигнатурне детектування загроз, поведінковий шаблон, проактивний антивірусний захист, евристичний аналіз.

Ключові слова: *шкідливе програмне забезпечення, вірус, комп'ютерний черв'як, троянська програма, антивірусна програма, детектування сигнатурне, поведінковий аналіз, проактивний захист.*

Постановка проблеми. Сьогодні суспільство не може нормально функціонувати без використання електронно-обчислювальних машин, оскільки майже всі сфери діяльності людини пов'язані з інформацією, що зберігається на них. Управління різними електронними пристроями, персональні дані, найважливіші документи, величезні кошти та багато іншого — доступ до цього здійснюється за допомогою безперервних процесів передачі та обробки інформації, отже, шкідливе програмне забезпечення є реальною загрозою, здатною паралізувати роботу різних організацій і 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, яка має вкрай високий пріоритет, адже зі зростанням значення комп'ютерів у житті суспільства зростає і потенційна небезпека через різні шкідливі програми.

Аналіз останніх досліджень та публікацій. Виконані дослідження з цієї тематики присвячені формалізованому опису видів комп'ютерних вірусів [1], шкідливості окремих видів вірусів [2–3], методик виявлення шкідливого ПЗ [4]. Проте не створена ієрархія шкідливого програмного забезпечення за ступенем небезпеки та класифікація за шкідливими функціями.

Мета статті. Метою статті є опис та класифікація загроз шкідливого програмного забезпечення, створення ієрархії загроз за ступенем небезпеки, визначення методів, які використовують сучасні антивірусні програми.

Класифікація шкідливого програмного забезпечення. До цього часу не була розроблена універсальна система класифікації шкідливого програмного забезпечення, а багато великих антивірусних компаній використовують свої власні методи розпізнавання та розбиття загроз на різні класи, проте, незважаючи на це, існують певні способи, що історично склалися, що дозволяють досягти у цьому питанні деякої спільності.

Одним із таких способів, що володіє мінімальною точністю, є класифікація на кшталт операційної системи, пристрої під керуванням якої заражає вірус. Більшість наявних у світі шкідливих програм розраховані на ОС сімейства Windows. Друге місце посідає ОС Android, в якій кількість заражень щорічно 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 цих систем на різних «розумних» пристроях). Четверте місце за поширеністю займає шкідливе програмне забезпечення для операційної системи Apple macOS. Інші системні платформи мають набагато менше в абсолютних значеннях число відомих загроз. Наприклад, за даними на 2020 рік, кількість шкідливих програм, розроблених під Apple iOS, не перевищує десяти [3].

Приклади шкідливості комп'ютерних вірусів. Наприкінці 1990-х і на початку 2000-х років загрози, пов'язані з вірусами, не були такі відомі, як зараз.

MyDoom атакував офіси в США в 2004 році завдяки стимулам за клік-лінк. Комп'ютерний хробак подорожував мережею і з'єднувався з 50 найближчими контактами зі списку поштової скриньки, щоб надіслати копії свого коду. Вважається одним з найбільш швидкозростаючих вірусів. За перші три години 1 з 10 електронних листів, надісланих в США, містив заражене програмне забезпечення, а збитки, які воно завдало, становлять близько 38 мільярдів доларів.

Є сайти, де зловмисне програмне забезпечення легко отримати, і вміст, який заохочує користувачів натискати призначені їм посилання. У 1999 році Девід Лі Сміт скористався цим, опублікувавши файл під назвою «alt.sex» на загальнодоступному форумі. Передбачалося, що в документі були паролі до безкоштовних сайтів для дорослих, але насправді там ховався комп'ютерний вірус ***Melissa***. Коли файл було відкрито в Microsoft Word, макровірус поширювався, надсилаючи свої копії контактам Outlook. Через перевантаження довелося вимкнути сервери поштових скриньок у багатьох великих підприємствах, включаючи Microsoft.

Iloveyou з'явився через рік після Melissa і в той час вважався вірусом, який швидко розвивався. Його створив на Філіппінах 23-річний хлопець. Вірус кохання, коли відкривали вкладення, розмножувався і надсилав свої копії людям зі списку контактів жертви. Файли на комп'ютері були замінені зараженими, і нарешті вірус крав паролі пристрою та відправляв їх на сервер на Філіппінах.

Slammer, також відомий як ***Sapphire***, атакував у 2001 році і націлився на найбільші сервери у світі. Ефект був помітний не лише в Інтернеті, а й в установах, розташованих по всьому світу. Банкомати американського банку були заблоковані, штаб-квартира Seattle 911 була змушена припинити свою роботу, багато рейсів було скасовано.

Clop Ransomware. За створення вірусу відповідає хакерська група Clop. Програмне забезпечення було вперше виявлено Майклом Гіллеспі в лютому 2019 року. Основна мета програми-вимагача Clop – шифрувати всі файли на пристрої (або пристроях) компанії та вимагати плату за доступ до пристрою розшифровки, що дозволить йому повернутися до стану, в якому він був до атаки. Додає розширення "Clop" до кожного файлу Clop. Наприклад, він перетворить текстовий файл з назвою "report.docx" в "report.docx.Clop". Нарешті, вірус залишає текстовий файл "ClopReadMe.txt" з інформацією про атаку та вимоги викупу в кожній наявній папці.

Перш ніж Clop почне шифрувати, він усуває всі потенційні перешкоди. Він вимикає всі ключові програми Windows, включаючи Microsoft Security Essentials і Windows Defender, а також блокує багато системних процесів.

У 2022 році компанія ExecuPharm, що належить американському фармацевтичному концерну Paraxel, з'ясувала, наскільки небезпечним може бути програмне забезпечення-вимагач Clop. У цьому випадку хакери не тільки зашифрували дані та вимагали плату за ключі дешифрування, але й оприлюднили персональні дані співробітників ExecuPharm та деяких співробітників Parexel.

Cryptojacking. Зрештою, навіщо інвестувати в дорогі та енергоємні системи, коли можна майнити криптовалюти на комп'ютерах інших користувачів? І ось з'являється програмне забезпечення для криптоджекінга, яке, ймовірно, без вашого відома, можливо, зараз копіює біткойн для когось на вашому комп'ютері чи смартфоні, а ви скаржитеся, що погані виробники штучно знижують продуктивність пристроїв, щоб люди купували нові.

GoBrut. Це один з найновіших комп'ютерних вірусів, який постійно вдосконалюється додатковим кодом, що ускладнює боротьбу з ним. Він не надто технічно просунутий, але дуже ефективний при зламі паролів. Також може помітно уповільнити роботу Інтернету та пошкодити комп'ютер. Він поширюється неймовірно швидко, вражаючи пристрої Windows та Linux.

На жаль, кількість найнебезпечніших вірусів, що атакують комп'ютери, досить багато. Щороку їхні творці придумують нові більш сміливі рішення, які наражають людей на небезпеку.

Класифікація шкідливих програм. Формальні ознаки.

Найбільш поширеною та логічно точною є класифікація шкідливих програм за низкою формальних ознак, що визначають їх шкідливі функції.

Віруси. Шкідливій програмі для зарахування її до класу вірусів необхідно відповідати двом основним критеріям: мати здатність до самореплікації та вміння інфікувати файлові об'єкти. Можливість самореплікуватися (розповсюджуватися 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 цього додатку. При запуску такої програми автоматично запускається вірус [5].

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 належать 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 [5].

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. Сьогодні цей термін застарів, і подібні грами прийнято називати «руткітами» [5].

Макровіруси — різновид вірусів, що створюється за допомогою макросів, вбудованих в різні додатки пакета Microsoft Office, і змінюють або заміняють макроси, що є послідовністю команд [4].

Резидентні віруси — віруси, які 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» [5].

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, які 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 називається 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 і файлів, при натисканні на які запуститься шкідлива програма [3].

Троянські програми (троянці чи трояни) — це широко поширений і найчисельніший 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 до піратських та зламаних комерційних програм [4].

Бекдори – це шкідливі програми, які відкривають зловмисникам повний доступ до інфікованого пристрою. До них зараховують деякі види вірусів та троянців [2].

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, тим самим 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 [3].

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 шкідливим ПЗ, що «впливає» і «прикриває» [3].

Біоскіти — це тип шкідливого ПЗ, що має здатність змінювати вміст мікросхем BIOS. Нині вони практично не зустрічаються, останнє виявлення подібної програми, що отримала назву Trojan.Bioskit.1, відбулося в 2011 році, тому серйозної загрози не несуть [3].

Боти — шкідливі програми, особливістю яких є можливість об'єднання в ботнети. Ботнети є дистанційно керованими з використанням командних серверів мережі, що складаються з інфікованих пристроїв, призначенням яких є здійснення централізованих атак на сервери різних сайтів мережі Інтернет. Наприклад, кілька сотень тисяч комп'ютерів посилають запити з інтервалом у кілька мікросекунд, завантажуючи сервер вщент. Цей вид атак зветься «атака на відмову в обслуговуванні» — «Distributed Denial of Service» (DDoS-атака). Інший приклад — масове розсилання спаму мільйонами комп'ютерів, що входять до спамерської бот-мережі. Деякі роботи в разі потреби здатні динамічно налаштовувати свою приналежність до того чи іншого командного сервера, а інші — зовсім обходитися без такого, формуючи децентралізовані

P2P-мережі, тим самим багаторазово ускладнюючи завдання виявлення та ліквідації таких мереж [3].

Шпигуни — даний тип шкідливого ПЗ призначений для стеження за користувачем та передачі інформації, що отримується з його пристрою. Шпигунське програмне забезпечення нині досить поширене, а значна його частина реалізована як класичні троянці. Найбільш поширеними видами програм-шпигунів є кейлогери (додатки, що реєструють і запам'ятовують коди клавіш, що натискаються користувачем), грабери (фіксують не всі натискання клавіш, а тільки ті, що цікавлять зловмисника, наприклад, паролі від різних акаунтів), троянці комп'ютера та програми-шпигуни, орієнтовані на ОС Android, які можуть відстежувати місцезнаходження інфікованого пристрою, переглядати журнал дзвінків, особисті дані, а також вести фото- та відеозйомку [3].

Приклад класифікації за шкідливими функціями наведено рисунку 1.

Рисунок 1 Класифікація за шкідливими функціями

Класифікації шкідливих програм за рівнем небезпеки. Нині багатьма антивірусними компаніями використовується принцип класифікації за рівнем небезпеки. Цей спосіб схожий з попереднім, проте його основною відмінністю є розбиття на класи не за набором шкідливих функцій, реалізованих у програмі, а за сукупним рівнем загрози, яку вона представляє системі. У даному способі класифікації використовується деяка шкала небезпеки, що встановлює ієрархію серед різних видів загроз, на вершині якої, як правило, розташовані файлові віруси та черв'яки (рис. 2).

Рисунок 2 Ієрархія шкідливого програмного забезпечення за ступенем небезпеки

Цей спосіб класифікації найбільш поширений через те, що більшість шкідливих програм, що з'являються, поєднують в собі функціонал, що належить одночасно до кількох класів загроз. У такому разі фахівець, керуючись описаною раніше ієрархією, відокремлює другорядні за рівнем небезпеки ознаки від першорядних і зараховує зразок до класу, ступінь небезпеки якого є найвищим, не забуваючи при цьому доповнити опис шкідливої програми ознаками інших класів [3].

Класифікація антивірусного забезпечення. З другої половини 80-х років почалося змагання між творцями шкідливого програмного забезпечення та розробниками антивірусних програм, яке продовжується і нині.

Саме поняття «антивірус» стосовно сучасних додатків такого роду є скоріше даниною моді, аніж відображає суть терміна, оскільки класичні віруси, що заражають файли, що виконуються, в наш час практично не зустрічаються.

Сучасні антивірусні програми складаються з великої кількості модулів, що володіють різним функціоналом і забезпечують всебічний захист пристрою, проте набір таких модулів, присутніх в тій чи іншій програмі, обмежений і залежить від її орієнтації на різні сегменти ринку.

Антивірусний сканер — компонент, призначений для пошуку загроз в оперативному і постійному пристрої комп'ютера, що запам'ятовують за бажанням користувача або за заздалегідь складеним графіком.

Резидентний монітор — модуль, що в реальному часі здійснює аналіз стану системи з метою запобігання діяльності шкідливих програм на пристрої.

Антируткіт — компонент, призначений для боротьби з руткітами.

Модуль превентивного захисту — модуль, що відповідає за збереження найважливіших для функціонування системи даних і блокує загрози до заподіяння ними серйозної шкоди пристрою.

Карантин — деяка захищена область пам'яті, що використовується антивірусом для перевірки всіх підозрілих файлів шляхом поміщення їх в цю область і спостереження за їх подальшими діями.

Брандмауер (файєрвол) — модуль, що виконує аналіз інтернет-з'єднання, перевіряє адреси відправника та одержувача кожного пакета даних, а також фільтрує дані, отримані комп'ютером без попереднього запиту. Цей компонент є свого роду фільтром, що регулює обмін інформацією між захищеним пристроєм та іншою мережею Інтернет.

Вебантивірус — модуль, що обмежує користувачеві доступ до сайтів, визнаних небезпечними та занесеними до спеціальних баз даних у зв'язку з можливістю фішингових атак або вмістом на них шкідливого програмного забезпечення.

Поштовий антивірус — компонент, основним завданням якого є пошук потенційно небезпечних посилань та вкладень, що надсилаються електронною поштою.

Модуль оновлення — компонент, який слідкує за виходом оновлень для інших модулів програми та забезпечує актуалізацію інформації відповідно до змін у вірусних базах.

Перераховані вище модулі є основними і найбільш поширеними, проте антивірусні програми також можуть містити безліч інших більш спеціалізованих компонентів, присутність або відсутність яких обумовлюється призначенням і версією самої програми [3].

Методи виявлення шкідливого ПЗ. Виявлення шкідливих програм сучасними антивірусними програмами здійснюється шляхом комбінування декількох різних методик, головною з яких є сигнатурне детектування загроз. Цей метод ґрунтується на створенні сигнатур шкідливих програм — унікальних цифрових ідентифікаторів файлу, одержуваних на основі вмісту досліджуваного файлу, які є спеціальним набором байтів. Сигнатуру можна порівняти з «відбитком пальців», властивим лише одному конкретному файлу, що дозволяє безпомилково впізнавати ту чи іншу шкідливу програму. Сигнатури збираються в набір, званий вірусною базою, з якого в процесі перевірки пристрою беруться зразки для порівняння з файлами, що зберігаються на цьому пристрої. У разі збігу такий файл вважається шкідливим. Ця методика має значний недолік: при найменшій зміні структури шкідливої програми її сигнатура змінюється, що робить її невиявленою для антивірусної програми доти, доки її сигнатура не потрапить у вірусну базу [1].

Не менш популярним є метод поведінкового аналізу, який використовується багатьма сучасними антивірусними програмами. Його суть полягає у стеженні за поведінкою додатків, і, якщо якийсь з них здається антивірусу «підозрілим», він буде миттєво заблокованим. Поведінка програми вивчається шляхом поміщення його у віртуальний контейнер, що обмежує доступ до пам'яті пристрою та компонентів операційної системи. Якщо програма намагається взаємодіяти із запущеними процесами, структурою виконуваного файлу або завантажувальним записом, вона отримує статус потенційної загрози. Як правило, для всіх екземплярів шкідливих програм створюються спеціальні записи, що містять шаблони поведінки цих екземплярів. У разі збігу поведінки однієї із запущених програм з будь-яким записом така програма миттєво позначається як шкідлива.

Завдяки опису одним поведінковим шаблоном одночасно групи подібних шкідливих програм цей підхід сприяє скороченню обсягу вірусних баз.

Крім того, використання поведінкового аналізу дозволяє виявляти небезпечні програми, що раніше не зустрічалися, бо збіг їх поведінки з одним з відомих шаблонів відразу дозволяє віднести їх до категорії шкідливих [3].

Ще одним із основних методів детектування шкідливого ПЗ є евристичний аналіз. Його принцип роботи полягає у надаванні умовного рейтингу небезпеки кожній функції, реалізованій у програмі. Деякі функції характеризуються меншими числовими значеннями небезпеки, а деякі більшими. Якщо сума оцінок усіх функцій цієї програми перевищує певний «поріг безпеки», програма визнається шкідливою. Головним недоліком цього методу є велика ймовірність помилкового спрацьовування, оскільки багато програм, що не є шкідливими, перевищують встановлене значення і визнаються такими (наприклад, деякі утиліти оновлення браузерів, що діють у фоновому режимі і відправляють запити на віддалені сервери з метою завантаження з них оновлень можуть бути сплутані з троянцем-завантажувачем). Евристичний аналіз використовує виявлення і блокування нових загроз, не занесених у вірусні бази, тому очевидним стає ще один його значний недолік: не завжди виходить усунути виявлену загрозу, оскільки її сигнатура відсутня у вірусній базі і алгоритмів її усунення ще було розроблено [4].

Останнім аналізованим методом боротьби з шкідливими програмами є проактивний антивірусний захист HIPS (Host-based Intrusion Prevention System, система запобігання вторгнень), що є однією з форм поведінкового аналізу, тобто стежить за поведінкою додатків і оцінює їх вплив на систему. Проактивний захист буває класичним, що залишає рішення про блокування або ігнорування загрози користувачеві, або експертним, що містить набір

дозволів і правил, що налаштовуються, на основі яких він самостійно виконує ті чи інші дії зі шкідливими програмами [3].

Висновки. Незважаючи на те, що створення принципово нових шкідливих програм, здатних обійти всі методи захисту, не є неможливим, це вимагає багато часу, великої кількості професіоналів та значних грошових вкладень, що зводить кількість таких додатків до мінімуму.

Таким чином, можливості сучасних антивірусних додатків дозволяють у більшості випадків успішно забезпечувати безпеку пристрою: реактивний захист, до якого належить, наприклад, сигнатурне детектування, дозволяє боротися з більшістю відомих загроз, а проактивний, представлений поведінковим аналізом, блокує ті, що раніше не зустрічались. Саме тому, згідно з останніми даними [6, 7], основним методом зараження (до 83% випадків атак на приватних осіб) стає соціальна інженерія, при якій зловмисники обманом змушують користувача самостійно запускати на своєму пристрої шкідливі програми або ділитися конфіденційною інформацією.

З огляду на все вищесказане можна зробити висновок про те, що тепер захисне програмне забезпечення здатне конкурувати з «атакуючим» і навіть трохи випереджати його, а середньостатистичному користувачу для максимального зниження ризику зараження достатньо встановити якісний антивірусний додаток і дотримуватися набору простих правил, що полягають в уникненні підозрілих посилань і вкладень, отриманих електронною поштою, відмови від скачування піратського програмного забезпечення, обережному серфінгу в мережі, тобто без кліків на різні рекламні банери, вікна тощо, а також регулярному скануванні стану системи.

Список використаних джерел

1. S. Iqbal and M. Zulkernine, "SpyDroid: A Framework for Employing Multiple Real-Time Malware Detectors on Android," 2018 13th International Conference on Malicious and Unwanted Software (MALWARE), 2018, pp. 1-8, doi: 10.1109/MALWARE.2018.8659365.
2. S. Z. Mohd Shaid and M. A. Maarof, "Malware behavior image for malware variant identification," 2014 International Symposium on Biometrics and Security Technologies (ISBAST), 2014, pp. 238-243, doi: 10.1109/ISBAST.2014.7013128.
3. S. M. Pudukotai Dinakarrao, H. Sayadi, H. M. Makrani, C. Nowzari, S. Rafatirad and H. Homayoun, "Lightweight Node-level Malware Detection and Network-level Malware Confinement in IoT Networks," 2019 Design, Automation & Test in Europe Conference & Exhibition (DATE), 2019, pp. 776-781, doi: 10.23919/DATE.2019.8715057.
4. R. Murali, A. Ravi and H. Agarwal, "A Malware Variant Resistant To Traditional Analysis Techniques," 2020 International Conference on Emerging Trends in

Information Technology and Engineering (ic-ETITE), 2020, pp. 1-7, doi: 10.1109/ic-ETITE47903.2020.264.
5. M. Howard, A. Pfeffer, M. Dalai and M. Reposa, "Predicting signatures of future malware variants," 2017 12th International Conference on Malicious and Unwanted Software (MALWARE), 2017, pp. 126-132, doi: 10.1109/MALWARE.2017.8323965.
6. W. Peng, F. Li, X. Zou and J. Wu, "Behavioral Malware Detection in Delay Tolerant Networks," in IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 1, pp. 53-63, Jan. 2014, doi: 10.1109/TPDS.2013.27.
7. S. Sen, E. Aydogan and A. I. Aysan, "Coevolution of Mobile Malware and Anti-Malware," in IEEE Transactions on Information Forensics and Security, vol. 13, no. 10, pp. 2563-2574, Oct. 2018, doi: 10.1109/TIFS.2018.2824250.

REFERENCES

8. S. Iqbal and M. Zulkernine, (2018). "SpyDroid: A Framework for Employing Multiple Real-Time Malware Detectors on Android," 2018 13th International Conference on Malicious and Unwanted Software (MALWARE), pp. 1-8, doi: 10.1109/MALWARE.2018.8659365. (in English)
9. S. Z. Mohd Shaid and M. A. Maarof, (2014). "Malware behavior image for malware variant identification," 2014 International Symposium on Biometrics and Security Technologies (ISBAST), pp. 238-243, doi: 10.1109/ISBAST.2014.7013128. (in English)
10. S. M. Pudukotai Dinakarrao, H. Sayadi, H. M. Makrani, C. Nowzari, S. Rafatirad and H. Homayoun, (2019). "Lightweight Node-level Malware Detection and Network-level Malware Confinement in IoT Networks," 2019 Design, Automation & Test in Europe Conference & Exhibition (DATE), pp. 776-781, doi: 10.23919/DATE.2019.8715057. (in English)
11. R. Murali, A. Ravi and H. Agarwal, (2020). "A Malware Variant Resistant To Traditional Analysis Techniques," 2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE), pp. 1-7, doi: 10.1109/ic-ETITE47903.2020.264. (in English)
12. M. Howard, A. Pfeffer, M. Dalai and M. Reposa, (2017). "Predicting signatures of future malware variants," 2017 12th International Conference on Malicious and Unwanted Software (MALWARE), pp. 126-132, doi: 10.1109/MALWARE.2017.8323965. (in English)
13. W. Peng, F. Li, X. Zou and J. Wu, (2014). "Behavioral Malware Detection in Delay Tolerant Networks," in IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 1, pp. 53-63, Jan. doi: 10.1109/TPDS.2013.27. (in English)
14. S. Sen, E. Aydogan and A. I. Aysan, (2018). "Coevolution of Mobile Malware and Anti-Malware," in IEEE Transactions on Information Forensics and Security, vol. 13, no. 10, pp. 2563-2574, Oct. doi: 10.1109/TIFS.2018.2824250. (in English)

DOI 10.32403/2411-9210-2022-2-48-142-154

CLASSIFICATION OF MALWARE AND BASIC PROTECTION METHODS

Havrysh B.M.[1], Tymchenko O.V.[2,3], Borzov Yu.O.[4], Kobevko A.T.[2]

[1]*Lviv Polytechnic National University*

12, St. Bandera St., Lviv, 79013, Ukraine

[2]*Ukrainian Academy of Printing*

19, Pid Holoskom St., Lviv, 79020, Ukraine

[3] *University of Warmia and Mazury in Olsztyn,*

5, Michała Oczapowskiego St., Olsztyn, 10719, Poland

[4] *Lviv State University of Life Safety*

35, Kleparivska St., Lviv, 79000, Ukraine

dana.havrysh@gmail.com, *o_tymch@ukr.net*,

olexandr.tymchenko@uwm.edu.pl

The article briefly describes the methods of penetration and influence on the computer system of the most common types of malicious software, considers several approaches to the classification of threats, in particular, regarding the harmfulness of the software and the level of danger. Examples of damage caused by certain types of viruses and losses are shown. A formal classification of malicious programs is carried out. It is noted that most of the existing malicious programs in the world are designed for Windows OS family, followed by Android OS. The minimum number of malicious programs, which means the highest level of protection, exists for Apple iOS. The hierarchy of malicious software is done by degree of danger. Also the main combat methods are considered used by modern anti-virus programs: signature detection of threats, behavioral pattern, proactive anti-virus protection, heuristic analysis.

Keywords*: malware, virus, computer worm, Trojan, antivirus, signature detection, behavioral analysis, proactive protection.*

Стаття надійшла до редакції 01.09.2022.

Received 01.09.2022.