МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ТА ЗАХИСТОМ ІНФОРМАЦІЇ**

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “Методи виявлення та блокування шкідливого програмного забезпечення ”

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Валентин ОСАУЛЕНКО
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-42

Валентин ОСАУЛЕНКО
Ім’я, ПРІЗВИЩЕ

Керівник: Дмитро РАБЧУН
к.т.н. Ім’я, ПРІЗВИЩЕ

Рецензент:
К.т.н., доцент Ім’я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра управління кібербезпекою та захистом інформації

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УКБЗІ
_____ Світлана ЛЕГОМІНОВА
“____”_____2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Осауленку Валентину Руслановичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Методи виявлення та блокування шкідливого програмного забезпечення ”,
керівник кваліфікаційної роботи РАБЧУН Дмитро, к.т.н.
(ПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “24“ лютого 2025 р. №56.

2. Строк подання кваліфікаційної роботи “12” травня 2025р.

3. Вихідні дані до кваліфікаційної роботи: *інформаційна безпека підприємства, методи та засоби управління персоналом з інформаційної безпеки, міжнародні стандарти, наукова та технічна література.*

4. Перелік питань, які мають бути розроблені:
4.1. Проаналізувати теоретичні основи шкідливого програмного забезпечення.
4.2. Дослідити існуючі методи виявлення та блокування шкідливого ПЗ.
4.3. Розробити практичні рекомендації щодо підвищення рівня захисту інформаційних систем.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “5“ березня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2025	
2.	Збір та аналіз літератури.	29.03.2025	
3.	Аналіз особливостей управління інформаційною безпекою підприємства	08.04.2025	
4.	Дослідження основних характеристик технологій формування обізнаності й навчання персоналу.	15.04.2025	
5.	Вивчення інструментів та методів формування обізнаності й навчання персоналу з інформаційної безпеки	22.04.2025	
6.	Формулювання висновків за результатами проведеного дослідження.	29.04.2025	
7.	Оформлення роботи.	06.05.2025	
8.	Оформлення презентації.	09.05.2025	
9.	Отримання рецензії на роботу.	12.06.2025	
10.	Захист в ДЕК.	__.06.2025	

Здобувачка вищої освіти _____ Валентин ОСАУЛЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Дмитро РАБЧУН
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня бакалавра

Направляється здобувачка Осауленко В.Р. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Методи виявлення та блокування шкідливого програмного забезпечення"

Кваліфікаційна робота і рецензія додаються.

Директор ННІКБЗІ _____ Євгенія ІВАНЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач ОСАУЛЕНКО Валентин у кваліфікаційній роботі проаналізував особливості загроз, пов'язаних із шкідливим програмним забезпеченням, дослідив класифікацію, принципи функціонування та сучасні методи виявлення і блокування шкідливого ПЗ, а також розробив практичні рекомендації щодо побудови багаторівневої системи захисту з урахуванням актуальних тенденцій кіберзагроз.

ОСАУЛЕНКО Валентин продемонстрував глибоке розуміння проблематики дослідження, володіння науковим апаратом та знання сучасних технологій забезпечення кібербезпеки. Проявив себе як відповідальний і цілеспрямований виконавець, здатний до самостійного аналізу, узагальнення матеріалу та розробки обґрунтованих практичних рішень.

Все це дозволяє оцінити кваліфікаційну роботу здобувача ОСАУЛЕНКА Валентина на оцінку "відмінно" та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Дмитро РАБЧУН
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____"_____2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Осауленко В.Р. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри
управління кібербезпекою та
захистом інформації _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

Здобувач вищої освіти ОСАУЛЕНКО Валентин
на тему: «Методи виявлення та блокування шкідливого програмного забезпечення».

Актуальність. У світі, де держави, бізнес і користувачі щоденно зіштовхуються з кібернетичними атаками, питання захисту інформаційних систем від шкідливого програмного забезпечення є надзвичайно актуальним. Шкідливе ПЗ постійно розвивається та ускладнюється, з'являються нові види атак (віруси, трояни, програми-вимагачі тощо), здатні обходити традиційні засоби кіберзахисту. Забезпечення ефективного виявлення та нейтралізації таких загроз вимагає впровадження сучасних підходів та технологій. Дослідження, проведене в кваліфікаційній роботі, відповідає нагальним потребам практики кібербезпеки, оскільки спрямоване на вдосконалення методів протидії шкідливому програмному забезпеченню. Отже, тема роботи є актуальною і має важливе теоретичне й прикладне значення.

Позитивні сторони.

1.У роботі всебічно досліджено теоретичні основи та сучасні методи виявлення і блокування шкідливого програмного забезпечення. Автор приділив увагу класифікації ШПЗ, аналізу принципів роботи антивірусних систем (сигнатурних, евристичних, поведінкових методів) та інших засобів захисту, що свідчить про глибоке розуміння теми.

2.Кваліфікаційна робота структурована і оформлена відповідно до встановлених вимог. Виклад матеріалу логічний і послідовний, кожен розділ завершується обґрунтованими висновками. Ключові положення та результати ілюстровано наочними рисунками, що полегшує сприйняття інформації.

3.Автор опрацював значну кількість джерел (близько 50 публікацій, у тому числі англомовних), що дозволило включити в дослідження актуальні світові підходи та досвід протидії ШПЗ. Бібліографія роботи свідчить про вміння критично аналізувати інформацію з різних джерел.

4.За результатами дослідження запропоновано практичні рекомендації щодо підвищення рівня захисту інформаційних систем від шкідливого програмного забезпечення. Зокрема, автор рекомендує впровадження сучасних засобів виявлення та реагування (EDR/XDR-систем), принципів Zero Trust архітектури, сегментації мережі та інших превентивних заходів, що є цінним вкладом у прикладну сферу кібербезпеки.

Недоліки.

У роботі доречно було б приділити більше уваги практичній перевірці запропонованих методів. Зокрема, результати дослідження могли б бути підкріплені експериментальним оцінюванням ефективності впроваджених рекомендацій (наприклад, імітацією кібератак до і після застосування запропонованих заходів захисту). Однак вказані зауваження не впливають істотно на загальну позитивну оцінку роботи.

Висновок: Кваліфікаційна робота виконана на високому науково-методичному рівні, відповідає встановленим вимогам до бакалаврських робіт за спеціальністю «Кібербезпека» та заслуговує оцінки «відмінно». Здобувач ОСАУЛЕНКО Валентин заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою «Управління інформаційною та кібернетичною безпекою».

Рецензент:
к.т.н., доцент _____ *підпис* Ім'я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню методів виявлення та блокування шкідливого програмного забезпечення в інформаційних системах. Робота складається зі вступу, трьох розділів, висновків, списку використаних джерел із 30 найменувань. Загальний обсяг роботи – 87 аркуші з них 4 аркушів займають список використаних джерел і перелік умовних скорочень.

Метою роботи є дослідження сучасних підходів до виявлення й блокування шкідливого програмного забезпечення та розробка практичних рекомендацій щодо підвищення рівня захищеності інформаційних систем від ШПЗ.

Об'єктом дослідження є шкідливе програмне забезпечення як загроза інформаційним системам та процеси протидії йому.

Предмет дослідження – методи виявлення шкідливого програмного забезпечення та засоби блокування його деструктивної діяльності.

Методи дослідження. У роботі використано методи аналізу і синтезу (для вивчення літературних джерел і нормативних документів), порівняння та класифікації (для систематизації видів ШПЗ і методів їх виявлення), експертної оцінки та системного підходу (для розробки рекомендацій з удосконалення систем захисту).

Як результат у роботі проаналізовано теоретичні основи та історичний розвиток шкідливого ПЗ; досліджено існуючі системи захисту від ШПЗ (антивірусні програми, системи виявлення вторгнень, засоби проактивного захисту) та оцінено їх ефективність і недоліки; розроблено комплекс практичних рекомендацій щодо підвищення ефективності захисту інформаційних систем від сучасних кіберзагроз на основі впровадження передових технологій (EDR, XDR, Zero Trust тощо).

Галузь застосування. Розроблені рекомендації та висновки можуть бути впроваджені у діяльність служб кібербезпеки підприємств при модернізації систем захисту від шкідливого ПЗ, а також використані в освітньому процесі для підготовки фахівців з кібербезпеки.

Ключові слова: ШКІДЛИВЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ВИЯВЛЕННЯ, БЛОКУВАННЯ, КІБЕРБЕЗПЕКА, ЗАХИСТ ІНФОРМАЦІЙНИХ СИСТЕМ.

ABSTRACT

The qualification work is devoted to the study of methods for detecting and blocking malware in information systems. The work consists of an introduction, three chapters, conclusions, a list of references of 30 titles. The total volume of the work is 87 pages, of which 4 pages are occupied by the list of references and the list of abbreviations.

The purpose of the work is to study modern approaches to detecting and blocking malicious software and to develop practical recommendations for improving the security of information systems against malware.

The object of the study is malware as a threat to information systems and processes of counteracting it.

The subject of the study is methods of detecting malware and means of blocking its destructive activities.

Research methods. The methods of analysis and synthesis (for studying literature and regulatory documents), comparison and classification (for systematizing the types of malware and methods of their detection), expert evaluation and systematic approach (for developing recommendations for improving protection systems) were used in the study.

As a result the paper analyzes the theoretical foundations and historical development of malware; investigates existing protection systems against malware (antivirus programs, intrusion detection systems, proactive protection tools) and assesses their effectiveness and shortcomings; develops a set of practical recommendations for improving the effectiveness of protecting information systems from modern cyber threats through the introduction of advanced technologies (EDR, XDR, Zero Trust, etc.).

Scope of application. The developed recommendations and conclusions can be implemented in the activities of enterprise cybersecurity services in the modernization of malware protection systems, as well as used in the educational process for training cybersecurity specialists.

Keywords: MALICIOUS SOFTWARE, DETECTION, BLOCKING, CYBERSECURITY, PROTECTION OF INFORMATION SYSTEMS.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

Скорочення	**Розшифрування**
ІБ	Інформаційна безпека
ПЗ	Програмне забезпечення
ШПЗ	Шкідливе програмне забезпечення
СУІБ	Система управління інформаційною безпекою
EDR	Endpoint Detection and Response (виявлення та реагування на кінцевих точках)
XDR	Extended Detection and Response (розширене виявлення та реагування)
SOAR	Security Orchestration, Automation and Response (Оркестрація, автоматизація та реагування на інциденти безпеки)
IoC	Indicators of Compromise (індикатори компрометації)
SIEM	Security Information and Event Management (керування інформацією та подіями безпеки)
AV	Антивірус
AI	Artificial Intelligence (штучний інтелект)
ML	Machine Learning (машинне навчання)
Zero Trust	Модель нульової довіри

ВСТУП

Актуальність теми. Сучасні кібератаки все частіше використовують шкідливе програмне забезпечення (ШПЗ) як один із основних інструментів. У світі, де державні установи, компанії та окремі користувачі постійно стають об’єктами кібератак, питання протидії ШПЗ є як ніколи актуальним. Шкідливе програмне забезпечення постійно еволюціонує: з’являються нові віруси, мережеві хробаки, трояни, програми-вимагачі, які здатні обходити традиційні засоби захисту. Значні фінансові та репутаційні втрати, спричинені успішними атаками із використанням ШПЗ (наприклад, атаками типу ransomware), підкреслюють важливість своєчасного виявлення та блокування таких загроз. Постійний розвиток IT-сфери, з одного боку, спрощує розробку все складнішого шкідливого коду, а з іншого боку – вимагає впровадження новітніх методів кіберзахисту. Тому дослідження ефективних методів виявлення та блокування ШПЗ є надзвичайно важливим науковим та практичним завданням сьогодення.

Мета роботи. Полягає у дослідженні методів виявлення та блокування шкідливого програмного забезпечення і розробці рекомендацій для підвищення рівня захисту інформаційних систем від таких кібератак.

Об’єкт дослідження. Процеси протидії шкідливому програмному забезпеченню в інформаційних системах.

Предмет дослідження. Методи та засоби виявлення і блокування шкідливого програмного забезпечення.

Для досягнення поставленої мети в роботі необхідно вирішити такі завдання:

1. Проаналізувати теоретичні основи шкідливого програмного забезпечення, зокрема поняття, класифікацію та життєвий цикл ШПЗ.

2. Дослідити та проаналізувати існуючі системи і методи захисту від ШПЗ (сигнатурні та евристичні методи антивірусного захисту, системи виявлення вторгнень, тощо), оцінити їх ефективність та обмеження.

3. Розробити практичні рекомендації щодо підвищення рівня захисту

інформаційних систем від сучасних видів ШПЗ, впровадження новітніх підходів (EDR/XDR, Zero Trust, сегментація мережі та інші) та удосконалення існуючих засобів захисту.

Методи дослідження. Для розв'язання поставлених задач використано загальнонаукові та спеціальні методи: аналіз і синтез (при вивченні літературних джерел та нормативної бази з тематики ШПЗ), порівняння та класифікація (для систематизації різновидів шкідливих програм і методів боротьби з ними), статистичний аналіз (при оцінюванні масштабів загроз і ефективності захисних заходів за даними звітів), а також системний підхід до управління інформаційною безпекою.

Практичне значення одержаних результатів. Результати дослідження мають прикладне значення для підрозділів кібербезпеки підприємств та організацій. Запропоновані рекомендації можуть бути використані при вдосконаленні корпоративних політик безпеки, впровадженні багаторівневих систем захисту від шкідливого ПЗ, налаштуванні засобів моніторингу та реагування на інциденти. Використання напрацювань роботи дозволить підвищити стійкість інформаційних систем до сучасних кіберзагроз і мінімізувати можливі збитки від атак шкідливого програмного забезпечення.

Апробація результатів. Основні результати кваліфікаційної роботи доповідалися та обговорювалися на Всеукраїнській науково-практичній конференції "Стратегії кіберстійкості: управління ризиками та безперервність бізнесу" (м. Київ, 27 лютого 2025 року).

Розділ 1 Теоретичні основи виявлення та блокування шкідливого програмного забезпечення

1.1 Що таке шкідливе програмне забезпечення?

Шкідливе програмне забезпечення, або «зловмисне програмне забезпечення» - це загальний термін, який описує будь-яку шкідливу програму або код, що завдає шкоди системам.

Вороже, нав'язливе і навмисно неприємне, шкідливе програмне забезпечення прагне вторгнутися, пошкодити або вивести з ладу комп'ютери, комп'ютерні системи, мережі, планшети і мобільні пристрої, часто беручи на себе частковий контроль над роботою пристрою. Подібно до людського грипу, воно заважає нормальному функціонуванню[1].

Іноді люди запитують про різницю між вірусом і шкідливим програмним забезпеченням. Різниця полягає в тому, що шкідливе програмне забезпечення - це загальний термін для позначення цілої низки онлайн-загроз, включаючи віруси, шпигунські програми, рекламні програми, програми-вимагачі та інші типи шкідливого програмного забезпечення. Комп'ютерний вірус - це лише один із видів шкідливого програмного забезпечення[2].

Мотиви, що стоять за шкідливими програмами, різні. Шкідливе програмне забезпечення може мати на меті заробити на вас гроші, саботувати вашу роботу, зробити політичну заяву або просто похвалитися своїми здібностями. Хоча шкідливе програмне забезпечення не може пошкодити фізичне обладнання систем або мережеве обладнання воно може викрасти, зашифрувати або видалити ваші дані, змінити або перехопити основні функції комп'ютера, а також шпигувати за вашою комп'ютерною діяльністю без вашого відома або дозволу.

Ви знаєте, як щороку медична спільнота закликає всіх зробити щеплення від грипу? Це тому, що спалахи грипу зазвичай мають сезон - пору року, коли він починає поширюватися і заражати людей. На противагу цьому, для комп'ютерів, смартфонів, планшетів та корпоративних мереж не існує

передбачуваних сезонних інфекцій. Для них це завжди сезон грипу. Але замість того, щоб страждати від ознобу та болю в тілі, користувачі можуть захворіти на різновид машинної хвороби - шкідливе програмне забезпечення.

Таким чином, розуміння загальних понять про шкідливе програмне забезпечення є фундаментом для подальшого дослідження. У наступному підрозділі розглянемо класифікацію цих загроз з урахуванням їх особливостей та впливу[1].

1.2 Класифікація шкідливого програмного забезпечення

Важливо розуміти різні типи атак шкідливих програм, щоб захистити себе від їхнього впливу. Деякі категорії шкідливих програм добре відомі (принаймні за назвами), інші - менш відомі:

Рекламні програми

Рекламні програми, скорочення від «програмне забезпечення з підтримкою реклами», відображають небажану, а іноді й шкідливу рекламу на екрані комп'ютера або мобільного пристрою, перенаправляють результати пошуку на рекламні веб-сайти та збирають дані користувача, які можуть бути продані рекламодавцям без згоди користувача. Не всі рекламні програми є шкідливими, деякі з них є законними і безпечними у використанні.

Користувачі часто можуть впливати на частоту появи рекламних програм або на те, які типи завантажень вони дозволяють, керуючи спливаючими елементами керування та налаштуваннями в своїх інтернет-браузерах або використовуючи блокувальник реклами.

Приклади рекламного ПЗ:

Fireball потрапив у заголовки газет у 2017 році, коли ізраїльська компанія з розробки програмного забезпечення виявила, що 250 мільйонів комп'ютерів і п'ята частина корпоративних мереж по всьому світу були заражені ним. Коли Fireball вражає ваш комп'ютер, він захоплює ваш браузер. Він змінює вашу домашню сторінку на фальшиву пошукову систему Trotus і вставляє нав'язливу

рекламу на будь-яку веб-сторінку, яку ви відвідуєте. Він також не дозволяє вам змінювати налаштування вашого браузера[3].

Appearch - ще одна поширена рекламна програма, яка діє як викрадач браузера. Зазвичай у комплекті з іншим безкоштовним програмним забезпеченням вона вставляє в браузер так багато реклами, що перегляд веб-сторінок стає дуже складним. Коли ви намагаєтеся відвідати веб-сайт, замість цього вас перенаправляють на Appearch.info. Якщо вам вдається відкрити веб-сторінку, Appearch перетворює випадкові блоки тексту на посилання, тому, коли ви вибираєте текст, спливаюче вікно пропонує вам завантажити оновлення програмного забезпечення.

Шпигунське програмне забезпечення

Шпигунське програмне забезпечення - це різновид шкідливого програмного забезпечення, яке ховається на вашому пристрої, відстежує активність і викрадає конфіденційну інформацію, наприклад, фінансові дані, інформацію про облікові записи, логіни тощо. Шпигунські програми можуть поширюватися, використовуючи вразливості програмного забезпечення, або ж у комплекті з легальним програмним забезпеченням чи у вигляді троянів.

Приклади шпигунських програм:

CoolWebSearch - ця програма використовує вразливості в Internet Explorer для перехоплення браузера, зміни налаштувань і надсилання даних про перегляд веб-сторінок своєму автору.

Gator - зазвичай у комплекті з файлообмінниками, такими як Kazaa, ця програма відстежує звички веб-серфінгу жертви і використовує цю інформацію, щоб показувати їй певну рекламу[3].

Програми-вимагачі та крипто-шкідливі програми

Програми-вимагачі - це шкідливе програмне забезпечення, призначене для блокування користувачів у їхніх системах або заборони доступу до даних до сплати викупу. Крипто-шкідливе програмне забезпечення - це тип програм-вимагачів, які шифрують файли користувача і вимагають оплату до певного терміну, часто за допомогою цифрової валюти, наприклад, біткоїна. Програми-

вимагачі вже багато років є постійною загрозою для організацій різних галузей. Оскільки все більше компаній впроваджують цифрову трансформацію, ймовірність стати мішенню для атаки зловмисників значно зросла.

Приклади програм-вимагачів:

CryptoLocker - це різновид шкідливого програмного забезпечення, поширений у 2013 та 2014 роках, який кіберзлочинці використовували для отримання доступу до файлів у системі та їх шифрування. Кіберзлочинці використовували тактику соціальної інженерії, щоб обманом змусити співробітників завантажити програму-вимагач на свої комп'ютери і заразити мережу. Після завантаження CryptoLocker відображав повідомлення з вимогою викупу з пропозицією розшифрувати дані, якщо оплата готівкою або біткойнами буде здійснена до зазначеного терміну. Хоча програма-вимагач CryptoLocker була видалена, вважається, що її оператори вимагали близько трьох мільйонів доларів від організацій, які нічого не підозрювали[3].

Phobos - різновид вірусу-вимагача, що з'явився у 2019 році. Цей штам вірусу-вимагача базується на раніше відомому сімействі вірусів-вимагачів Dharma (також відомому як CrySis).

Троянські програми

Троянська програма (або «троянський кінь») маскується під легальне програмне забезпечення, щоб обманом запустити на вашому комп'ютері шкідливе програмне забезпечення. Оскільки воно виглядає надійним, користувачі завантажують його, ненавмисно дозволяючи шкідливому програмному забезпеченню потрапити на свій пристрій. Троянські програми самі по собі є лазівкою. На відміну від хробака, для роботи їм потрібен хост. Після встановлення трояна на пристрій хакери можуть використовувати його для видалення, модифікації або перехоплення даних, використання вашого пристрою як частини ботнету, шпигунства за вашим пристроєм або отримання доступу до вашої мережі.

Приклади троянів:

Шкідливе програмне забезпечення Qbot, також відоме як «Qakbot» або «Pinkslipbot», є банківським трояном, активним з 2007 року і спрямованим на крадіжку даних користувачів та банківських облікових даних. Шкідливе програмне забезпечення еволюціонувало, з'явилися нові механізми доставки, методи управління та функції антианалізу.

Шкідливе програмне забезпечення TrickBot, вперше виявлене у 2016 році, - це троянська програма, розроблена та експлуатована досвідченими кіберзлочинцями. Спочатку розроблений як банківський троян для крадіжки фінансових даних, TrickBot перетворився на модульне багатоступеневе шкідливе програмне забезпечення, яке надає своїм операторам повний набір інструментів для здійснення численних незаконних кібератак[3].

Хробаки

Один з найпоширеніших видів шкідливого програмного забезпечення, черв'яки, поширюється через комп'ютерні мережі, використовуючи вразливості операційної системи. Хробак - це автономна програма, яка реплікує себе для зараження інших комп'ютерів, не вимагаючи жодних дій з боку користувача. Оскільки вони можуть швидко поширюватися, черв'яки часто використовуються для виконання корисного навантаження - фрагмента коду, створеного для пошкодження системи. Корисне навантаження може видаляти файли на хост-системі, шифрувати дані для атаки з вимогою викупу, викрадати інформацію, видаляти файли та створювати ботнети.

Приклад хробака:

SQL Slammer був відомим комп'ютерним хробаком, який не використовував традиційні методи розповсюдження. Замість цього він генерував випадкові IP-адреси і розсилає себе на них, шукаючи ті, що не захищені антивірусним програмним забезпеченням. Невдовзі після того, як він з'явився у 2003 році, результатом стало понад 75 000 інфікованих комп'ютерів, які несвідомо брали участь у DDoS-атаках на кілька великих веб-сайтів.

Незважаючи на те, що відповідний патч безпеки доступний вже багато років, SQL Slammer, тим не менш, пережив відродження в 2016 і 2017 роках[3].

Віруси

Вірус - це фрагмент коду, який вбудовується в програму і виконується під час її запуску. Потрапивши в мережу, вірус може бути використаний для крадіжки конфіденційних даних, DDoS-атак або атак з вимогою викупу. Зазвичай вірус поширюється через заражені веб-сайти, спільний доступ до файлів або завантаження вкладень в електронній пошті, і перебуває в сплячому режимі до тих пір, поки не буде активований заражений файл або програма. Як тільки це відбувається, вірус може розмножуватися і поширюватися у ваших системах.

Приклад вірусу:

Stuxnet - Stuxnet з'явився у 2010 році і, як вважається, був розроблений урядами США та Ізраїлю, щоб зірвати ядерну програму Ірану. Поширюючись через флешку, він був націлений на промислові системи управління Siemens, спричиняючи збої в роботі центрифуг та їхнє самознищення з рекордною швидкістю. Вважається, що Stuxnet заразив понад 20 000 комп'ютерів і зруйнував п'яту частину ядерних центрифуг Ірану, відкинувши його програму на роки назад[3].

Кейлоггери

Кейлоггер - це тип шпигунського програмного забезпечення, яке відстежує активність користувача. Кейлоггери можуть використовуватися в законних цілях - наприклад, сім'ями, які використовують їх для відстеження активності своїх дітей в Інтернеті, або організаціями, які використовують їх для моніторингу діяльності співробітників. Однак, встановлені зі зловмисною метою, клавіатурні шпигуни можуть бути використані для крадіжки даних паролів, банківської інформації та іншої конфіденційної інформації. Кейлоггери можуть бути вставлені в систему за допомогою фішингу, соціальної інженерії або шкідливих завантажень.

Приклад кейлоггера:

У 2017 році студент Університету штату Айова був заарештований після того, як встановив кейлоггер на комп'ютери співробітників, щоб викрасти облікові дані для входу в систему, щоб модифікувати і змінювати оцінки. Студента визнали винним і засудили до чотирьох місяців ув'язнення[3].

Боти та ботнети

Бот - це комп'ютер, який був заражений шкідливим програмним забезпеченням, щоб хакер міг керувати ним віддалено. Бот, який іноді називають комп'ютером-зомбі, може бути використаний для здійснення нових атак або стати частиною колекції ботів, яка називається бот-мережею. Ботнети можуть включати мільйони пристроїв, оскільки вони поширюються непоміченими. Ботнети допомагають хакерам здійснювати численні зловмисні дії, зокрема DDoS-атаки, розсилання спаму та фішингових повідомлень, а також поширення інших видів шкідливого програмного забезпечення.

Приклади ботнетів:

Шкідливе програмне забезпечення Andromeda - ботнет Andromeda був пов'язаний з 80 різними сімействами шкідливого програмного забезпечення. Він настільки розрісся, що в якийсь момент заражав мільйон нових комп'ютерів щомісяця, поширюючи себе через соціальні мережі, миттєві повідомлення, спам, набори експлойтів тощо. У 2017 році операція була припинена ФБР, Європейським центром з боротьби з кіберзлочинністю Європолу та іншими організаціями, але багато комп'ютерів продовжували бути зараженими.

Mirai - У 2016 році масована DDoS-атака залишила значну частину східного узбережжя США без доступу до інтернету. Атака, яку влада спочатку вважала справою рук ворожої національної держави, була спричинена ботнетом Mirai. Mirai - це тип шкідливого програмного забезпечення, яке автоматично знаходить пристрої Інтернету речей (IoT) для зараження і залучає їх до ботнету. Звідти ця армія IoT може бути використана для проведення DDoS-атак, під час яких потік небажаного трафіку заливає сервери жертви шкідливим трафіком. Mirai продовжує створювати проблеми і сьогодні[3].

Шкідливе програмне забезпечення PUP

ПНП - що означає «потенційно небажані програми» - це програми, які можуть містити рекламу, панелі інструментів та спливаючі вікна, які не пов'язані з програмним забезпеченням, яке ви завантажили. Строго кажучи, ПНП не завжди є шкідливим програмним забезпеченням - розробники ПНП зазначають, що їхні програми завантажуються за згодою користувачів, на відміну від шкідливого програмного забезпечення. Але загальновизнано, що люди здебільшого завантажують ПНП, тому що не усвідомлюють, що дали на це згоду.

ПНП часто йдуть у комплекті з іншими, більш легальними програмами. Більшість людей в кінцевому підсумку отримують ПНП, тому що завантажили нову програму і не прочитали дрібний шрифт під час її встановлення - і тому не усвідомлюють, що погоджуються на додаткові програми, які не служать реальній меті.

Приклад шкідливого програмного забезпечення PUP:

Шкідливе програмне забезпечення Mindspark - це легко інстальоване ПНП, яке потрапляє на комп'ютери користувачів так, що вони не помічають його завантаження. Mindspark може змінювати налаштування та запускати певні дії на пристрої без відома користувача. Його, як відомо, важко усунути[3].

Гібриди

Сьогодні більшість шкідливих програм є комбінацією різних типів шкідливого програмного забезпечення, часто включаючи частини троянів і черв'яків, а іноді і вірусів. Зазвичай, шкідлива програма виглядає для кінцевого користувача як троянська програма, але після запуску вона атакує інших жертв у мережі як черв'як.

Приклад гібридного шкідливого програмного забезпечення:

У 2001 році розробник шкідливого програмного забезпечення, який називав себе «Lion», випустив гібридне шкідливе програмне забезпечення - комбінацію черв'яка та руткіта. Руткіти дозволяють хакерам маніпулювати файлами операційної системи, тоді як хробаки є потужним вектором для швидкого поширення фрагментів коду. Ця шкідлива комбінація спричинила

хаос: вона завдала шкоди більш ніж 10 000 систем Linux. Комбінація черв'як/руткіт була спеціально розроблена для використання вразливостей в системах Linux[3].

Безфайлове шкідливе програмне забезпечення

Безфайлове шкідливе програмне забезпечення - це тип шкідливого програмного забезпечення, яке використовує легітимні програми для зараження комп'ютера. Воно не покладається на файли і не залишає жодних слідів, що ускладнює його виявлення та видалення. Безфайлове шкідливе програмне забезпечення з'явилося в 2017 році як основний тип атаки, але багато з цих методів атаки існують вже давно.

Безфайлові інфекції не зберігаються у файлах і не встановлюються безпосередньо на комп'ютері, вони потрапляють безпосередньо в пам'ять, і шкідливий вміст ніколи не торкається жорсткого диска. Кіберзлочинці все частіше звертаються до безфайлових шкідливих програм як до ефективної альтернативної форми атаки, що ускладнює виявлення традиційних антивірусів через малий розмір і відсутність файлів для сканування.

Приклади безфайлових шкідливих програм:

Frodo, Number of the Beast і The Dark Avenger були першими прикладами цього типу шкідливих програм[3].

Логічні бомби

Логічні бомби - це тип шкідливого програмного забезпечення, яке активується лише за певних умов, наприклад, у певну дату та час або при 20-му вході в обліковий запис. Віруси та хробаки часто містять логічні бомби, щоб доставити своє корисне навантаження (тобто шкідливий код) у заздалегідь визначений час або при виконанні іншої умови. Шкода, яку завдають логічні бомби, варіюється від зміни байтів даних до нечитабельності жорстких дисків.

Приклад логічної бомби:

У 2016 році програміст спричиняв збої в роботі електронних таблиць у філії корпорації Siemens кожні кілька років, так що вони змушені були наймати

його назад, щоб вирішити проблему. У цьому випадку ніхто нічого не підозрював, доки збіг обставин не змусив шкідливий код вийти назовні.

Класифікація дає змогу чітко розмежувати типи шкідливого ПЗ і підібрати до кожного з них відповідні методи виявлення. Саме методам виявлення цих загроз присвячено наступний підрозділ[3].

1.3 Методи виявлення шкідливого ПЗ

Ефективна практика безпеки використовує поєднання досвіду та технологій для виявлення та запобігання шкідливому програмному забезпеченню. Випробувані та перевірені методи включають[4].

Виявлення на основі сигнатур

Виявлення на основі сигнатур використовує відомі цифрові індикатори шкідливого програмного забезпечення для виявлення підозрілої поведінки. Списки індикаторів компрометації (IOC), які часто зберігаються в базі даних, можуть бути використані для виявлення порушень. Хоча IOC можуть бути ефективними для виявлення зловмисної активності, вони є реактивними за своєю природою. Тому CrowdStrike використовує індикатори атаки (IOA) для проактивного виявлення кібератак, що відбуваються в процесі[4].

Статичний аналіз файлів

Вивчення коду файлу без його запуску для виявлення ознак зловмисних намірів. Імена файлів, хеші, рядки, такі як IP-адреси, і дані заголовка файлу - все це можна оцінити, щоб визначити, чи є файл шкідливим. Хоча статичний аналіз файлів є хорошою відправною точкою, досвідчені команди безпеки використовують додаткові методи для виявлення складних шкідливих програм, які можуть залишитися невиявленими під час статичного аналізу[4].

Динамічний аналіз шкідливого програмного забезпечення

Динамічний аналіз шкідливого програмного забезпечення виконує підозрілий шкідливий код у безпечному середовищі, яке називається пісочницею. Ця закрита система дозволяє фахівцям з безпеки спостерігати і

вивчати шкідливе програмне забезпечення в дії без ризику зараження системи або проникнення в корпоративну мережу[4].

Динамічний моніторинг масових операцій з файлами

Спостереження за масовими операціями з файлами, такими як команди перейменування або видалення, для виявлення ознак втручання або пошкодження. Динамічний моніторинг часто використовує інструмент моніторингу цілісності файлів для відстеження та аналізу цілісності файлових систем за допомогою як реактивного форензік-аудиту, так і проактивного моніторингу на основі правил[4].

Розширення файлів blocklist/blocklisting

Розширення файлів - це літери, що стоять після крапки в імені файлу і вказують на формат файлу. Ця класифікація може бути використана зловмисниками для пакування шкідливого програмного забезпечення для доставки. Як наслідок, поширеним методом захисту є внесення відомих шкідливих типів розширень файлів у «блок-лист», щоб запобігти завантаженню або використанню небезпечного файлу користувачами, які нічого не підозрюють[4].

Список дозволених додатків

Протилежність blocklist/blocklisting, коли організація дозволяє системі використовувати додатки із затвердженого списку. Allowlisting може бути дуже ефективним у запобіганні використанню шкідливих програм за допомогою жорстких параметрів. Однак, він може бути складним в управлінні та знижувати операційну швидкість і гнучкість організації[4].

Файли-приманки для шкідливого ПЗ

Файли-приманки для шкідливого ПЗ імітують програмне забезпечення або інтерфейс прикладного програмування (API), щоб відволікти увагу зловмисників від атак у контрольованому, безпечному середовищі. Аналогічно, файл-приманка - це файл-приманка, який заманює зловмисників і виявляє їх. Таким чином, команди безпеки можуть проаналізувати методи атаки і розробити або

вдосконалити рішення для захисту від шкідливого програмного забезпечення для усунення цих конкретних вразливостей, загроз або дійових осіб[4].

Контрольна сума/циклічна перевірка надмірності (CRC)

Обчислення набору даних, наприклад, файлу, для підтвердження його цілісності. Однією з найпоширеніших контрольних сум є CRC, яка передбачає аналіз як значення, так і позиції групи даних. Підрахунок контрольних сум може бути ефективним для виявлення корупції в даних, але не є безвідмовним для визначення втручання[4].

Ентропія файлів/вимірювання змін даних у файлах

З розвитком розвідки загроз та кібербезпеки зловмисники все частіше створюють динамічні виконувані файли шкідливого програмного забезпечення, щоб уникнути виявлення. Це призводить до того, що модифіковані файли мають високий рівень ентропії. Як наслідок, зміна даних у файлі, виміряна через ентропію, може виявити потенційне шкідливе програмне забезпечення[4].

Поведінковий аналіз машинного навчання

Машинне навчання (ML) є підмножиною штучного інтелекту (ШІ) і відноситься до процесу навчання алгоритмів вивчати закономірності на основі наявних даних для прогнозування відповідей на нові дані. Ця технологія може аналізувати поведінку файлів, виявляти закономірності та використовувати ці знання для покращення виявлення нових і неідентифікованих шкідливих програм[4].

Методи виявлення шкідливого ПЗ є ключовим компонентом будь-якої системи безпеки. Щоб краще зрозуміти практичні аспекти застосування цих методів, звернемося до інструментів і платформ які їх реалізують.

1.4 Інструменти та платформи для виявлення шкідливого ПЗ

Інструменти аналізу шкідливого програмного забезпечення допомагають фахівцям з кібербезпеки аналізувати та розуміти шкідливе програмне забезпечення, що дозволяє ефективно виявляти загрози, реагувати на них та

запобігати їм. Існує безліч інструментів, які допомагають аналітикам з безпеки розслідувати та протидіяти шкідливому програмному забезпеченню - від рішень з відкритим кодом до комерційних продуктів. Ці інструменти можуть допомогти у статичному та динамічному аналізі, зворотному інжинірингу, поведінковому аналізі та автоматизованому виявленні загроз. Ось декілька з них:

Any.run

ANY.RUN - це онлайн-сервіс для аналізу шкідливого програмного забезпечення, що пропонує як динамічні, так і статичні інструменти для дослідження різноманітних кіберзагроз. Його інтерактивний інструмент аналізу дозволяє дослідникам вивчати виконання завдань і спостерігати за створенням процесів у реальному часі під час симуляцій.

ANY.RUN аналізує підозрілі URL-адреси в декількох браузерах, що дозволяє більш комплексно виявляти вектори атак. Сервіс використовує матрицю MITRE ATT&CK для зіставлення сигнатур, що дозволяє легко зрозуміти структуру атак і методи, які використовуються. Графіки процесів ANY.RUN відображають шаблони атак у вигляді інтерактивної візуальної деревоподібної структури, що дозволяє аналітикам швидко ідентифікувати шкідливі процеси та отримувати більш детальну інформацію. Сервіс підтримує аналіз різних типів файлів, об'єднуючи тисячі звітів про шкідливе програмне забезпечення для постійного аналізу та експорту даних для зовнішнього використання. ANY.RUN пропонує користувацькі HTML-звіти, якими можна легко поділитися або роздрукувати, надаючи вичерпну інформацію про результати, включаючи індикатори компрометації, скріншоти та графіки поведінки процесів.

Крім того, його інструменти мережевого аналізу дозволяють користувачам досліджувати HTTP-з'єднання, оцінювати мережеві потоки та експортувати ключі PCAP і SSL для зовнішнього аналізу. Таким чином, ANY.RUN - це універсальний сервіс для аналізу шкідливого програмного забезпечення для розуміння та захисту від широкого спектру кіберзагроз[5].

Cuckoo Sandbox

Cuckoo Sandbox - це автоматизована система аналізу шкідливого програмного забезпечення з відкритим вихідним кодом, сумісна з платформами Windows, macOS, Linux та Android. Вона ефективно перевіряє підозрілі файли за лічені хвилини, надаючи детальний звіт про виявлену поведінку в реалістичному, ізольованому середовищі. Це дозволяє компаніям краще розуміти кіберзагрози та вживати необхідних заходів для захисту.

Основною функцією Cuckoo Sandbox є дослідження різних шкідливих файлів, таких як виконувані файли, офісні документи, PDF-файли та електронні листи, а також шкідливих веб-сайтів у віртуалізованих системах. Вона відстежує виклики API та загальну поведінку файлів, майже миттєво перетворюючи інформацію на зрозумілі високорівневі дані та підписи. Система може збирати та аналізувати мережевий трафік, навіть якщо він зашифрований за допомогою SSL/TLS, і пропонує власну підтримку мережевої маршрутизації. Крім того, вона проводить розширений аналіз пам'яті зараженої віртуалізованої системи, використовуючи Volatility і YARA для пам'яті процесів.

Модульний дизайн Cuckoo Sandbox з відкритим вихідним кодом дозволяє користувачам налаштовувати кожен аспект середовища аналізу, обробки результатів і етапу звітування. Вона також може бути розміщена в різних місцях залежно від вимог. Така гнучкість забезпечує безперешкодну інтеграцію з існуючими фреймворками та бекендами користувачів без будь-яких ліцензійних вимог[5].

Hybrid Analysis

Hybrid Analysis - це платформа для аналізу шкідливого програмного забезпечення, яка використовує технології Falcon Sandbox і Hybrid Analysis для проведення поглиблених статичних і динамічних досліджень. Ця платформа може аналізувати навіть найскладніші шкідливі програми, об'єднуючи дані під час виконання з аналізом дампа пам'яті.

Це рішення дозволяє витягувати індикатори поведінки та вираховувати додаткові індикатори компрометації (IoC), такі як рядки та ланцюжки викликів

API. Воно використовує унікальну технологію гібридного аналізу для виявлення та вивчення невідомих загроз. Користувачі можуть завантажувати та обмінюватися колекціями файлів, які потім перевіряються різними методами, включаючи машинне навчання за допомогою CrowdStrike Falcon Static Analysis, пошук по репутації та антивірусні системи. Всі завантажені файли стають доступними для пошуку широкій спільноті, що дозволяє розширити співпрацю та обмін розвідданими.

Hybrid Analysis також пропонує величезну базу даних з понад 767 мільйонами IoC, за якими користувачі можуть здійснювати пошук. Крім того, платформа дозволяє користувачам шукати зразки шкідливого програмного забезпечення, використовуючи правила YARA або зіставлення рядкових і шістнадцяткових шаблонів на байтовому рівні, забезпечуючи комплексне рішення для виявлення і розуміння загроз шкідливого програмного забезпечення. Інструмент доступний як у безкоштовній, так і в преміум-версії, що робить його легкодоступним для будь-якої організації. Використовуючи безкоштовну версію, користувачі можуть сканувати до 20 файлів; з преміум-версією вони можуть сканувати тисячі файлів, а також отримати доступ до веб-сервісу, API, моніторів виконання, контролера балансування навантаження, технології гібридного аналізу, генератора звітів, всіх індикаторів, сигнатур і скриптів[5].

Hex-rays IDA Pro

IDA Pro - провідний інструмент аналізу бінарного коду, який широко використовується аналітиками програмного забезпечення, реверс-інженерами, аналітиками шкідливих програм і фахівцями з кібербезпеки. Він включає в себе потужний дизасемблер і універсальний налагоджувач для комплексного аналізу, і аналізує двійкові файли за лічені секунди.

Як дизасемблер, IDA Pro генерує вихідний код на асемблері з машинного коду, роблячи складний код більш зрозумілим для людини. Налагоджувач підтримує декілька цілей налагодження, працює з віддаленими додатками та надає можливості крос-платформного налагодження. IDA Pro пропонує

інтерактивне середовище, яке дозволяє аналітикам швидко скасовувати його рішення або надавати підказки для більш інтуїтивного аналізу двійкового коду. IDA Pro повністю програмується за допомогою надійної макроподібної мови (IDC або IDAPython) для автоматизації простих і середніх за складністю завдань. Він сумісний з багатьма форматами файлів, процесорами і платформами, що забезпечує безперешкодну інтеграцію і дозволяє користувачам запускати тисячі тестових кейсів 24/7.

Відкрита архітектура плагінів IDA Pro дозволяє легко розширювати його функціональність, а також включає в себе сервер Lumina для покращення лістингу дизасемблювання та технологію швидкої ідентифікації та розпізнавання бібліотек (F.L.I.R.T.) для розпізнавання стандартних бібліотечних функцій. Довівши свою ефективність, зрілість і безпеку, IDA Pro постійно розвивається завдяки суттєвим оновленням і підтримує різні операційні системи, такі як Windows, Linux і macOS[5].

Joe Security Joe Sandbox

Joe Security - компанія, що спеціалізується на розробці систем аналізу шкідливого програмного забезпечення для виявлення шкідливого програмного забезпечення та криміналістичних цілей. Їхні унікальні технології дозволяють проводити поглиблений аналіз шкідливого програмного забезпечення, який раніше був недосяжним. Вони пропонують свої послуги або через хмарну платформу, або як окремий програмний пакет.

Joe Sandbox Cloud, що базується на продукті Joe Sandbox Ultimate, - це веб-сервіс, який дозволяє фахівцям з кібербезпеки завантажувати файли та URL-адреси для тестування. Цей сервіс надає звіти про аналіз, які можна завантажити, та інші важливі дані розвідки загроз. Joe Sandbox не покладається на статичний аналіз, натомість використовує метод детонації в безпечному середовищі, що дозволяє досягти вищого рівня виявлення та розуміння шкідливого програмного забезпечення. Глибокий аналіз шкідливого програмного забезпечення, що надається Joe Security, охоплює різні системи, такі як Windows, Android, macOS і Linux. Послуга доступна як для віртуальних, так і для фізичних машин і включає

в себе плагіни для декомпіляції та гіпервізора на додаток до основних функцій, доступних в Joe Sandbox Cloud.

Всі звіти аналізу залишаються конфіденційними, а хмарна лабораторія аналізу шкідливого програмного забезпечення доступна з виділеним доступом для ручного аналізу шкідливого програмного забезпечення та тестування безпеки кінцевих точок. Загалом, послуги Joe Security допомагають організаціям аналізувати загрози кібербезпеки та отримувати цінну інформацію для захисту[5].

PeStudio

PeStudio - це інструмент аналізу шкідливого програмного забезпечення, який спрощує процес первинної оцінки для фахівців з безпеки. Статичний аналіз виконуваних файлів спрощується за допомогою PeStudio, якому довіряють команди реагування на комп'ютерні надзвичайні ситуації (CERT), операційні центри безпеки (SOC) і лабораторії цифрової криміналістики по всьому світу.

PeStudio пропонує дві версії - стандартну та професійну, які підходять як для приватного, так і для професійного використання. Стандартна версія, яка є безкоштовною, включає в себе такі функції, як виявлення підписів файлів, виявлення жорстко закодованих URL і IP-адрес, збір метаданих, імпорт, експорт, рядки, маніфест, ресурси, оверлейний пошук і інтеграцію з VirusTotal для оцінки. Професійна версія, вартістю 139 євро за користувача на рік, включає в себе всі стандартні функції. Додаткові функції професійної версії включають пакетну обробку за допомогою pestudiox.exe, організацію елементів за групами і кольорами, створення файлів звітів у форматі XML, відображення матриці MITRE ATT&CK, відображення просторів імен .NET і дамп вбудованих файлів .NET[5].

Microsoft Process Monitor

Process Monitor - це інструмент моніторингу в режимі реального часу, розроблений Windows Sysinternals, підрозділом веб-сайту Microsoft TechNet. Цей безкоштовний інструмент призначений для відстеження всіх дій з файловою системою в Microsoft Windows або Unix-подібних операційних системах, його

можна запускати в Windows 10 або Windows Server 2012 і новіших версіях. Інструмент здатний відстежувати і записувати всі дії, спрямовані проти реєстру Microsoft Windows, виявляючи невдалі спроби читання і запису ключів реєстру.

Process Monitor пропонує детальний моніторинг системи; кожен процес можна відстежувати і реєструвати в режимі реального часу. Він також дозволяє здійснювати розширену фільтрацію за певними ключами, процесами, ідентифікаторами та значеннями процесів, надаючи користувачам глибоке розуміння того, як програми взаємодіють з файлами та бібліотеками DLL. Він також допомагає виявляти критичні помилки в системних файлах. Process Monitor також пропонує неруйнівну фільтрацію, широкі властивості подій, надійну інформацію про процеси, повні стеки потоків з інтегрованою підтримкою символів для кожної операції та одночасне ведення журналу у файл. Завдяки своїм універсальним і потужним можливостям Process Monitor відіграє центральну роль в усуненні системних несправностей і виявленні шкідливого програмного забезпечення.

Завдяки легкому перегляду і доступу до інформації про зображення процесу і відформатованих даних, які не поміщаються в стовпці, Process Monitor пропонує варіанти конфігурації для стовпців властивостей подій, що налаштовуються. Його вдосконалена архітектура журналювання може обробляти великі обсяги захоплених подій і даних журналів, що робить його безцінним інструментом для підприємств, які прагнуть підтримувати контроль над своїми IT-системами[5].

REMnux

REMnux - це інструментарій на базі Linux, призначений для реінжинірингу та аналізу шкідливого програмного забезпечення. Він пропонує кураторську колекцію безкоштовних інструментів, розроблених спільнотою, щоб допомогти аналітикам у дослідженні шкідливого програмного забезпечення без клопоту з пошуком, встановленням та налаштуванням кожного інструменту окремо.

Ядром REMnux є дистрибутив Linux на базі Ubuntu, який містить численні інструменти, що використовуються аналітиками шкідливого програмного

забезпечення для різних завдань. Ці завдання включають вивчення статичних властивостей підозрілих файлів, статичний і динамічний аналіз шкідливого коду, аналіз пам'яті на заражених системах, дослідження мережевих взаємодій, дослідження системних взаємодій шкідливого програмного забезпечення, а також аналіз шкідливих документів і даних про загрози. На сайті з документацією до набору можна знайти повний перелік інструментів REMnux, а також інструкції з використання для кожного інструменту. Щоб почати використовувати REMnux, користувачі можуть завантажити віртуальний пристрій, встановити його на виділену систему, додати до існуючої машини або запустити його як Docker-контейнер.

Крім того, REMnux пропонує Docker-образи популярних інструментів аналізу шкідливого програмного забезпечення, що дозволяє користувачам запускати їх як контейнери без необхідності встановлювати інструменти безпосередньо в системі. Така універсальність робить REMnux цінним ресурсом для аналітиків шкідливого програмного забезпечення, які шукають комплексний набір інструментів для своїх розслідувань[5].

VirusTotal

VirusTotal - це краудсорсингова платформа для аналізу загроз, яка дозволяє користувачам аналізувати підозрілі файли, домени, IP-адреси та URL-адреси на наявність потенційного шкідливого програмного забезпечення та інших порушень. Об'єднуючи інформацію з різних антивірусних продуктів і систем онлайн-сканування, VirusTotal надає командам безпеки комплексний контекст і розширені можливості для проактивного захисту своїх мереж від кіберзагроз.

Платформа аналізує контент за допомогою понад 70 антивірусних сканерів і служб блокування URL-адрес/доменів, при цьому користувачам доступні різні способи надсилання файлів. Надсилаючи контент до VirusTotal, користувачі сприяють підвищенню світових стандартів IT-безпеки. Надіслані файли та URL-адреси аналізуються, а результати надсилаються відправнику, партнерам з експертизи та спільноті VirusTotal, що сприяє спільному підходу до виявлення шкідливого контенту та виявлення помилкових спрацьовувань. Зведені дані

VirusTotal надають цінну інформацію для фахівців з кібербезпеки та розробників продуктів безпеки, допомагаючи організаціям виявляти та протидіяти новим загрозам.

На додаток до основного аналізу, VirusTotal пропонує такі функції, як Спільнота, де користувачі можуть коментувати файли та URL-адреси і ділитися нотатками один з одним. Хоча базове рішення є безкоштовним, клієнти Premium VirusTotal мають доступ до більш просунутих інструментів і ресурсів, що дозволяє їм виконувати складний пошук на основі критеріїв для виявлення шкідливих файлів і розробки нових засобів захисту[5].

Wireshark

Wireshark - це широко використовуваний аналізатор пакетів з відкритим вихідним кодом, призначений для усунення несправностей мережі, аналізу, розробки програмного забезпечення та комунікаційних протоколів, а також для освітніх цілей. Як провідний аналізатор мережевих протоколів, Wireshark пропонує всебічний, мікроскопічний погляд на мережеву активність, що робить його галузевим стандартом у багатьох сферах та установах.

Деякі ключові особливості Wireshark включають сумісність з різними платформами, такими як Windows, Linux, OS X, FreeBSD, NetBSD та іншими; можливість виконувати перехоплення в реальному часі і аналіз в автономному режимі; підтримку дешифрування різних протоколів, таких як IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP і WPA/WPA2. Крім того, Wireshark надає можливості глибокої перевірки сотень протоколів, які постійно оновлюються. Крім того, перехоплені мережеві дані можна переглядати і аналізувати за допомогою графічного інтерфейсу користувача або утиліти TShark в режимі TTY. Пропонуючи універсальну функціональність, Wireshark має потужні фільтри відображення і багатий аналіз VoIP, що спрощує аналіз мережевих даних. Крім того, Wireshark підтримує численні формати файлів захоплення, такі як tcpdump (libpcap), Pcap NG, Catapult DCT2000 і Microsoft Network Monitor, серед інших. Вихідні дані платформи можна експортувати в XML, PostScript, CSV або звичайний текстовий формат для полегшення звітування та обміну. Ця

платформа має дуже інтуїтивно зрозумілий інтерфейс і легко налаштовується. Крім того, є багато навчальних посібників і документації. Таким чином, ми рекомендуємо Wireshark будь-яким організаціям, які шукають зручний, але повнофункціональний інструмент для аналізу шкідливого програмного забезпечення[5].

Огляд інструментів дозволяє побачити, як теоретичні методи реалізуються на практиці за допомогою сучасного програмного забезпечення. Разом із цим необхідно враховувати нормативні вимоги, які регулюють використання таких засобів у сфері кібербезпеки.

1.5 Нормативна-правова база у сфері кібербезпеки

З розвитком інформаційних технологій проблема шкідливого програмного забезпечення набула глобального характеру. З метою забезпечення ефективного захисту інформаційних ресурсів на національному рівні сформовано систему нормативно-правових актів, які регулюють основні засади кібербезпеки, в тому числі заходи щодо запобігання та протидії шкідливому програмному забезпеченню.

До основних нормативно-правових актів України у сфері кібербезпеки належать:
Закон України «Про основні засади забезпечення кібербезпеки України» №2163-VIII від 5 жовтня 2017 року[6].

Цей Закон визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» №80/94-ВР від 5 липня 1994 року[7].

Цей Закон регулює відносини у сфері захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах

Кримінальний кодекс України:

Стаття 361. Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж[8].

Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж - карається штрафом від однієї тисячі до трьох тисяч неоподатковуваних мінімумів доходів громадян або пробаційним наглядом на строк до трьох років, або обмеженням волі на той самий строк.

Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, караються штрафом від трьох тисяч до семи тисяч неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк від двох до п'яти років, або позбавленням волі на той самий строк.

Стаття 361-1. Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут[9].

Створення з метою протиправного використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, караються штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або позбавленням волі на строк до трьох років.

Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, караються позбавленням волі на строк до п'яти років.

Доктрина інформаційної безпеки України (Указ Президента №47/2017)[10].

Цим документом було визначено поширення шкідливого ПЗ як ключову загрозу інформаційній безпеці України в інформаційному просторі та встановлює пріоритет державної політики у сфері кіберзахисту.

У сфері кібербезпеки зокрема протидії шкідливому ПЗ, фігурують такі національні стандарти:

ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту системи управління інформаційною безпекою[11].

Встановлює загальні вимоги до побудови, впровадження, експлуатації та постійного удосконалення систем управління інформаційною безпекою.

ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки[12].

Містить рекомендації щодо заходів протидії шкідливому програмному забезпеченню.

Особливу роль у міжнародній координації боротьби з кіберзлочинністю відіграє:

Конвенція про кіберзлочинність (Будапештська конвенція) 2001 року

Будапештська конвенція про кіберзлочинність, офіційно відома як Конвенція Ради Європи про кіберзлочинність (Convention on Cybercrime, Council of Europe) – перший міжнародний договір, спрямований на боротьбу з інтернет-злочинністю та комп’ютерною злочинністю (кіберзлочинністю), була відкрита для підписання 23 листопада 2001 року як перший міжнародний договір, спрямований на боротьбу зі злочинами, що вчиняються через Інтернет та інші комп’ютерні мережі. Конвенція була створена у відповідь на зростання кіберзлочинності наприкінці 1990-х років у зв’язку із збільшенням використання Інтернету. Станом на квітень 2023 року Конвенцію ратифікували 68 країн (Україна ратифікувала Конвенцію 7 вересня 2005 року; проти Конвенції виступає рф і зазвичай відмовляється співпрацювати з правоохоронними органами у розслідуванні кіберзлочинів)[13].

Правове регулювання створює рамки для безпечного використання ІТ-засобів і захисту від кіберзагроз. Завершимо розділ узагальненням ключових

положень і висновків щодо методів виявлення шкідливого ПЗ та нормативного супроводу.

Висновки до розділу 1

Класифікація шкідливого ПЗ не є універсальною; найпоширеніші підходи базуються на формальних ознаках та операційній системі призначення. За формальними ознаками виділяють віруси, трояни, черв’яки та інші класи, а за ОС виявлено, що переважна більшість загроз націлена на Windows.

Для захисту використовуються спеціалізовані інструменти і правові норми. Сучасні антивірусні продукти поєднують сигнатурний, поведінковий, проактивний та евристичний аналіз для виявлення загроз. Водночас правова база України передбачає кримінальну відповідальність за створення й розповсюдження шкідливого коду (до 5 років позбавлення волі за ст. 361-1 ККУ), що підсилює протидію кіберзагрозам.

Розділ 2. Методи виявлення шкідливого програмного забезпечення

2.1. Сигнатурний аналіз як традиційний метод виявлення

Майже 90% кібератак - це відомі методи, які можуть виявити належні системи, але більшість організацій не мають найкращого захисту. Виявлення на основі сигнатур є життєво важливим аспектом кібербезпеки. Воно пропонує певні переваги, але також має певні недоліки. Нижче я розберу їх, щоб розглянути як можна зміцнити свій захист від нових загроз.

Що таке сигнатурний аналіз?

Виявлення на основі сигнатур - одна з найпоширеніших методик у кібербезпеці. По суті, це метод, який виявляє загрози шляхом пошуку відомих шаблонів, або «сигнатур», в даних або активності системи. Ці сигнатури заздалегідь визначені і зберігаються в базі даних, що дозволяє системам виявлення легко порівнювати з ними вхідні дані[14].

Чому це важливо:

Виявлення на основі сигнатур працює так, ніби система безпеки перевіряє вхідні дані на відповідність відомому шаблону загрози. Припустимо, організація отримала фішинговий лист, в якому у шкідливому вкладенні міститься певний унікальний код, який був помічений під час попередніх атак. Система виявить цей код і одразу позначить лист як шкідливий, а отже, заблокує його отримання. Такий підхід забезпечує швидку ідентифікацію та стримування таких загроз на основі встановлених сигнатур, що робить його важливим елементом кібербезпеки.

Як працює сигнатурне виявлення.

Крок 1. Генерація сигнатур: Коли виявляється нова загроза, наприклад, вірус або шкідливе програмне забезпечення, дослідники вивчають її поведінку і генерують унікальний відбиток, або сигнатуру. Це може бути певний шаблон коду або послідовність дій, які він виконує.

Крок 2. База даних сигнатур: Цей підпис зберігається в центральній базі даних. Інструменти безпеки, такі як антивірусне програмне забезпечення або системи виявлення вторгнень, перевіряють наявність загрози за цією базою даних.

Крок 3. Сканування та співставлення: Коли дані або дії проходять через систему, цей інструмент безпеки сканує їх і намагається співставити зі збереженими сигнатурами. Якщо вони збігаються, система позначає їх як зловмисні[14].

Рис 2.1 Покрокова інструкція

Переваги виявлення за сигнатурами

Виявлення на основі сигнатур є надійним інструментом протягом десятиліть, а його сильні сторони полягають у точності та простоті. Давайте розберемося, чому цей метод досі залишається наріжним каменем сучасної кібербезпеки.

Чому він ефективний:

Швидкість і точність: він неймовірно швидко ідентифікує відомі загрози, оскільки підписи є специфічними та попередньо перевіреними.

Низький рівень хибних спрацьовувань: Оскільки він покладається на точні збіги, ймовірність позначення легітимних файлів або дій як зловмисних є відносно низькою.

Простота: Концепція та реалізація прості, що дозволяє легко вбудовувати їх в існуючі інфраструктури безпеки.

Доведена ефективність: Виявлення на основі сигнатур - це усталений метод, який протягом десятиліть доводив свою ефективність у боротьбі з відомими загрозами.

Недоліки виявлення на основі сигнатур:

Звіти з кібербезпеки показують, що понад 60% успішних атак використовують раніше невидимі вразливості, оминаючи традиційні засоби захисту.

Ця статистика підкреслює нагальну потребу в розумінні обмежень виявлення на основі сигнатур та пошуку додаткових рішень[14].

Проблема:

Нездатність виявляти нові загрози: Він не виявляє атаки нульового дня, які представляють собою нові загрози, що ще не мають сигнатур, а також поліморфні шкідливі програми, коди яких постійно змінюються.

Залежність від оновлень: Система значною мірою залежить від оновлень. Система настільки хороша, наскільки хороша її база даних. Якщо сигнатури не оновлюються регулярно, вона не буде ефективною.

Реактивний підхід: За своєю природою він є реактивним, оскільки може виявляти лише ті загрози, які вже були знайдені та проаналізовані[14].

Що можна зробити?

Можна поєднувати системи на основі сигнатур з евристичними методами або методами виявлення аномалій, щоб ще більше посилити свою систему кібербезпеки.

Також раджу регулярно оновлювати антивірус або систему виявлення вторгнень, щоб включати найновіші сигнатури загроз.

Незважаючи на свою точність, сигнатурний метод виявлення має обмеження у випадках нових або модифікованих загроз. Тому наступний підрозділ буде присвячено еврестичним методам, які здатні доповнити цю слабку сторону.

2.2. Евристичні методи виявлення: принципи та особливості

Що таке евристичне виявлення?

Евристичне виявлення - це метод, який використовується багатьма програмними рішеннями для комп'ютерної безпеки для виявлення загроз і нових варіацій існуючих вірусів, які раніше не були помічені або каталогізовані у файлах визначення вірусів. Це проактивний підхід у боротьбі з кіберзагрозами, що забезпечує перевагу систем захисту в умовах, коли цифрові загрози регулярно еволюціонують[15].

У практиці комп'ютерного програмування та безпеки евристика - це набір запрограмованих інструкцій, які проводять аналіз і діагностику, щоб забезпечити вирішення проблеми, яка зазвичай не може бути вирішена за допомогою звичайних методів. Евристичний аналіз розширює межі, щоб перевершити звичайні моделі ідентифікації вірусів, коли виявлені загрози порівнюються з каталогом відомих загроз. Натомість він інтелектуально визначає наміри та можливості потенційних загроз, досліджуючи такі дії, як створення копій програмних скриптів, розповсюдження, переписування скриптів та інші дії, що зазвичай практикуються вірусами.

Евристичне виявлення в програмному забезпеченні для кібербезпеки, що ґрунтується на принципах вирішення проблем, навмисно розроблене для моделювання різних потенційних стратегій, які можуть вирішити проблему (нові інфекції) шляхом навчання або адаптації на основі досвіду. Програма комп'ютерної безпеки використовує евристику, що імітує можливості людського мозку - опрацьовує потенційні рішення, коли стикається з неідентифікованими проблемами або загрозами.

Використовуючи алгоритми, що враховують кілька факторів, евристичне виявлення розширює сферу своєї дії, дозволяючи відрізнити нешкідливі програмні скрипти від шкідливих вірусів. Крім розрізнення нешкідливих і шкідливих скриптів, евристичне виявлення також виконує ще одну основну

функцію: раннє виявлення. Це, як правило, передбачає виявлення потенційно шкідливого програмного забезпечення та ізоляцію його до того, як воно спричинить зараження системи.

На відміну від статичних методів виявлення загроз, з огляду на те, що ландшафт кіберзагроз постійно змінюється, регулярно з'являються нові віруси. Евристичне виявлення доводить свою здатність адаптуватися до цих нових загроз, розширюючи можливості антивірусного програмного забезпечення та надаючи йому підвищену здатність виявляти шкідливий код, вбудований у програмне забезпечення черв'яків та вірусів, який статичні методи розпізнавання не обов'язково помітять.

Евристичне виявлення не позбавлене недоліків. Як і в будь-якому методі, що залежить від стратегічного підходу, хибні спрацьовування є серйозною проблемою, коли нешкідливе або доброякісне програмне забезпечення помилково ідентифікується як шкідливе або зловмисне. Це може призвести до вимкнення або видалення функціональних програм через помилкове переконання, що вони становлять загрозу, що спричиняє перебої в роботі та незручності для користувачів. Удосконалення евристичних процесів для досягнення тонкого балансу між надмірною необмеженістю (а отже, меншою ймовірністю помилкової ідентифікації безпечних дій як підозрілих) і надмірною обережністю (а отже, схильністю вважати прості дії зловмисними і запускати хибнопозитивні сповіщення) може виявитися непростим завданням.

Евристичне виявлення логічно вимагає більших обчислювальних ресурсів, ніж звичайні методи виявлення вірусів. Оскільки воно аналізує і сканує широкий спектр програмного коду, шукаючи будь-які ознаки підозрілої або зловмисної діяльності, це може призвести до значного збільшення використання системних ресурсів, що впливає на швидкість роботи комп'ютера і його ефективність.

Незважаючи на ці виклики, евристичне виявлення залишається фундаментальною основою для зміцнення інфраструктури кібербезпеки та антивірусного захисту. Оскільки цифровий простір продовжує культивувати і вітати новознайдену складність і відкритість, мережі і системи можуть стати

жертвами досі небаченого шкідливого програмного забезпечення і кібератак. Для проактивного захисту від сучасних кіберзагроз процеси евристичного виявлення продовжують вдосконалюватися в постійному прагненні до надійного і динамічного антивірусного захисту та кібербезпеки.

Евристичне виявлення є незамінним інструментом в арсеналі програмного забезпечення для кібербезпеки. Відходячи від традиційного підходу, що полягає у створенні архіву розпізнаних загроз, він пропонує адаптивні, випереджаючі рішення та детектори. Він без особливих зусиль виявляє загрози ще до того, як пролунають тривожні дзвіночки, створюючи основу для більш агресивного, превентивного та ефективного підходу до боротьби з кіберзагрозами порівняно з традиційними методами виявлення вірусів[15].

Як працює евристичний аналіз?

Евристичний аналіз виконується за допомогою декількох різних методів:

1. Статичний евристичний аналіз

Статичний евристичний аналіз передбачає вивчення вихідного коду програми і порівняння його з вихідним кодом відомих вірусів, які вже були зареєстровані в базі даних. Якщо достатньо збігів з тим, що є в базі даних, код позначається як потенційна загроза.

2. Динамічний евристичний аналіз

Динамічний евристичний аналіз використовує віртуальну машину, яка діє як пісочниця. Пісочниця - це безпечне, ізольоване середовище, в якому програма може виконуватися, не впливаючи на решту системи або мережі. Під час динамічного евристичного аналізу середовище пісочниці дозволяє запустити файл, щоб ви могли побачити, що він зробить, якщо буде запущений у чутливому середовищі.

Наприклад, під час динамічного евристичного аналізу програма, за якою ведеться спостереження, може самовідтворюватися, намагатися залишитися в резидентній пам'яті після виконання, перезаписувати файли або робити інші речі, на які часто запрограмовані віруси[16].

Переваги та недоліки евристичного аналізу

У евристичного аналізу є кілька переваг і недоліків, але, незважаючи на недоліки, він все ще залишається дуже потужним інструментом.

Переваги:

Евристичний аналіз може виявляти не лише модифіковані форми існуючих шкідливих програм. Він також може виявляти раніше невідомі шкідливі програми. Це відбувається тому, що він аналізує поведінку потенційної загрози, а не ім'я її файлу.

Цей метод аналізу також зменшує кількість хибних спрацьовувань, оскільки деякі типи поведінки є дуже специфічними для шкідливих програм, і евристичний аналіз може їх ідентифікувати, точно визначаючи загрозу. Наприклад, якщо програма намагається видалити файли, які потрібні операційній системі, вона, швидше за все, є шкідливою. Евристичний аналіз може виявити таку поведінку і позначити загрозу, щоб її можна було видалити.

З іншого боку, просто вивчивши сигнатуру програми і порівнявши її з сигнатурами відомих загроз, загроза може залишитися непоміченою, просто тому, що вона не збігається з відомими загрозами. Це часто трапляється, коли ми маємо справу з загрозою нульового дня або раніше невідомою загрозою. Евристичний аналіз може позначити загрозу на основі того, що вона робить, незалежно від того, чи була вона вже зареєстрована в системі управління загрозами.

Недоліки:

Евристичний аналіз призначений для виявлення відомої поведінки загрози. Якщо загроза не виконує жодних дій, на розпізнавання яких запрограмована технологія виявлення загроз, вона може вислизнути з-під радара.

Щоб проілюструвати це, припустимо, що ваше антивірусне програмне забезпечення було розроблене так, щоб позначати програму, яка намагається видалити файли, необхідні вашій операційній системі, але не файли, які розшифровують самі себе. У цьому випадку, якщо антивірус натрапить на

саморозшифрований файл, він може не помітити, що це загроза - навіть якщо така дія є типовою для загроз.

Існує також ймовірність того, що антивірусне/антивірусне програмне забезпечення використовує евристичне сканування на основі занадто широкого діапазону поведінки. У цьому прикладі евристичного аналізу процес може призвести до помилкового позначення нешкідливих файлів як загрозливих. Однак це частіше трапляється у старих програмах евристичного аналізу, тому якщо у вас новіша програма, яку нещодавно було оновлено, швидше за все, вона використовує сучасні методи, які обмежують кількість хибних спрацьовувань[16].

Евристика дозволяє виявляти загрози на основі підозрілої поведінки, що розширює можливості детекції. Продовжимо розгляд, зосередившись на ще більш динамічному підході – машинному навчанні.

2.3. Використання технологій машинного навчання для детектування шкідливого ПЗ

Алгоритми машинного навчання можуть аналізувати величезні обсяги даних. Вони можуть виявляти закономірності, які можуть вислизнути від людського спостереження і традиційного антивірусного програмного забезпечення. Системи можуть набувати знань і покращувати свою продуктивність без явного програмування. Процес передбачає надання алгоритмам значного обсягу даних для виявлення закономірностей і кореляцій. На основі виявлених закономірностей алгоритми можуть прогнозувати або визначати відповідний курс дій для нових даних.

Ідентифікація шкідливого програмного забезпечення може бути полегшена завдяки використанню методів машинного навчання:

Завдяки аналізу великих обсягів даних про шкідливе програмне забезпечення алгоритми машинного навчання здатні визначати шаблони та характеристики шкідливого програмного забезпечення.

Після завершення навчання ці алгоритми демонструють здатність точно виявляти нові екземпляри шкідливого програмного забезпечення.

Такий підхід потенційно може підвищити ефективність виявлення та видалення шкідливого програмного забезпечення.

Він може полегшити виявлення нових ризиків для безпеки[17].

У цій частині ми розглянемо потенціал машинного навчання для полегшення та покращення ідентифікації шкідливого програмного забезпечення з більшою легкістю та точністю.

Роль машинного навчання у виявленні шкідливих програм

Машинне навчання - це процес, який дозволяє інструментам самостійно набувати здатності змінювати свою поведінку без чітких інструкцій. Процес передбачає надання алгоритмам значної кількості даних, щоб вони могли виявляти кореляції та асоціації. На основі цих закономірностей алгоритми здатні передбачати або приймати рішення щодо обробки нових даних[17].

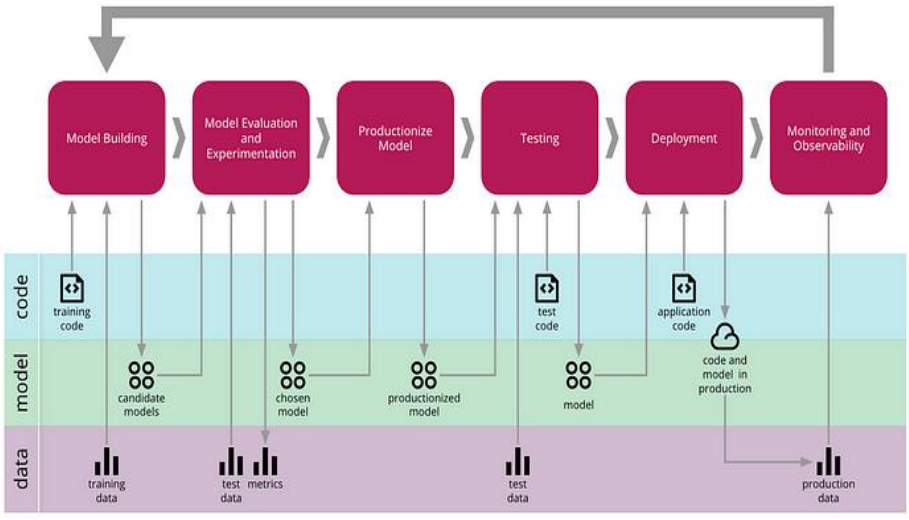

Рис 2.2 Життєвий цикл машинного навчання, що деталізує етапи від побудови моделі, оцінки та впровадження до тестування, розгортання та моніторингу, з відповідними потоками даних, моделі та коду.

Зазвичай процес машинного навчання передбачає включення наступних кроків:

Крок 1. Збір даних: Велика кількість даних збирається та організовується у спосіб, придатний для аналізу.

Крок 2. Попередня обробка даних: Дані очищаються і готуються до аналізу. Це включає такі завдання, як видалення дублікатів, обробка відсутніх значень і перетворення даних у відповідний формат.

Крок 3. Вилучення ознак: Витягуються характеристики даних, щоб показати закономірності та взаємозв'язки. Цей етап має вирішальне значення в машинному навчанні, оскільки якість ознак впливає на точність і ефективність моделі.

Крок 4. Навчання моделі: Алгоритм машинного навчання навчається на вилучених ознаках, щоб вивчити закономірності та взаємозв'язки в даних.

Крок 5. Оцінка моделі: Ефективність моделі оцінюється на окремому наборі даних, щоб перевірити її точність та узагальнюваність.

Крок 6. Розгортання моделі: Навчена модель розгортається для прогнозування або прийняття рішень на нових даних[17].

Враховуючи безперервний характер машинного навчання, включення додаткових даних має потенціал для підвищення продуктивності моделі. Методи машинного навчання можна умовно поділити на три типи: контрольовані, неконтрольовані та методи на основі підкріплення. Далі ми розглянемо, як ці групи можна використовувати для виявлення шкідливого програмного забезпечення.

Існують різні методи машинного навчання, зокрема контрольовані, неконтрольовані та методи на основі підкріплення. Існують різні методології використання методів машинного навчання для виявлення шкідливих програм.

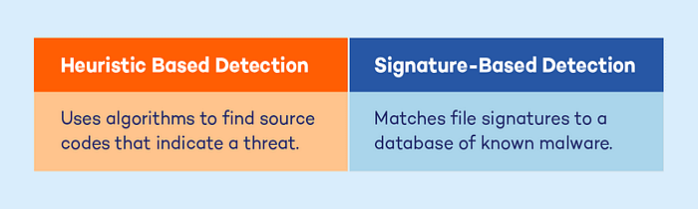

Рис 2.3 Порівняння евристичного виявлення, яке використовує алгоритми для виявлення потенційних загроз у вихідних кодах, з виявленням на основі сигнатур, яке порівнює сигнатури файлів з базою даних відомого шкідливого програмного забезпечення.

Виявлення на основі машинного навчання: Алгоритми аналізують величезні масиви даних про відоме шкідливе програмне забезпечення, щоб знайти шаблони та атрибути шкідливого програмного забезпечення. Цей метод дозволяє виявляти відомі та неочікувані загрози, а також скоротити час виявлення та видалення шкідливого програмного забезпечення.

Шкідливе програмне забезпечення можна знайти до, під час і після атаки за допомогою машинного навчання. Алгоритми машинного навчання можуть переглядати вкладення електронної пошти або URL-адреси до того, як вони будуть завантажені, відстежувати мережеві дані на предмет дивної поведінки та знаходити шкідливе програмне забезпечення на вже заражених комп'ютерах[17].

Навчання під контролем: Мітки даних навчили систему розрізняти шкідливі та безпечні файли. Вона розуміє складні зв'язки між даними і має рацію щодо відомих ризиків. Система потребує багато маркованої інформації і може не спрацювати для невідомих ризиків.

Навчання без нагляду: Алгоритм навчається на основі структури даних, а не міток. Він може виявляти несподівані небезпеки та викиди даних. Він може пропустити або неправильно ідентифікувати загрози.

Навчання з підкріпленням: Алгоритм отримує призи або покарання залежно від того, наскільки добре він працює. Він може реагувати на нові загрози і вчитися на минулому досвіді. Він потребує багато навчальної інформації і може не спрацювати для ризиків, які важко передбачити.

Кожен алгоритм машинного навчання має свої плюси і мінуси, а обраний метод залежить від конкретного випадку використання і наданих даних[17].

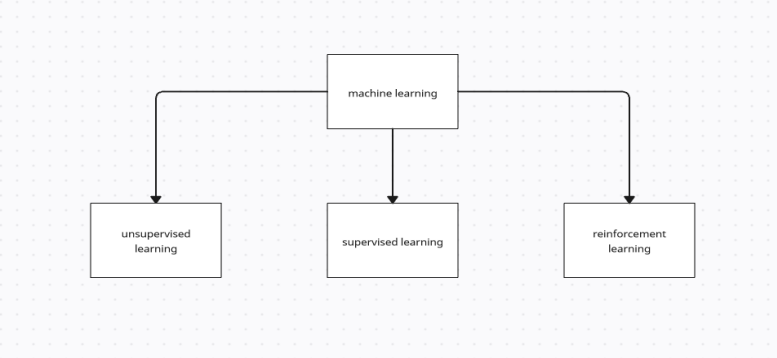

Рис 2.4 Представлення основних трьох методів ML (Unsupervised Learning - Supervised Learning - Reinforcement Learning)

Вигоди та переваги

Інтеграція машинного навчання в системи виявлення шкідливого програмного забезпечення дає численні переваги, які підвищують рівень безпеки та операційну ефективність. Ці переваги пов'язані з розширеними можливостями алгоритмів машинного навчання аналізувати величезні обсяги даних, адаптуватися до нових загроз і автоматизувати процеси виявлення. У наступному розділі висвітлено ключові переваги використання машинного навчання для виявлення шкідливого програмного забезпечення:

Висока точність: Алгоритми машинного навчання можуть знаходити шкідливе програмне забезпечення, якщо вони навчаються на великій кількості шкідливих і безпечних файлів, які були марковані. Це позбавляє від помилкових спрацьовувань і відхилень та запобігає потраплянню шкідливого програмного забезпечення.

Автоматизація: Шкідливе програмне забезпечення може бути знайдене автоматично за допомогою алгоритмів машинного навчання, що економить час і ресурси експертів з безпеки. Це добре для великих систем з великим трафіком і можливими ризиками.

Адаптивність: Алгоритми, які використовують машинне навчання, можуть адаптуватися до нових небезпек і вчитися на своїх минулих помилках. Оновлені та перенавчені моделі машинного навчання можуть знаходити нові хвороби.

Машинне навчання може підвищити швидкість, точність, адаптивність і масштабованість ідентифікації шкідливого програмного забезпечення. Це може допомогти запобігти зараженню шкідливим програмним забезпеченням та іншим проблемам безпеки. Ось п'ять поширених методів машинного навчання, за допомогою яких можна підвищити точність і швидкість виявлення шкідливого програмного забезпечення:

Вилучення ознак. Вони можуть ефективно витягувати ознаки, пов'язані зі шкідливим програмним забезпеченням, такі як розмір, тип і поведінка. Аналізуючи ці характеристики, алгоритми машинного навчання можуть визначати тенденції шкідливого програмного забезпечення, тим самим підвищуючи точність і швидкість виявлення шкідливого програмного забезпечення.

Розпізнавання шаблонів. Розпізнавання шаблонів у даних, які можуть бути пропущені при аналізі людиною. Вивчаючи великі масиви даних, ці алгоритми можуть виявляти тенденції в поведінці шкідливого програмного забезпечення, такі як типи файлів, мережевий трафік і поведінкові аномалії. Ця можливість дозволяє швидше і точніше виявляти шкідливе програмне забезпечення.

Навчання на власному досвіді. Системи машинного навчання постійно вдосконалюються, виявляючи закономірності у великих масивах даних, які можуть бути пропущені аналітиками. Ці алгоритми розпізнають тенденції в поведінці шкідливого програмного забезпечення, включаючи типи файлів, мережевий трафік і дії. Цей безперервний процес навчання покращує здатність системи виявляти шкідливе програмне забезпечення з більшою швидкістю і точністю.

Розширений аналіз. Швидкий аналіз великих масивів даних для виявлення та реагування на загрози в режимі реального часу. Досліджуючи мережевий

трафік та інші джерела даних, ці алгоритми можуть миттєво виявляти шкідливе програмне забезпечення, ефективно запобігаючи інцидентам безпеки.

Автоматизація. Можливості автоматизації алгоритмів ML можуть значно зменшити навантаження на експертів з безпеки, автоматизуючи процес виявлення шкідливого програмного забезпечення. Це дозволяє швидко аналізувати великі масиви даних і швидко виявляти загрози, тим самим покращуючи загальний стан безпеки організації.

Виділення ознак, розпізнавання шаблонів, навчання на власному досвіді, аналіз у реальному часі та автоматизація можуть підвищити точність і швидкість виявлення шкідливого програмного забезпечення. Алгоритми машинного навчання можуть швидко та ефективно виявляти загрози, запобігаючи зараженню шкідливим програмним забезпеченням та іншим подіям, пов'язаним з безпекою[17].

Тематичні дослідження

Ці тематичні дослідження ілюструють трансформаційний потенціал машинного навчання для покращення виявлення та запобігання шкідливому програмному забезпеченню. Кожен приклад демонструє значні інвестиції та вражаючі результати з точки зору рівня виявлення, швидкості та загальної ефективності. Незважаючи на значні витрати, окупність інвестицій у вигляді покращення безпеки та зменшення загроз очевидна. Продовження досліджень і розробок у сфері машинного навчання матиме вирішальне значення для випередження еволюції загроз шкідливого програмного забезпечення та підтримання надійного захисту кібербезпеки:

Microsoft Defender Advanced Threat Protection.

Цей хмарний інструмент безпеки використовує машинне навчання для виявлення та запобігання сучасним загрозам шкідливого програмного забезпечення. Microsoft Defender ATP виявляє понад 7 мільйонів випадків використання шкідливого програмного забезпечення щомісяця. Він може похвалитися 99% рівнем виявлення. Повідомляється, що проект коштує 1 мільярд доларів. Високий рівень виявлення та значна кількість щомісячних

ідентифікацій шкідливого програмного забезпечення підкреслюють ефективність інвестицій Microsoft у машинне навчання для кібербезпеки[17].

Cylance.

Cylance використовує машинне навчання для виявлення та запобігання атакам шкідливих програм на кінцеві точки. З моменту свого дебюту програма вартістю 200 мільйонів доларів зупинила понад 9,5 мільйонів атак. Така значна кількість попереджених атак демонструє майстерність Cylance у використанні машинного навчання для захисту кінцевих точок. Проект коштує 200 мільйонів доларів. Використання Cylance машинного навчання виявилося економічно ефективним рішенням для зменшення загроз шкідливого програмного забезпечення на кінцевих точках[17].

Symantec Endpoint Protection.

Symantec інтегрує алгоритми машинного навчання в свою систему захисту кінцевих точок для запобігання загрозам шкідливого програмного забезпечення. Symantec стверджує, що її алгоритми машинного навчання дозволяють уникнути 99,9% атак "нульового дня". Такий високий показник запобігання атакам "нульового дня" підкреслює можливості передових алгоритмів Symantec. Як повідомляється, проект коштує 1,2 мільярда доларів. Значні інвестиції в алгоритми машинного навчання Symantec дозволили створити високоефективний захист від загроз "нульового дня"[17].

Palo Alto Networks.

WildFire від Palo Alto Networks використовує алгоритми машинного навчання для виявлення та запобігання атакам шкідливих програм. Він може виявити та запобігти атакам шкідливого програмного забезпечення за 5 хвилин з точністю 99%. Швидкий час виявлення та висока точність роблять WildFire потужним інструментом для боротьби із загрозами в режимі реального часу. Повідомляється, що проект коштує 750 мільйонів доларів. Інвестиції Palo Alto Networks дали змогу отримати швидке і точне рішення для виявлення шкідливого програмного забезпечення, що підвищило їхні загальні можливості кібербезпеки[17].

Cisco AMP для кінцевих точок.

Рішення Cisco AMP для кінцевих точок використовує машинне навчання для виявлення та запобігання атакам шкідливого програмного забезпечення. Cisco стверджує, що її алгоритми машинного навчання можуть виявляти та запобігати атакам зловмисного програмного забезпечення з точністю 99% всього за 3 секунди. Надзвичайно швидкий час виявлення і висока точність підкреслюють ефективність підходу Cisco до машинного навчання. Як повідомляється, проект коштує 2 мільярди доларів. Значні інвестиції Cisco в машинне навчання дозволили створити високоефективну і надійну систему виявлення шкідливого програмного забезпечення, що підкреслює важливість швидкості в кібербезпеці[17].

Подібні проекти з виявлення шкідливого програмного забезпечення на основі машинного навчання є поширеними сьогодні, оскільки воно набуває все більшого значення у виявленні та запобіганні шкідливому програмному забезпеченню в міру розвитку та ускладнення кіберзагроз.

Використання моделей штучного інтелекту значно покращує виявлення складних атак і нульового дня. Далі розглянемо інструменти поведінкового аналізу, зокрема пісочниці, що дозволяють оцінити активність ПЗ в ізольованому середовищі.

2.4. Пісочниці (sandboxing) та поведінковий аналіз

Пісочниця в аналізі шкідливого програмного забезпечення - це практика запуску потенційно шкідливого програмного забезпечення в контрольованому середовищі, яке називається "пісочниця". Пісочниця забезпечує безпечний та ізольований простір, де шкідливе програмне забезпечення може бути виконане та проаналізоване, не впливаючи на хост-систему або мережу.

Основна мета пісочниці - зрозуміти поведінку і функціональність шкідливого програмного забезпечення без ризику поставити під загрозу безпеку комп'ютера або мережі аналітика. Запускаючи шкідливе програмне забезпечення

в контрольованому середовищі, аналітики можуть спостерігати за його діями, відстежувати його взаємодію з системою і фіксувати будь-які зловмисні дії, які воно може спробувати виконати. Такий підхід допомагає зібрати цінну інформацію про можливості шкідливого програмного забезпечення, наприклад, про його мережеву взаємодію, модифікації файлів, зміни в реєстрі, системні виклики та потенційне корисне навантаження.

Пісочниця може бути виконана за допомогою різних методів та інструментів. Віртуальні машини (ВМ) зазвичай використовуються для цілей пісочниці. ВМ дозволяє аналітикам створювати ізольоване середовище операційної системи на хост-машині. Будь-які зміни, внесені шкідливим програмним забезпеченням у ВМ, можуть бути легко відкинуті, що гарантує безпеку хост-системи. Інші методи пісочниці включають контейнеризацію, яка забезпечує легку віртуалізацію, та інструменти динамічного аналізу, які пропонують середовища, подібні до пісочниці, для виконання та моніторингу шкідливого програмного забезпечення[18].

Переваги пісочниці в аналізі шкідливого програмного забезпечення:

Ізоляція та безпека: Пісочниці забезпечують безпечне середовище, утримуючи шкідливе програмне забезпечення у віртуальній машині або контейнері, запобігаючи зараженню хост-системи та поширенню в мережі.

Аналіз поведінки: Пісочниця дозволяє аналітикам спостерігати за діями та поведінкою шкідливого програмного забезпечення, такими як мережеві комунікації, модифікації файлів та системні взаємодії. Це допомагає визначити мету і потенційний вплив шкідливого програмного забезпечення.

Аналіз корисного навантаження: Виконуючи шкідливе програмне забезпечення в пісочниці, аналітики можуть вивчати корисне навантаження і будь-які потенційні дії, які воно може виконувати, такі як витік даних, компрометація системи або запуск подальших атак.

Динамічний аналіз: Пісочниця дозволяє відстежувати дії шкідливого програмного забезпечення в режимі реального часу, перехоплюючи системні виклики, взаємодію з API та мережевий трафік. Цей динамічний аналіз

допомагає зрозуміти поведінку шкідливого програмного забезпечення під час виконання[18].

Недоліки пісочничі в аналізі шкідливого програмного забезпечення:

Незважаючи на численні переваги пісочниці, існує ряд обмежень у її використанні для динамічного аналізу шкідливого програмного забезпечення. Використання автономних додатків-пісочниць, таких як Sandboxie, особливо коли вони підключені до Інтернету, не обов'язково гарантує безпеку системи, оскільки судове розслідування, проведене на основі різних висновків, показує артефакти, які були створені в системі в результаті виконання певного шкідливого програмного забезпечення. Шкідливе програмне забезпечення може створювати з'єднання за протоколом управління передачею (TCP) з віддаленими хостами. Деякі з подальших обмежень наведені нижче.

Методи ухилення: Розробники шкідливого програмного забезпечення стають все більш витонченими в розробці методів ухилення, щоб виявити, чи працює їхній код в середовищі пісочниці. Вони можуть змінювати свою поведінку або залишатися неактивними під час виконання в пісочниці, що ускладнює дослідникам шкідливого програмного забезпечення спостереження за повними можливостями шкідливого програмного забезпечення.

Чутливість до часу: Деякі шкідливі програми розроблені таким чином, щоб затримувати свою шкідливу діяльність на тривалий час, потенційно уникаючи виявлення в обмеженому в часі середовищі "пісочниці". Оскільки аналіз може тривати лише заздалегідь визначений час, зловмисна поведінка може бути не повністю зафіксована.

Обмеженість ресурсів: Здебільшого пісочниці працюють з обмеженими ресурсами для імітації реальних умов, що не дозволяє певним типам шкідливих програм повністю активуватися або виконати своє корисне навантаження, що призводить до неповного аналізу.

Відмінності в середовищі: Завжди дуже важко відтворити реальне виробниче середовище в умовах пісочниці, що призводить до того, що середовище може суттєво відрізнятися від реального цільового середовища, в

якому має працювати шкідливе програмне забезпечення. Шкідливе програмне забезпечення, призначене для конкретних конфігурацій або систем, безумовно, може поводитися по-іншому або взагалі не виконуватися в пісочниці, що призведе до неточних висновків.

Мережеві обмеження: Деякі шкідливі програми покладаються на реальну мережеву взаємодію для завершення своєї шкідливої діяльності. Пісочниця може не імітувати реальне мережеве середовище, що може перешкоджати аналізу певних аспектів поведінки шкідливого програмного забезпечення.

Поліморфне шкідливе програмне забезпечення: Цей тип шкідливого програмного забезпечення змінює структуру свого коду та зовнішній вигляд щоразу, коли заражає нову систему. Така адаптивна поведінка ускладнює ефективний аналіз шкідливого програмного забезпечення в умовах статичної пісочниці.

Юридичні та етичні проблеми: Аналіз реального шкідливого програмного забезпечення в середовищі пісочниці може потенційно порушувати закони або етичні норми, тому дослідники шкідливого програмного забезпечення повинні переконатися, що вони мають належний дозвіл і дотримуються правових та етичних протоколів при роботі зі справжніми зразками шкідливого програмного забезпечення[19].

Типи тестування в пісочниці

Різні варіанти використання та галузі вимагають різних середовищ тестування в пісочниці. Ось найпоширеніші типи, про які вам варто знати:

Пісочниця безпеки

Використовується в антивірусних програмах і системах виявлення вторгнень, пісочниця безпеки безпечно виконує потенційно шкідливий код для аналізу його поведінки, не піддаючи хост-систему загрозам. Наприклад, ви можете використовувати її для запуску підозрілих вкладень електронної пошти та перевірки на наявність шкідливого коду, перш ніж відкривати їх в основній мережі[20].

Одноразова пісочниця

Цей тип пісочниці створений для одноразового тестування і швидко скидається після використання. Він часто використовується в автоматизованих конвеєрах тестування. Це допомагає запускати автоматизовані тести кожного разу, коли вноситься новий код. Ознайомтеся з цим детальним посібником з автоматизації тестування[20].

Пісочниця для додатків

Операційні системи, такі як Android та iOS, розгортають пісочницю, щоб обмежити доступ додатків до несанкціонованих системних ресурсів або даних користувача, таких як місцезнаходження, контакти або камера, якщо користувач явно не надасть дозвіл у налаштуваннях програми[20].

Хмарна пісочниця

Як випливає з назви, це ізольоване середовище, де ви можете тестувати конфігурації серверів перед їх розгортанням. AWS, Azure та Google Cloud надають для цього середовища для розробки або тестування. Дізнайтеся про хмарне тестування докладніше[20].

Пісочниця веб-браузера

Сучасні браузери використовують цей метод для ізоляції веб-сторінок і запобігання шкідливим скриптам, які можуть скомпрометувати базову операційну систему. Наприклад, якщо ви відвідуєте сайт зі шкідливим програмним забезпеченням, пісочниця вашого браузера гарантує, що воно не зможе отримати доступ до ваших особистих файлів[20].

Пісочниця для розробки програмного забезпечення

Окремі розробники або команди розробників використовують пісочниці для безпечного тестування нового коду за допомогою віртуальних машин (ВМ) або контейнерних середовищ, зберігаючи ізоляцію. Наприклад, банківський додаток може використовувати пісочницю для тестування нової логіки транзакцій[20].

Пісочниця на основі віртуальних машин (ВМ)

Це створює повністю ізольоване середовище операційної системи, що ідеально підходить для тестування сумісності програмного забезпечення. Наприклад, розробник гри може використовувати пісочницю на базі віртуальної машини, щоб перевірити, чи працює його гра безперебійно на різних версіях Windows[20].

Поведінковий аналіз дає змогу виявляти шкідливу активність на основі реального виконання коду в безпечному середовищі. Наступний підрозділ покаже, як сучасні тенденції впливають на розвиток усіх згаданих технологій.

2.5. Сучасні тенденції у виявленні шкідливого ПЗ

Ландшафт аналізу шкідливого програмного забезпечення значно змінився завдяки зростаючій складності кіберзагроз та передовим методам, що розробляються для боротьби з ними. Кількість атак шкідливих програм на американський бізнес цього року зросла на 30% порівняно з минулим роком, причому багато організацій зазнали крадіжки даних внаслідок таких атак. У 3 кварталі 2024 року середня кількість щотижневих кібератак на одну організацію зросла до історичного максимуму - 1 876, що на 75% більше, ніж за аналогічний період 2023 року, і на 15% більше, ніж у попередньому кварталі. У цьому розділі досліджуються ключові тенденції, що формують сферу аналізу шкідливого програмного забезпечення, висвітлюються виклики та інновації для лідерів бізнесу та кібербезпеки[21].

Шкідливе програмне забезпечення зі штучним інтелектом

Однією з найпомітніших тенденцій 2024 року стало зростання кількості шкідливих програм на основі штучного інтелекту. Ці шкідливі програми використовують штучний інтелект для адаптації та обходу традиційних заходів безпеки. Шкідливе програмне забезпечення зі штучним інтелектом може вчитися у своєму оточенні, що ускладнює його виявлення та нейтралізацію. Це створює значні виклики для фахівців з кібербезпеки, які повинні розробляти не менш

досконалі методи протидії цим загрозам. Динамічна природа шкідливих програм зі штучним інтелектом вимагає постійного моніторингу та адаптації протоколів безпеки, щоб випереджати потенційні атаки[21].

Безфайлове шкідливе програмне забезпечення

Безфайлове шкідливе програмне забезпечення є ще однією проблемою, що зростає у сфері кібербезпеки. На відміну від традиційних шкідливих програм, які покладаються на файли, що зберігаються на диску, безфайлові шкідливі програми працюють виключно в пам'яті. Це ускладнює його виявлення звичайними методами, оскільки немає файлів для сканування. Натомість, для виявлення та усунення безфайлового шкідливого програмного забезпечення потрібні розширені дослідження пам'яті та поведінковий аналіз. Цей тип шкідливого програмного забезпечення часто використовує легальні системні процеси, що ще більше ускладнює його виявлення[21].

Квантово-стійке шифрування

З розвитком квантових обчислень зростає потреба у квантово-стійкому шифруванні. Нові штами шкідливих програм починають використовувати квантово-стійке шифрування для захисту своїх каналів зв'язку. Це створює новий виклик для аналітиків шкідливого програмного забезпечення, які повинні розробити методи для розшифрування та аналізу цих повідомлень. Впровадження квантово-стійкого шифрування шкідливими програмами підкреслює важливість випередження технологічного прогресу в галузі кібербезпеки[21].

Шкідливе програмне забезпечення Інтернету речей

Поширення пристроїв Інтернету речей (IoT) створило для кіберзлочинців широке поле для атак. Шкідливе програмне забезпечення IoT націлене на ці пристрої, які часто мають різноманітну архітектуру та обмежені заходи безпеки. Ефективний аналіз шкідливого програмного забезпечення Інтернету речей вимагає спеціалізованих інструментів і методів, адаптованих до унікальних характеристик пристроїв Інтернету речей. Оскільки кількість підключених

пристроїв продовжує зростати, зростає і важливість їх захисту від атак шкідливого програмного забезпечення[21].

Атаки на ланцюги постачання

Атаки на ланцюги постачання стають дедалі поширенішими, використовуючи довірені мережі розповсюдження програмного забезпечення для вбудовування шкідливого програмного забезпечення в легальні програми. Ці атаки можуть мати далекосяжні наслідки, оскільки вони ставлять під загрозу цілісність широко використовуваного програмного забезпечення. Аналіз атак на ланцюжки постачання вимагає нових методів для ретельного вивчення ланцюжків постачання програмного забезпечення та виявлення потенційних вразливостей. Складність цих атак підкреслює необхідність комплексних заходів безпеки протягом усього життєвого циклу розробки програмного забезпечення[21].

Поліморфні та метаморфні шкідливі програми

Поліморфні та метаморфні шкідливі програми розроблені таким чином, щоб постійно змінювати структуру свого коду, щоб уникнути виявлення. Поліморфне шкідливе програмне забезпечення змінює свій зовнішній вигляд при кожному зараженні, тоді як метаморфне шкідливе програмне забезпечення повністю переписує свій код. Ці методи ускладнюють ідентифікацію шкідливого програмного забезпечення традиційними методами виявлення на основі сигнатур. Гібридні методики аналізу, які зосереджуються на інваріантних компонентах шкідливого програмного забезпечення, є важливими для ефективного виявлення та усунення загроз[21].

Крос-платформне шкідливе програмне забезпечення

Крос-платформне шкідливе програмне забезпечення здатне заражати декілька операційних систем, створюючи значну загрозу для різних обчислювальних середовищ. Цей тип шкідливого програмного забезпечення вимагає від аналітиків глибокого розуміння різних платформ і розробки універсальних інструментів аналізу. Здатність крос-платформного шкідливого програмного забезпечення поширюватися на різні системи підкреслює

необхідність комплексних стратегій безпеки, які охоплюють всі потенційні цілі[21].

Отже, тенденції в аналізі шкідливих програм відображають зростаючу складність і витонченість кіберзагроз. Шкідливе програмне забезпечення на основі штучного інтелекту, безфайлове шкідливе програмне забезпечення, квантово-стійке шифрування, шкідливе програмне забезпечення для Інтернету речей, атаки на ланцюги поставок, поліморфне і метаморфне шкідливе програмне забезпечення та крос-платформне шкідливе програмне забезпечення - все це створює унікальні виклики для фахівців з кібербезпеки. Для боротьби з цими загрозами необхідні передові технології та постійна адаптація. На даний момент 7 з 10 керівників компаній розгорнуть інструменти Gen AI для кіберзахисту протягом наступних 12 місяців, щоб компенсувати постійний дефіцит кадрів.

У постійно мінливому ландшафті кіберзагроз розвідка загроз відіграє вирішальну роль у розумінні ширшого контексту атак. Збираючи та аналізуючи дані про нові загрози, фахівці з кібербезпеки можуть розробляти проактивні заходи захисту та розширювати свої можливості аналізу шкідливого програмного забезпечення. Розвідка загроз дозволяє організаціям випереджати потенційні атаки та ефективно реагувати на нові та еволюціонуючі загрози.

Також будо знайдено декілька вражаючих статистичних даних та тенденцій щодо шкідливого програмного забезпечення (2023-2025)

Глобальні тенденції шкідливого програмного забезпечення

За перші три квартали 2023 року у світі було зафіксовано приблизно 5,6 мільярда спроб атак зловмисного програмного забезпечення.

Обсяги шкідливого програмного забезпечення в 3 кварталі 2023 року зросли на 5% порівняно з 2 кварталом того ж року.

40% глобальних кіберінцидентів, на які реагували фірми з безпеки у 2023 році, були пов'язані з тією чи іншою формою шкідливого програмного забезпечення.

Станом на середину 2023 року дослідники безпеки спостерігали в середньому 400 000 нових варіантів шкідливого програмного забезпечення щодня.

До 2025 року кіберзлочинність, включно з атаками, спричиненими шкідливим програмним забезпеченням, може коштувати світовій економіці 10,5 трильйонів доларів щорічно.

Програми-вимагачі залишаються найбільшою загрозою, яка з'являється у 27% великих кіберінцидентів у 2023 році.

Середня вартість злому, спричиненого вірусом-здирником у 2023 році, перевищила $5 млн, порівняно з $4,6 млн наприкінці 2022 року.

У 2023 році кількість шкідливих програм на базі Інтернету речей зросла на 55% у порівнянні з попереднім роком, націлених на "розумні" пристрої та критично важливу інфраструктуру.

Щонайменше 63% атак у 2023 році були здійснені через шкідливі вкладення або посилання в електронних листах.

Поліморфне шкідливе програмне забезпечення (яке мутує свій код) склало 18% нових штамів, виявлених у 2023 році.

Прогнозується, що до кінця 2024 року на безфайлові атаки (що використовують скрипти або корисне навантаження в пам'яті) припадатиме 70% усіх серйозних інцидентів, пов'язаних зі шкідливим програмним забезпеченням.

Середній час життя (час від початкового зараження до виявлення) шкідливого програмного забезпечення у 2023 році склав 16 днів, що менше, ніж у 2022 році, коли він становив 21 день.

Станом на 3 квартал 2023 року 85% компаній зіткнулися принаймні з одним інцидентом безпеки, пов'язаним зі зловмисним програмним забезпеченням, протягом 12 місяців.

83% опитаних фахівців з безпеки називають "швидку еволюцію шкідливого програмного забезпечення" головним викликом на 2024 рік.

У першій половині 2023 року кількість зашифрованих загроз (шкідливих програм, прихованих в SSL/TLS-трафіку) зросла на 45%.

На початку 2023 року кількість нових штамів шкідливих програм, орієнтованих на хмарні сервери, зросла на 28%, а кількість шкідливих програм, орієнтованих на Linux, збільшилася на 28%.

Кількість випадків криптоджекінгу (прихованого видобутку криптовалют) зросла на 200% у першій половині 2023 року, що пов'язано зі зростанням цін на криптовалютному ринку.

Очікується, що у 2024 році пропозиції шкідливого програмного забезпечення як послуги (MaaS) в темному Інтернеті зростуть на 30%, що сприятиме широкій комерціалізації.

У 2023 році до 39% організацій середнього розміру зіткнулися з повторним зараженням шкідливим програмним забезпеченням після неповного усунення наслідків у 2023 році.

Групи вірусів-вимагачів, керовані людьми, відповідальні за 62% цілеспрямованих атак на підприємства у 2023 році.

До 4 кварталу 2024 року, за оцінками, 86% нового шкідливого програмного забезпечення матимуть "навмисне ухилення", щоб обійти традиційні антивірусні програми на основі сигнатур.

Кіберстраховики повідомляють, що 75% їхніх виплат у 2023 році пов'язані з інцидентами, пов'язаними з програмами-вимагачами.

У 2 кварталі 2023 року поширення фішингового шкідливого програмного забезпечення зросло на 32%, що пов'язано з масштабними спам-кампаніями.

Середньомісячна кількість експлойтів "нульового дня", що використовуються в кампаніях зловмисників у 2023 році, становить 5,5, що майже вдвічі більше, ніж 2,8 на початку 2022 року.

За прогнозами експертів, до 2025 року 80% компаній середнього бізнесу впровадять ту чи іншу форму розширеного виявлення та реагування (Extended Detection and Response, XDR) для боротьби з сучасними шкідливими програмами[22].

Статистика шкідливого програмного забезпечення для охорони здоров'я, освіти, фінансів та державного сектору

На початку 2023 року освіта була найбільш часто атакованою вертикаллю - на неї припадало 20% усіх зареєстрованих інцидентів зі зловмисним програмним забезпеченням.

75% опитаних у 2023 році шкіл K-12 зазнали щонайменше одного інциденту зі зловмисним програмним забезпеченням, який перервав навчальний процес.

У вищих навчальних закладах у першому кварталі 2023 року на програми-вимагачі припадало 33% усіх виявлених заражень шкідливим програмним забезпеченням.

Організації охорони здоров'я повідомили про 12% зростання загальної кількості атак шкідливих програм у 2 кварталі 2023 року порівняно з 1 кварталом.

89% IT-директорів у сфері охорони здоров'я вважають програми-вимагачі головною загрозою у 2024 році.

У першій половині 2023 року в секторі фінансів та страхування спостерігався 66%-вий сплеск порушень, спричинених шкідливим програмним забезпеченням.

Банківські трояни атакували кожну третю фінансову установу в другому кварталі 2023 року, зосередившись на крадіжці облікових даних.

З січня по червень 2023 року уряд/державний сектор пережив 16%-вий сплеск інцидентів, спричинених шкідливим програмним забезпеченням.

70% респондентів з державних/місцевих органів влади в опитуванні 2023 року стикалися з програмами-вимагачами принаймні один раз у цьому році.

Станом на середину 2023 року 62% фірм-виробників повідомили про щонайменше один збій в роботі через шкідливе програмне забезпечення.

У першій половині 2023 року кількість шкідливих програм, націлених на ICS/SCADA, зросла на 48% у критичній інфраструктурі.

У 2023 році кількість атак шкідливого програмного забезпечення на комунальні послуги (водопостачання, електропостачання тощо) зросла на 31% у порівнянні з попереднім роком.

Роздрібна торгівля постраждала від більшої кількості атак вірусів-вимагачів у вихідні та святкові дні, причому 22% з них припали на великі шопінг-дати.

54% рітейлерів, опитаних в середині 2023 року, мали інциденти зі зловмисним програмним забезпеченням на торгових точках за останні 12 місяців.

На малий бізнес (<250 співробітників) припадає 45% зареєстрованих інцидентів зі зловмисним програмним забезпеченням у 2 кварталі 2023 року.

37% малих та середніх підприємств, які зазнали атаки шкідливого програмного забезпечення у 2023 році, знадобилося більше тижня для повного відновлення роботи.

У технологічному секторі на 13% зросла кількість цілеспрямованих атак зловмисного програмного забезпечення з метою крадіжки інтелектуальної власності у порівнянні з попереднім роком.

61% юридичних фірм зіткнулися принаймні з одним порушенням, пов'язаним зі зловмисним програмним забезпеченням у 2023 році, переважно з вимогами викупу.

Некомерційні та неурядові організації повідомили про 19% зростання кількості кампаній зі зловмисним програмним забезпеченням у 2 кварталі 2023 року, які часто включають фішингові приманки.

62% навчальних закладів не мають повністю укомплектованої команди з кібербезпеки, що посилює ризики зловмисного програмного забезпечення.

5 з 10 фінансових установ планують збільшити бюджети на виявлення кінцевих точок до 2024 року, щоб протистояти новим загрозам шкідливого програмного забезпечення.

85% постачальників медичних послуг мають намір впровадити рішення з нульовою довірою до 2025 року, щоб зменшити кількість інцидентів, пов'язаних зі шкідливим програмним забезпеченням.

У державному секторі 45% заражень шкідливим програмним забезпеченням у 2023 році були спричинені застарілими системами, на яких не були встановлені важливі виправлення.

11% виробничих організацій в опитуванні, проведеному в третьому кварталі 2023 року, заплатили викуп у розмірі понад 1 мільйон доларів для відновлення роботи ІКС.

23% атак на об'єкти критичної інфраструктури у 2023 році були спричинені шкідливим програмним забезпеченням, спеціально розробленим для порушення фізичних процесів[22].

Тенденції мобільного шкідливого програмного забезпечення

У першому півріччі 2023 року на мобільне шкідливе програмне забезпечення припадало 21% від загальної кількості виявлених загроз.

Середньостатистичне підприємство блокує понад 2 500 мобільних загроз на місяць, що на 15% більше, ніж наприкінці 2022 року.

Пристрої Android залишаються головною мішенню, на яку припадає 92% усіх мобільних шкідливих програм у 2023 році.

Експлойти для iOS (наприклад, шпигунське ПЗ типу Pegasus) були причетні до 3% мобільних інфекцій, досліджених у 2 кварталі 2023 року.

Мобільний фішинг (смішинг) зріс на 36% у першій половині 2023 року.

6% глобальних пристроїв Android зіткнулися з принаймні однією спробою зараження шкідливим програмним забезпеченням у 2 кварталі 2023 року.

Серед найпопулярніших сімейств мобільних шкідливих програм у 2023 році - SpyNote, XLoader та FluBot.

Мобільні програми-вимагачі залишаються нішевими, але їхня кількість зросла на 24% у першому кварталі 2023 року, в першу чергу вражаючи користувачів Android.

Банківські трояни, такі як Anubis і Cerberus, у 2023 році атакували понад 380 фінансових додатків у Google Play.

Виявлення мобільного криптоджекінгу підскочило на 58% з 4-го кварталу 2022 року до 1-го кварталу 2023 року.

35% великих підприємств зазнали щонайменше одного витоку даних через скомпрометований мобільний пристрій у 2023 році.

Кожна п'ята організація з політикою BYOD не має рішення для виявлення мобільних загроз.

82% співробітників визнають, що використовують робочі додатки на персональних пристроях, які не мають керованої корпоративної безпеки.

У 2023 році на шкідливу рекламу припадає 12% точок проникнення мобільного шкідливого програмного забезпечення, часто через рекламу в додатках.

Фішинг у соціальних мережах на мобільних пристроях подвоївся на початку 2023 року, заробляючи на викрадених сесіях.

Шкідливе програмне забезпечення для шахрайства з мобільною рекламою коштувало рекламодавцям приблизно 1,6 мільярда доларів у всьому світі в 2023 році.

Кількість шахрайських мобільних профілів (профілів конфігурації, що встановлюють шкідливі кореневі сертифікати) зросла на 70% у 2023 році.

Кількість шахрайств зі зміною SIM-карт зросла на 44% в середині 2023 року, що дало зловмисникам доступ до облікових записів, захищених 2FA.

У секторі освіти з січня по травень 2023 року кількість мобільних шкідливих програм зросла на 130%, здебільшого через шкідливі програми для електронного навчання.

До 2025 року мобільні загрози можуть становити 30% від загального обсягу шкідливого програмного забезпечення, чому сприятиме повсюдне поширення смартфонів[22].

Нові загрози та перспективи на майбутнє

Прогнозується, що до кінця 2024 року кількість безфайлових шкідливих програм зросте на 65%, випередивши багато файлових методів.

Двійкові файли, що живуть поза землею, використовуються в 79% цільових атак у 2023 році, що зменшує потребу в типових файлах шкідливого програмного забезпечення.

Кількість шкідливих програм Infostealer у 2023 році зросла на 220%, що зумовлено попитом на викрадені облікові дані на темних інтернет-ринках.

Атаки на основі облікових даних стали основним вектором доступу в 2023 році, випередивши фішинг на 6%.

На програми-вимагачі з подвійним вимаганням (крадіжка даних + шифрування) припадає 81% інцидентів у 2023 році.

Потрійне вимагання (з додаванням DDoS або прямого контакту з жертвою) підскочило до 14% випадків у першому півріччі 2023 року.

Вимагання лише даних (без шифрування) зросло на 37% у 2023 році, тиснучи на жертв витоками публічних даних.

Кількість шахрайств з використанням глибоких підробок зросла на 2 500% у 2023 році завдяки вдосконаленню генеративного ШІ.

Очікується, що до 2025 року шкідливе програмне забезпечення зі штучним інтелектом становитиме 20% нових штамів.

У другому кварталі 2023 року на форумах у темному інтернеті почали з'являтися інструменти для генерації шкідливих програм, що використовують великі мовні моделі.

Національні державні суб'єкти пов'язані з 8% кампаній зі створення шкідливого програмного забезпечення, виявлених у 2023 році, переважно з метою шпигунства.

74% керівників державних IT-відомств стурбовані тим, що у 2024-2025 роках шкідливе програмне забезпечення-"стирач" може стати геополітичною зброєю.

У першій половині 2023 року кількість атак на ланцюжки поставок зросла на 38%, при цьому часто використовуються бекдори у довірених оновленнях програмного забезпечення.

Експлуатація вразливості MOVEit в середині 2013 року вплинула на понад 2 000 організацій, що призвело до витоку десятків мільйонів записів.

Кількість експлойтів "нульового дня", які використовувалися для створення сучасного шкідливого програмного забезпечення, у 2023 році подвоїлася порівняно з початком 2022 року.

Прогнозується, що квантово-стійке шифрування дещо зменшить майбутній успіх шкідливого програмного забезпечення, але до 2025 року його впровадження залишиться на рівні <10%.

69% організацій планують інтегрувати виявлення аномалій на основі ШІ до кінця 2024 року.

39% команд безпеки наразі використовують передові технології EDR/XDR з моделями машинного навчання для виявлення невідомого шкідливого програмного забезпечення.

54% компаній відчувають труднощі з виявленням безфайлових атак, які використовують вбудовані інструменти ОС.

У 2023 році кількість шкідливих програм, націлених на хмарні технології, зросла на 61%, особливо серед SaaS-провайдерів, які обробляють конфіденційні дані.

Боти для підбору облікових даних, які підтримуються новими скриптами зі штучним інтелектом, у 2023 році здійснили на 36% більше успішних вторгнень.

Кількість віртуальних приватних серверів, що використовуються як C2 (командно-контрольні) хаби для шкідливого програмного забезпечення, зросла на 42% в середині 2023 року.

Темні інтернет-ринки викрадених RDP/VPN облікових даних зросли на 28% з 4-го кварталу 2022 року до 2-го кварталу 2023 року.

Подвійне шифрування (шифрування одних і тих самих даних за допомогою двох різних програм-вимагачів) було зафіксовано у 9% випадків у 2023 році.

Кількість інцидентів, пов'язаних з інсайдерською допомогою (коли внутрішній користувач допомагає встановити шкідливий код), зросла на 11% у 2023 році.

У 2023 році шкідливе програмне забезпечення, пов'язане з міждержавними конфліктами (наприклад, у Східній Європі), опосередковано вплинуло на 5% світових компаній.

До 2025 року, за оцінками, 75% світових організацій перейдуть на архітектуру нульової довіри для боротьби з сучасним шкідливим програмним забезпеченням.

У 2023 році кількість партнерських програм-здирників (RaaS) зросла на 40%, що дозволило приєднатися до них зловмисникам з низькою кваліфікацією.

Очікується, що до кінця 2024 року шкідливе програмне забезпечення для обходу біометричних даних, яке підробляє розпізнавання відбитків пальців/обличчя, вийде на широкий загал.

У третьому кварталі 2023 року організації стикалися в середньому з 1920 кібератаками на тиждень, що на 72% більше, ніж у третьому кварталі 2022 року - у більшості з них було задіяно шкідливе програмне забезпечення.

Актуальність тенденцій демонструють зростання ролі автоматизації, поведінкового аналізу та штучного інтелекту у боротьбі з кіберзагрозами. Це свідчить про необхідність подальшого розвитку адаптивних систем захисту на основі комплексного підходу[22].

Сучасні підходи до виявлення шкідливого програмного забезпечення – такі як розширений поведінковий аналіз і алгоритми машинного навчання – дозволяють виявляти загрози в режимі реального часу. Відомо, що багаторівневий захист використовує поєднання поведінкового аналізу, алгоритмів ШІ і даних кіберрозвідки для своєчасного виявлення та нейтралізації атак. Платформи автоматизації та оркестрації безпеки (SOAR) консолідують дані з різних джерел і застосовують штучний інтелект і автоматичні реакції для швидкого реагування на інциденти. Враховуючи наведені тенденції та складність сучасних загроз, у наступному розділі будуть запропоновані практичні рекомендації, засновані на багаторівневій стратегії захисту інформаційних систем (зокрема впровадження EDR/XDR-систем, SOAR-платформ, моделей Zero Trust та чіткої мережевої сегментації).

Висновки до розділу 2

Сигнатурні методи ефективні проти відомих загроз, але безсилі перед «новими» нульовими днями. Як показано в аналізі обмежень засобів виявлення, сигнатурний аналіз виявляє лише відоме ПЗ і неефективний щодо невідомих варіантів «вимогальників», руткітів тощо. Тому сучасні системи доповнюються евристичним (поведінковим) аналізом і машинним навчанням для виявлення невідомих та аномальних проявів шкідливої активності.

Динамічний аналіз (пісочниці) із застосуванням ML значно підвищує якість виявлення складних загроз. Запуск підозрілих зразків у контрольованому середовищі (sandbox) з наступною перевіркою їхньої поведінки за допомогою машинного навчання дозволяє виявити навіть складні програми-вимагачі та нові види атак незалежно від вектора розповсюдження. Такий підхід демонструє високу ефективність у блокуванні передових загроз.

Розділ 3 Розробка рекомендацій для підвищення рівня захисту інформаційних систем від шкідливого програмного забезпечення

3.1 Вирішення проблем і недоліків AV у сучасному ландшафті загроз.

Традиційне антивірусне програмне забезпечення історично було основним засобом захисту кінцевих пристроїв. Антивіруси працюють переважно на основі сигнатур, тобто виявляють відомі зразки шкідливого коду шляхом порівняння з базою даних сигнатур. Хоча такий підхід ефективний проти значної частини відомого шкідливого програмного забезпечення, він має суттєві обмеження. По-перше, сигнатурні методи не здатні виявляти нові, раніше невідомі загрози (атаки нульового дня) – доки вірус не буде досліджено й додано до бази, типовий антивірус його не розпізнає. По-друге, традиційний антивірус неефективний проти сучасних технік атак, як-от безфайлове (fileless) шкідливе ПЗ чи атаки з використанням легітимних утиліт системи (Living-off-the-Land), які обходять сигнатурне виявлення. За оцінками фахівців, класичний антивірус здатен виявити понад 90% відомих загроз, але лише близько 20% атак нульового дня, 10% безфайлових атак і близько 30% цілеспрямованих APT-атак. Таким чином, значна частина сучасного шкідливого ПЗ може залишитися непоміченою при використанні лише антивірусу[23].

Крім низької ефективності проти новітніх загроз, антивіруси за своєю природою здебільшого реагують постфактум. Виявлення загрози часто відбувається вже після компрометації системи, що призводить до необхідності cleanup– усунення наслідків зараження, простою систем та втрати даних. Сучасні нападники активно перевіряють свої віруси на здатність обійти популярні антивіруси, тому покладатися тільки на сигнатурний захист небезпечно. Показово, що навіть великі розробники засобів безпеки визнають зміну парадигми: ще у 2014 році в галузі пролунала теза «антивірус мертвий», підкреслюючи, що класичні підходи більше не гарантують належного рівня захисту. Свіжі дослідження підтверджують цю думку. Зокрема, у звіті IBM за

2023 рік відзначено, що так звані fileless-атаки мають у десять разів більші шанси успішно уразити систему, ніж звичайне вірусне ПЗ, оскільки вони експлуатують легітимні процеси ОС[23].

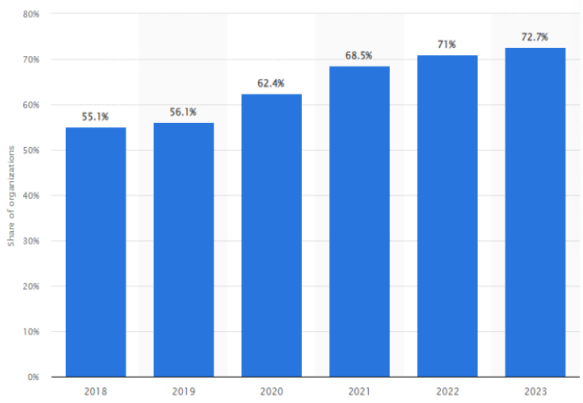

Рис. 3.1 Річна частка організацій, постраждалих від атак програм-вимагачів у всьому світі впродовж 2018–2023 рр.

Хоча антивірусне програмне забезпечення все ще може бути корисним, особливо для менш досвідчених користувачів, часто рекомендується багаторівневий підхід до безпеки, який включає безпечні практики та оновлення системи.

Є кілька причин, чому деякі люди не рекомендують використовувати традиційне антивірусне програмне забезпечення:

Хибне відчуття безпеки: Деякі користувачі можуть вважати, що наявність антивірусного програмного забезпечення означає, що вони в цілковитій безпеці, що призводить до ризикованої поведінки в Інтернеті[24].

Проблеми з продуктивністю: Антивірусні програми можуть споживати значні системні ресурси, що призводить до зниження продуктивності пристроїв, особливо старих[24].

Еволюція загроз: Кіберзагрози еволюціонують, і багато сучасних атак (наприклад, фішинг, програми-вимагачі та експлойти нульового дня) не можуть бути ефективно нейтралізовані традиційними антивірусними рішеннями[24].

Вбудовані засоби захисту: Багато операційних систем зараз постачаються з вбудованими функціями безпеки (наприклад, Windows Defender в Windows 10 і 11), які можуть забезпечити належний захист без необхідності використання стороннього антивірусного програмного забезпечення[24].

Зосередьтеся на поведінці користувачів: Деякі експерти стверджують, що навчання користувачів безпечним методам перегляду веб-сторінок, розпізнавання фішингових атак та підтримка оновлень програмного забезпечення може бути ефективнішим, ніж покладання лише на антивірусні програми[24].

Занепокоєння щодо конфіденційності: Деякі антивірусні програми можуть збирати дані про поведінку користувачів і використання системи, що викликає занепокоєння щодо конфіденційності[24].

Витрати проти переваг: Для деяких користувачів, особливо технічно підкованих, вартість антивірусного програмного забезпечення може не виправдати переваг, особливо якщо вони вже вживають інших заходів безпеки[24].

Отже, організація, що спирається лише на традиційний антивірус, залишається вразливою перед сучасними загрозами. Ці недоліки диктують потребу в більш просунутих рішеннях захисту, здатних проактивно виявляти і зупиняти складні атаки.

3.2 Шляхи підвищення рівня захисту від ШПЗ

Для протидії вищезгаданим проблемам використовують комплексний підхід, що поєднує сучасні інструменти кіберзахисту. Серед ключових рішень – системи виявлення і реагування, які доповнюють можливості антивірусу; інструменти автоматизації реагування; принципи Zero Trust із сегментацією мережі; надійне резервне копіювання; програми навчання персоналу; та постійний аналіз розвідувальних даних про загрози. Кожен з цих елементів відіграє окрему роль у захисній стратегії, однак разом вони формують

багаторівневий механізм «активного» захисту. Нижче наведено характеристику кожного компонента та його роль у цій системі

Рекомендація щодо впровадження EDR/XDR

З огляду на обмеженість антивірусів, провідні компанії впроваджують системи виявлення та реагування на кінцевих точках EDR як сучасну альтернативу. EDR (Endpoint Detection and Response) – це технологія моніторингу та захисту кінцевих пристроїв, що поєднує постійний нагляд за активністю системи з інтелектуальним аналізом поведінки. На відміну від антивірусу, який шукає відомі шкідливі сигнатури, EDR відстежує підозрілу поведінку процесів на пристрої та може виявити атаки, навіть якщо шкідливий код раніше не зустрічався[23]. Наприклад, раптове шифрування великої кількості файлів законним процесом (типова ознака рансомвера) або спроби нестандартного підвищення привілеїв можуть бути негайно розпізнані як аномалія. EDR-система не тільки сигналізує про виявлену загрозу, але й здатна миттєво реагувати: ізолювати заражений хост від мережі, завершити шкідливі процеси, зібрати дані для форензики. Така поведінкова (проактивна) модель захисту дозволяє зупиняти атаки до того, як вони завдадуть шкоди, на відміну від реактивного «прибирання» після інциденту. Завдяки цьому EDR сьогодні розглядається як необхідний елемент захисту підприємств, що стикаються зі складними та цілеспрямованими атаками. Як зазначають дослідники, шляхом безперервного аналізу поведінки кінцевих точок EDR здатен виявляти й зупиняти розвинуті загрози, які традиційний антивірус пропустить, що робить його ключовим інструментом кібербезпеки для сучасних організацій[23].

Подальшим розвитком концепції EDR є технологія XDR (Extended Detection and Response) – розширене виявлення та реагування. Якщо EDR зосереджений переважно на кінцевих точках (персональні комп’ютери, ноутбуки, сервери та інші хости), то XDR інтегрує інформацію з різних компонентів інфраструктури: мережевого трафіку, хмарних сервісів, серверів, засобів автентифікації, застосунків тощо. По суті, XDR є розширеною версією EDR, що надає ширший огляд ситуації в масштабах всієї IT-екосистеми

підприємства. Це означає, що XDR-платформа може корелювати події з різних джерел (endpoint-агентів, мережевих сенсорів, журналів безпеки) для виявлення комплексних багатовекторних атак, які окремими засобами могли б лишитися непоміченими. Наприклад, XDR здатна співставити підозрілу активність на робочій станції з одночасними аномаліями в мережевому трафіку та спробою доступу до хмарних ресурсів – така кореляція дає змогу виявити складну атаку, що складається з кількох стадій. Результатом впровадження XDR є єдина консолідована картина кібербезпеки: аналітики отримують централізовані сповіщення про інциденти зі всіх середовищ, що спрощує розслідування та прискорює реагування. Таким чином, рекомендується поступово переходити від ізольованих антивірусів до комплексних EDR-рішень, а за можливості – до інтегрованих XDR-платформ, особливо для середніх та великих організацій. Це забезпечить вищий рівень виявлення сучасних загроз і координацію захисту на різних рівнях системи[25].

Інтеграція SOAR для автоматизованого реагування

Навіть маючи потужні засоби виявлення (як-от EDR/XDR), організаціям потрібно оперативно реагувати на інциденти, щоб мінімізувати їхній вплив. У великих мережах щоденно генеруються сотні й тисячі сповіщень систем безпеки (журнали брандмауерів, сигнали EDR, попередження SIEM тощо). Обробити та належно відреагувати на такий потік вручну надзвичайно складно – людський ресурс обмежений, і затримки в реагуванні можуть дати змогу атаці розвинутися. Тому в сучасних стратегіях кібербезпеки критичною є інтеграція рішень класу SOAR (Security Orchestration, Automation and Response) – оркестрації, автоматизації та реагування на інциденти безпеки[26].

SOAR - це набір інструментів і технологій, які допомагають організаціям керувати інцидентами безпеки та реагувати на них з більшою ефективністю та результативністю. Це досягається завдяки поєднанню трьох ключових функцій:

Оркестрування безпеки: Інтеграція різних інструментів і систем безпеки для безперебійної спільної роботи. Оркестрування уможливлює централізоване

управління операціями з безпеки, дозволяючи різним інструментам обмінюватися інформацією та координувати дії.

Автоматизація безпеки: Використання програмного забезпечення для автоматизації рутинних завдань безпеки, що дозволяє командам безпеки зосередитися на стратегічних заходах. Автоматизація зменшує робоче навантаження, а також допомагає забезпечити послідовність і точність обробки інцидентів.

Реагування на інциденти безпеки: Процес структурованого та своєчасного реагування на інциденти безпеки. Сюди входять кроки, спрямовані на виявлення, локалізацію, усунення та відновлення після загроз безпеці.

Роль SOAR у сучасній системі захисту полягає в різкому скороченні часу від виявлення загрози до протидії їй. Наприклад, у разі спрацювання EDR (виявлено підозрілий процес) SOAR-платформа може автоматично виконати серію дій: ізолювати хост у мережі, створити тикет для команди безпеки, зібрати додаткову інформацію (зробити знімок пам’яті, витягти хеш файлу) та навіть заблокувати відповідні IoC на мережевому рівні (наприклад, заборонити трафік на Command&Control сервер). Усе це відбувається за лічені секунди, тоді як ручний процес зайняв би від кількох хвилин до годин. Автоматизація також дозволяє уникнути людського фактору при виконанні рутинних дій реагування – сценарій спрацьовує щоразу однаково правильно, виключаючи можливість помилки чи зволікання. Оркестрація в рамках SOAR забезпечує узгоджену роботу різних систем: інструменти обміну інформацією та API-інтеграції дозволяють, щоб EDR, SIEM, мережеві екрани, системи управління квитками та інші компоненти діяли як єдиний механізм. Завдяки цьому досягається єдиний цикл реагування: від реєстрації інциденту, його пріоритизації, збагачення контекстом (наприклад, додавання даних розвідки загроз) – до безпосереднього усунення загрози[26].

Таким чином, впровадження SOAR-рішень є рекомендованим кроком для організацій, що вже мають базові засоби моніторингу. SOAR значно підвищує масштабованість операцій безпеки – навіть мала команда аналітиків, озброєна

автоматизацією, здатна ефективно обробляти великий обсяг інцидентів. Це особливо актуально з огляду на дефіцит кадрів у кібербезпеці: автоматизація дозволяє оптимально використовувати наявні ресурси, спрямовуючи зусилля експертів на аналіз та розслідування складних випадків, в той час як рутинні заходи виконує машина. Загальний рівень захисту від шкідливого ПЗ при цьому зростає, адже навіть масовані або швидкоплинні атаки (наприклад, хробак, що поширюється мережею) будуть негайно локалізовані автоматизованими засобами реагування[26].

Впровадження Zero Trust і сегментації мережі

Окрім засобів виявлення та реагування, надзвичайно важливою є правильна побудова архітектури захисту мережі, яка мінімізує потенційні наслідки проникнення шкідливого програмного забезпечення. Традиційно корпоративні мережі будувалися за принципом периметрової безпеки: вважалося, що всередині внутрішньої мережі користувачам і пристроям можна більшою мірою довіряти, а основні захисні бар'єри зосереджувалися на межі (периметрі) між внутрішньою і зовнішньою мережею. Однак за останні роки ефективність такого підходу значно впала[27]. Поширення хмарних сервісів, віддаленої роботи та політики Bring Your Own Device призвело до того, що межі корпоративної мережі розмиті. Зловмисники також навчилися обходити периметровий захист, проникаючи у внутрішню мережу (наприклад, через скомпрометовані облікові дані або фішингові атаки на співробітників) і залишаючись непоміченими. В результаті традиційні методи виявилися вразливими перед сучасними атаками, коли нападник після проникнення у внутрішню мережу може практично безперешкодно переміщуватися нею та здобувати доступ до критичних ресурсів. У таких умовах постала нова парадигма захисту – концепція Zero Trust («нульова довіра»), яка пропонує кардинально інший принцип: не довіряти нікому та нічому за замовчуванням, незалежно від розташування в мережі чи попередніх перевірок автентичності. Відповідно до моделі Zero Trust, кожен доступ до ресурсу мусить бути явно авторизований і перевірений. Користувачі та пристрої повинні постійно підтверджувати свою

автентичність, а їхні права доступу мають бути обмежені мінімально необхідними привілеями[27].

Впровадження принципів Zero Trust у корпоративному середовищі передбачає кілька практичних кроків. По-перше, ретельна автентифікація і авторизація при кожній взаємодії з ресурсами: це означає обов'язкове використання багатофакторної автентифікації, управління доступом на основі ролей та контексту, постійний моніторинг аномалій у поведінці користувачів. По-друге, мережева сегментація – поділ мережі на ізольовані зони – виступає ключовим механізмом мінімізації шкідливих наслідків уразлення однієї ділянки. Сегментація зводить до мінімуму можливість латерального пересування зловмисника в разі компрометації якоїсь підмережі. Наприклад, мережева інфраструктура може бути логічно розділена на сегменти за функціональною ознакою (сегмент для фінансової системи, сегмент для виробничих АСУТП, сегмент для офісних Workstations тощо). Кожен сегмент ізольований фаєрволом або іншими засобами контролю таким чином, що компрометація одного сегмента не дає нападнику прямого доступу до інших. Мікросегментація – ще більш детальний підхід, за якого навіть всередині одного сегмента застосовуються обмеження (наприклад, між окремими серверами або сервісами) – додатково ускладнює поширення шкідливого ПЗ. Zero Trust і сегментація тісно взаємопов'язані: модель нульової довіри вимагає, щоб кожна ланка мережі була потенційно ізольованою і захищеною. Якщо зловмисник все ж отримає доступ до внутрішньої системи, ізольовані сегменти й відсутність «прописаної довіри» не дозволять йому розширити свою присутність далі. Саме тому впровадження Zero Trust архітектури та мережевої сегментації є ефективною рекомендацією для підвищення стійкості до атак: навіть якщо шкідливе ПЗ проникне всередину, шкода буде локалізована в обмеженому сегменті, і атака не переросте в повномасштабний інцидент[28].

Окрім безпосереднього стримування поширення шкідливого коду, Zero Trust підхід покращує загальну керованість безпеки. Чітко сегментована мережа з жорсткими політиками доступу легше контролюється та моніториться – будь-

яка нетипова взаємодія між сегментами або спроба отримати вищі привілеї відразу привертає увагу систем моніторингу. У сукупності Zero Trust і сегментація мережі формують принцип «розділяй і захищай»: кожна частина інфраструктури ізольована настільки, наскільки це можливо, і жодному елементу не надається довіри більше, ніж потрібно. В сучасних умовах, коли атаки стають все більш витонченими, такий архітектурний підхід є необхідним доповненням до засобів активного захисту, розглянутих у попередніх підрозділах[28].

Навчання персоналу як захист від людського фактору

Технічні засоби кіберзахисту будуть неповними без урахування людського фактору. Значну частку інцидентів інформаційної безпеки спричиняють саме помилки або необережність користувачів та співробітників. Згідно з дослідженнями, до 95% успішних кібератак стаються за участі людського фактору – через помилки, нехтування правилами або цілеспрямоване використання психологічних прийомів соціальної інженерії[29]. Нападники часто обирають найлегший шлях проникнення: замість лому складних технічних бар'єрів, вони схиляють людину ненавмисно відкрити їм двері – клікнути на шкідливе посилання, відкрити заражений файл, ввести пароль на фішинговому сайті чи підключити невідомий носій. Тому навчання персоналу в питаннях кібербезпеки є одним з найважливіших напрямів підвищення захищеності системи. Метою програм навчання є перетворення кожного співробітника з потенційної «вразливості» на активний елемент захисту – так званий «людський брандмауер»[29].

Ефективне навчання з кібербезпеки має бути безперервним процесом, що включає як ознайомлення з базовими принципами, так і регулярні оновлення знань у зв'язку з появою нових загроз. Співробітників слід навчати розпізнавати типові ознаки фішингових листів (неправильні адреси відправників, підозрілі вкладення, провокаційні запити тощо), правильно реагувати на підозрілі ситуації (незвичний запит на доступ, раптова поява вимог ввести пароль тощо), дотримуватися правил кібергігієни (використання складних унікальних паролів,

безпечна робота в інтернеті, обережність з зовнішніми носіями). Методи підвищення обізнаності можуть включати періодичні тренінги, онлайн-курси, внутрішні розсилки з порадами безпеки, а також імітаційні атаки (наприклад, контрольований фішинговий тест) для перевірки навичок на практиці. Важливо, щоб керівництво підтримувало культуру безпеки: працівники повинні розуміти, що кібербезпека – це спільна відповідальність, і не боятися повідомляти про свої помилки чи підозрілі інциденти. Регулярне навчання приносить відчутні результати: компанії, що інвестують у програми Security Awareness, фіксують значне зниження кількості інцидентів, пов'язаних із людським фактором (перш за все успішних фішингових атак). До того ж навчений персонал краще взаємодіє з іншими елементами системи захисту: наприклад, швидше реагує на оповіщення від EDR/SIEM, чітко діє за інструкціями при карантині зараженого пристрою або евакуації даних.

Отже, людський фактор з пасиву можна перетворити на актив – шляхом побудови сильної культури кібербезпеки та постійного розвитку знань і навичок співробітників. Навчання персоналу є відносно малозатратним, але надзвичайно ефективним інструментом: воно закриває ті «лазівки» для шкідливого програмного забезпечення, які неможливо повністю перекрити технічними методами. У поєднанні з технологічними засобами захисту, обговореними в інших підрозділах, компетентний і пильний персонал значно підвищує загальну стійкість інформаційної системи до кібератак[29].

Використання Threat Intelligence для проактивного захисту

На завершення, ще одним важливим компонентом сучасної стратегії кібербезпеки є перехід від суто реактивних дій до проактивного захисту на основі розвідки про загрози (Threat Intelligence). Threat Intelligence у сфері кібербезпеки – це систематичний процес збору, аналізу та використання даних про актуальні та потенційні кіберзагрози. Такими даними можуть бути показники компрометації (IoC) – наприклад, відомі зловмисні IP-адреси, домени, хеші файлів, сигнатури шкідливих програм; відомості про тактики, техніки та процедури (TTPs) груп зловмисників; інформація про нові вразливості

програмного забезпечення, які експлуатуються в атаках тощо. Перетворюючи необроблені розрізнені відомості на структуровані знання, система Threat Intelligence забезпечує аналітичний базис для прийняття рішень з безпеки. Головна цінність таких розвідданих – можливість на випередження протидіяти загрозам, що тільки зароджуються або знаходяться поза межами організації, але можуть її зачепити[30].

Роль Threat Intelligence у сучасному захисті інформаційних систем проявляється у кількох аспектах. По-перше, розвідка загроз дає покращене ситуаційне розуміння: команди безпеки бачать ширшу картину того, які атаки відбуваються у світі, які методи актуальні у кіберзлочинців, проти яких секторів спрямовані кампанії атак тощо. Це дозволяє визначити найбільш релевантні для даної організації загрози і відповідно пріоритизувати свої захисні заходи. По-друге, Threat Intelligence забезпечує проактивну модернізацію захисту: замість чекати, поки атака станеться, організація завчасно оновлює свої засоби безпеки на основі отриманих розвідданих. Наприклад, дізнавшись від спецслужб чи галузевих CERT-організацій про нову хвилю атак зі використанням певної вразливості, адміністратори можуть негайно застосувати патчі до своїх систем, не чекаючи, поки цю вразливість експлуатуватимуть проти них. Або отримавши фід з зовнішніми IoC (шкідливими адресами, файлами), можна оперативно завантажити їх у власні брандмауери, проксі, EDR та інші контролі, блокуючи відомі шкідливі об’єкти на підльоті. По-третє, розвідка загроз сприяє цілеспрямованому виявленню та розслідуванню: на основі відомостей про техніки атаки фахівці можуть проводити thread hunting – проактивне «полювання» в своїй мережі, перевіряючи, чи не лишилося непомічених ознак активності, пов’язаних з відомими кампаніями. Threat Intelligence надає гіпотези та напрямки для таких пошуків (наприклад, «перевірити чи не запускалися у мережі такий-то скрипт, відомий як характерна ознака групи X»). Нарешті, по-четверте, розвіддані підвищують швидкість і якість реагування на інциденти, що все ж сталися: маючи інформацію про супротивника, його мотивацію та інструменти, команда реагування може точніше визначити пріоритети (які

системи в першу чергу захищати, чи є ризик double-extortion при рансомвер-атаці тощо) і більш впевнено нейтралізувати загрозу[30].

Використання Threat Intelligence реалізується через спеціалізовані платформи (TIP – Threat Intelligence Platform) чи сервіси, які агрегують дані з численних джерел – відкритих баз даних, приватних аналітичних фірм, спільнот обміну інформацією про загрози (ISAC), державних структур кіберзахисту. Важливо налагодити інтеграцію цих платформ з внутрішніми засобами безпеки (SIEM, SOAR, EDR та ін.), аби розвіддані автоматично збагачували внутрішні сповіщення та використовувалися в правилах кореляції. Таким чином, організація переходить на новий рівень зрілості кібербезпеки – проактивний захист, коли заходи вживаються на основі передбачення атак, а не лише реагування на них. Як зазначає CrowdStrike, ефективне застосування Threat Intelligence дозволяє зрушити позицію оборони з реактивної на проактивну, тобто передбачати і попереджувати атаки до того, як вони досягли цілі. Це дає конкурентну перевагу у кіберпросторі: замість того щоб постійно наздоганяти зловмисників, компанія завжди «на крок попереду». Впровадження розвідки загроз особливо актуальне для великих організацій та критичної інфраструктури, але й середній бізнес може отримати значну вигоду, використовуючи навіть базові відкриті джерела Threat Intelligence для підвищення обізнаності про небезпеки. Загалом, інтеграція цього елементу доповнює решту складових системи захисту, створюючи замкнутий цикл: розвідка – превентивні дії – виявлення – реагування – навчання, що безперервно підвищує кіберстійкість організації[30].

Висновки до розділу 3

Комплексний багаторівневий захист забезпечують рішення EDR/XDR з аналітикою на основі ML та SIEM. Системи EDR/XDR збирають детальні телеметричні дані з кінцевих точок і застосовують автоматичне реагування, що дозволяє оперативно виявляти та локалізувати складні атаки. Рекомендовано

інтегрувати ці платформи з аналітикою штучного інтелекту (AI/ML) та системами кореляції подій (SIEM) для підвищення точності й швидкості реагування.

Архітектура Zero Trust суттєво підвищує безпеку, відмовляючись від «довіри за замовчуванням». Підхід Zero Trust вимагає перевіряти кожен запит на доступ незалежно від місцеположення користувача чи пристрою, що суттєво ускладнює для зловмисників рух по мережі та розгортання шкідливого ПЗ. Впровадження Zero Trust є перспективним напрямом розвитку інформаційної безпеки, особливо для складних гібридних мереж.

ВИСНОВКИ

У кваліфікаційній роботі здійснено комплексне дослідження проблематики виявлення та блокування шкідливого програмного забезпечення, що дало змогу глибоко проаналізувати джерела загроз інформаційній безпеці, визначити сучасні методи їх виявлення та запропонувати практичні рішення щодо підвищення стійкості інформаційних систем.

Систематизовано основні типи шкідливого програмного забезпечення, такі як віруси, трояни, хробаки, руткіти, кейлогери, програми-вимагачі, а також проаналізовано їхні характеристики, принципи дії та вектори поширення. Встановлено, що велике різноманіття форм і механізмів деструктивного впливу потребує комплексного підходу до їх класифікації та вивчення.

Розглянуто ключові методи виявлення шкідливих програм, зокрема сигнатурні та евристичні алгоритми, поведінковий аналіз, методи динамічного дослідження у віртуалізованих середовищах (sandbox), а також інструменти на основі машинного навчання. Визначено, що інтеграція кількох підходів у межах єдиної системи забезпечує значне підвищення точності, адаптивності та швидкості реагування.

Запропоновано підхід до побудови багаторівневої системи кіберзахисту з урахуванням сучасних тенденцій та практик. Зокрема, рекомендовано впровадження рішень класу EDR/XDR для моніторингу кінцевих точок і мережевої активності, використання SOAR-платформ для автоматизації реагування на інциденти, а також реалізацію концепції Zero Trust для мінімізації ризиків несанкціонованого доступу.

Окремо підкреслено важливість організаційних заходів: регулярне резервне копіювання критичних даних, підвищення рівня кіберобізнаності персоналу, а також використання систем Threat Intelligence для оперативного отримання інформації про нові загрози. Сукупність зазначених технічних і управлінських механізмів створює надійну модель захисту в умовах зростання кількості цілеспрямованих атак.

Результати проведеного дослідження мають вагоме практичне значення та можуть бути використані під час модернізації корпоративних систем кіберзахисту, побудови адаптивних стратегій протидії сучасним загрозам та формування освітніх програм у сфері кібербезпеки. Окрім того, напрацювання створюють наукову базу для подальших досліджень, орієнтованих на розвиток інтелектуальних, самонавчальних систем виявлення шкідливого програмного забезпечення та автоматизованого управління інцидентами в умовах зростаючої складності та масштабності кіберзагроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. What is Malware? Malwarebytes. URL: https://www.malwarebytes.com/malware

2. Types of Malware. Kaspersky. URL: https://www.kaspersky.com/resource-center/threats/types-of-malware

3. What is Malware? Cisco. URL: https://www.cisco.com/site/us/en/learn/topics/security/what-is-malware.html

4. Malware Detection. CrowdStrike. URL: https://www.crowdstrike.com/en-us/cybersecurity-101/malware/malware-detection/

5. Top Malware Analysis Tools. Expert Insights. URL: https://expertinsights.com/network-security/the-top-malware-analysis-tools

6. Закон України №2163-19. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

7. Закон України №80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

8. Кримінальний кодекс України. Стаття 361. URL: https://protocol.ua/ua/kriminalniy_kodeks_ukraini_stattya_361/

9. Кримінальний кодекс України. Стаття 361-1. URL: https://protocol.ua/ua/kriminalniy_kodeks_ukraini_stattya_361_1_1/

10. Закон України №47/2017. URL: https://zakon.rada.gov.ua/laws/show/47/2017/ed20170225#n12

11. Будстандарт. ДСТУ 1. URL: https://online.budstandart.com/ua/catalog/doc-page?id_doc=66910

12. Будстандарт. ДСТУ 2. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66911

13. Будапештська конвенція про кіберзлочинність. URL: https://law.chnu.edu.ua/budapeshtska-konventsiia-pro-kiberzlochynnist/

14. Signature-Based Detection. Fidelis Security. URL: https://fidelissecurity.com/threatgeek/network-security/signature-based-detection/

15. Heuristic Detection. ReasonLabs Cyberpedia. URL: https://cyberpedia.reasonlabs.com/EN/heuristic%20detection.html

16. Heuristic Analysis. Fortinet. URL: https://www.fortinet.com/resources/cyberglossary/heuristic-analysis

17. Machine Learning in Malware Detection. Medium. Mawgoud. URL: https://mawgoud.medium.com/machine-learning-in-malware-detection-concept-techniques-and-use-cases-1067d99208ac

18. Cybersecurity 101: Sandboxing. Medium.Ilham Firdiyanto. URL: https://medium.com/@ilham.firdiyanto/cybersecurity101-sandboxing-in-malware-analysis-ee4bc5382bce

19. Importance and Limitations of Sandboxing. Forbes. URL: https://www.forbes.com/councils/forbestechcouncil/2023/08/17/importance-and-limitations-of-sandboxing-in-malware-analysis/

20. Sandbox Environment for Testing. Testgrid. URL: https://testgrid.io/blog/sandbox-environment-for-testing/

21. Modern Hybrid Infrastructures. Forbes. URL: https://www.forbes.com/sites/connection/2024/10/28/enabling-performance-and-security-why-it-departments-no-longer-have-to-choose-with-modern-hybrid-infrastructures/

22. Malware Statistics and Trends. ControlD. URL: https://controld.com/blog/malware-statistics-trends/

23. EDR vs Antivirus. InventiveHQ. URL: https://inventivehq.com/edr-vs-antivirus-why-traditional-security-isnt-enough/#:~:text=%E2%9D%8C%20It%20relies%20on%20known,day%20attacks

24. Discussion on Antivirus. Quora. URL: https://www.quora.com/Why-are-there-people-who-recommend-not-using-an-antivirus

25. ITSSI Journal. URL: https://itssi-journal.com/index.php/ittsi

26. Automation and Response. Security Orchestration, TuxCare. URL: https://tuxcare.com/blog/security-orchestration-automation-and-response/

27. Вісник ЛДУ БЖД. URL: https://journal.ldubgd.edu.ua/index.php/Visnuk

28. Zero Trust. CyberSet. URL: https://cyberset.com.ua/cybersecurity/zero-trust

29. Human Error. Australian Cyber Security Magazine. URL: https://australiancybersecuritymagazine.com.au/almost-100-cyber-incidents-result-of-human-error/#:~:text=The%20recent%20Future%20of%20Cyber,are%20caused%20by%20human%20error

30. Threat Intelligence. CrowdStrike. URL: https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/#:~:text=Threat%20intelligence%20refers%20to%20the,in%20defending%20against%20cyber%20threats