Харківський національний університет імені В.Н. Каразіна

Факультет комп'ютерних наук

Безпека інформаційних систем і технологій

«Допущено до захисту»

Зав. кафедрою БІСТ

Сватовський І.І _____

« » 2023 р.

Пояснювальна записка

до кваліфікаційної роботи бакалавра

за спеціальністю: 125 - Кібербезпека

на тему: «Аналіз розвитку і використання експлойтів, та дослідження можливостей протидії цій загрозі»

Оцінка « » Керівник Малахов С.В.
(прізвище та ініціали/підпис)

Голова ЕК Рецензент Гостев О.Л.
(прізвище та ініціали/підпис)

Лемешко О.В._____ Виконавець студентка групи КБ-42

Богданова Є.С.
(прізвище та ініціали/підпис)

Харків – 2023

РЕФЕРАТ

Пояснювальна записка містить: 63 сторінки, 7 рисунків, 1 таблицю, 31 використаних джерел, 1 додаток.

Мета роботи: - аналіз розвитку і особливостей використання експлойтів та узагальнення основних напрямів протидії цій загрозі.

Об’єкт дослідження: - способи застосування експлойтів, як інструменту здійснення атак і засобу тестування вразливостей сучасних інформаційних систем (ІС) та мережевого обладнання.

Предмет дослідження: - заходи комплексної протидії атакам, що обумовлені впливом (експлуатацією) експлойтів.

Основними методами досліджень є аналіз та порівняння.

В роботі досліджено питання розвитку і практичного застосування експлойтів, як засобу реалізації атак та інструменту для проведення тестувань ІС на проникнення (*pentesting*). Розглянуто відомі інциденти з використанням експлойтів за останні 5 років. Проведено аналіз типової внутрішньої побудови експлойтів та запропоновано їх класифікацію. Окрема увага приділена питанням узагальнення можливостей з протидії атакам, котрі використовують експлойти. Виконано аналіз й узагальнення методів та технологій, що можуть бути використані для завчасного виявлення та запобігання вразливостей нульового дня (zero-das експлойтів).

Результати роботи можуть бути використані в освітніх цілях та як допоміжний (довідковий) матеріал для підвищенні рівня обізнаності персоналу сучасних компаній з питань: - протидії атакам з використанням експлойтів; - та усунення передумов експлуатації вразливостей в наявному програмному забезпеченні (ПЗ).

Ключові слова: ЕКСПЛОЙТИ, ВРАЗЛИВОТСІ, ИНФОРМАЦІЙНА СИСТЕМА, ЗАГРОЗА, ІНФОРМАЦІЙНА БЕЗПЕКА, EXPLOIT KIT, CVE, АТАКА, АНТИВІРУС, ПАТЧ-БЕЗПЕКИ.

ABSTRACT

The explanatory note to the master's project contains: 63 pages, 7 figures, 1 table, 31 source references, 1 appendix.

The purpose of the work: - analysis of the development and features of the use of exploits and generalization of the main directions of counteraction to this threat

The object of research: - methods of using exploits as a tool for conducting attacks and a means of testing vulnerabilities of modern information systems (IS) and network equipment.

Subject of research: - measures to counter attacks caused by the influence (exploitation) of exploits.

The main research methods are analysis and comparison.

The paper examines the development and practical use of exploits as a means of implementing attacks and a tool for conducting IS penetration testing (pentesting). Known incidents with the use of exploits over the past 5 years have been considered. An analysis of the typical internal construction of exploits was carried out and their classification was proposed. Special attention is paid to the issues of generalization of possibilities for countering attacks that use exploits. The analysis and generalization of methods and technologies that can be used for early detection and prevention of zero-day vulnerabilities (zero-das exploits) is performed.

The results of the work can be used for educational purposes and as auxiliary (reference) material to increase the level of awareness of the personnel of modern companies on the following issues: - countering attacks using exploits; - and elimination of prerequisites for exploiting vulnerabilities in existing software (software).

Key words: EXPLOITS, VULNERABILITIES, INFORMATION SYSTEM, THREAT, INFORMATION SECURITY, EXPLOIT KIT, CVE, ATTACK, ANTI-VIRUS, SECURITY PATCHES.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ СКОРОЧЕНЬ І ТЕРМІНІВ

ІБ	–	Інформаційна безпека
ІС	–	Інформаційна система
ПЗ	–	Програмне забезпечення
ШІ	–	Штучний інтелект
AI	–	Artificial Intelligence
API	–	Application Programming Interface
IDS/IPS	–	Intrusion Detection System / Intrusion Prevention System
USB	–	Universal Serial Bus
VPN	–	Virtual Private Network
XDR	–	Extended Detection and Response
ОС	–	Операційна система
EK	–	Exploit Kit
CVE	–	Common Vulnerabilities and Exposures
SE	–	Social Engineering
RAT	–	Remote Access Trojan
НСД	–	Нерозподілена система даних
FUD	–	Full UnDetectable
SQL	–	Structured Query Language
CVSS	–	Common Vulnerability Scoring System
ML	–	Machine Learning
DNS	–	Domain Name System
NVD	–	National Vulnerability Database
POP	–	Post Office Protocol
IMAP	–	Internet Message Access Protocol

HTTP	–	Hypertext Transfer Protocol
FTP	–	File Transfer Protocol
XSS	–	Cross-Site Scripting
APT	–	Advanced Persistent Threat
SSDLC	–	Secure Software Development Lifecycle

ВСТУП

За останні 20 років, у сфері забезпечення інформаційної безпеки (ІБ), експлойти (*фр. exploit – експлуатувати*) продовжують залишатися однією з серйозних проблем. Сучасні зловмисники використовують все більше та більше різних методів для порушення безпеки систем і програм. Одним з найпоширеніших методів атак є використання експлойтів, тобто програмного коду, який використовує вразливості програм та операційної системи (ОС) для здійснення атак. Проблема існування експлойтів практично однаково стосується, як розробників програмного забезпечення (ПЗ) і різних захисних рішень, так і співробітників підрозділів ІБ компаній, та організацій. При цьому серед професійних спеціалістів, досі зберігається неоднозначність у визначенні фактичної ролі та місця експлойтів. І насамперед, в частині того, чи може експлойт самостійно наносити шкоду інформаційній системі (ІС) і/або її інформаційним ресурсам, або ж його слід розглянути, як інструмент (засіб) для вторгнення і наступного запуску іншого шкідливого коду. [1]

Пік «популярності» експлойтів припадає на минуле десятиліття, однак вони досі розглядаються зловмисниками, як ефективний «прецизійний» засіб для проникнення в сучасні ІС *(наприклад, атака вірусу WannaCryptor)*. При цьому експлойти стають все більш вишуканими, враховуючи особливості як атакуючого ресурсу, так і його системи безпеки. [1]

З ростом використання цифрових технологій з'являється все більше загроз для кібербезпеки, зокрема зловмисниками використовуються експлойти - програмні помилки, що застосовуються для отримання несанкціонованого доступу (НСД) до цільової комп'ютерної системи (засобу). Розвиток технологій дозволяє зловмисникам створювати все більш складні та небезпечні експлойти, що вносять серйозні загрози для інформаційної безпеки (ІБ) сучасних ІС.

Метою даної роботи є аналіз особливостей використання експлойтів та дослідження можливостей протидії цій загрозі. У роботі розглянуто основні етапи розвитку та різновиди відомих експлойтів і визначені особливості їх застосування при реалізації різних стратегій атак. В межах роботи виконано аналіз існуючих напрямів парирування цій загрозі та сформульовані пропозиції, стосовно можливостей комплексної протидії при реалізації відомих методик та засобів атак з використанням експлойтів.

Тематика досліджень є безумовно актуальною, оскільки безпека ІС залишається однією з найважливіших проблем у сучасному світі, а питання використання експлойтів, як інструменту здійснення атак, на превеликий жаль, досі залишаються в умовній "зоні тіні" (з погляду уваги профільних фахівців), що створює серйозні передумови для постійної та прихованої експлуатації даного типу загроз безпеці.

Зростання кількості кібератак та збільшення кількості пошкоджень від них змушує розробників ПЗ та спеціалістів з кібербезпеки постійно вдосконалювати свої методи та засоби захисту. Такі атаки можуть призвести до дуже серйозних наслідків, таких як витік конфіденційної інформації, крадіжка коштів, контроль роботи використовуваних Web-сервісів, реалізація несанкціонованих дій в технологічних процесах та довготривале порушення функціонування ІС критичної інфраструктури тощо. Тому, з урахуванням все більш масштабної цифровізації всіх сфер життя сучасного суспільства, протидія цій загрозі стає все більш актуальною задачею для багатьох компаній, установ та організацій. Поряд з цім, відомо [2], що за допомогою застосування програм експлойтів, фахівцями з ІБ може тестуватися на проникнення їх ІТ інфраструктури, що дозволяє завчасно відтворювати різні вектори атак на власні корпоративні ресурси. Більш того, оскільки у пошуку вразливостей «зацікавлені» обидві сторони, то активних експлойтів стає все більше [2]. Вочевидь, що для упорядкування цього напрямку діяльності, необхідна класифікація, як вже існуючих, так і майбутніх експлойтів, що в певній мірі полегшить організацію протидії потенційним зловмисникам та допоможе впорядкувати роботу фахівців ІБ у разі виникнення подібних загроз

(атак на інформаційні ресурси). Саме тому в роботі приділено найпильнішу увагу огляду відомих інцидентів з використання експлойтів, а також питанням класифікації, застосування й методам запобігання атакам з їх використанням. Таким чином, всебічний розгляд відповідних питань має своєю ціллю формування рекомендацій щодо комплексного усунення передумов реалізації відповідного типу загроз, із урахуванням наявного досвіду та специфік відомих інцидентів.

1 ОГЛЯД ІНЦИДЕНТІВ З ВИКОРИСТАННЯ ЕКСПЛОЙТІВ

Використання експлойтів як вид атаки на скомпрометовану систему існує с появи комп'ютерів. Перший експлойт був призначений для злому системи з контролю версій, яку розробив Дуглас Інгелбарт у 1967 р. для управління документами і кодом програмного забезпечення. Цей експлойт дозволяв користувачам отримувати несанкціонований доступ до інформації, що зберігалася в системі контролю версій, і змінювати її за потреби. З подальшим розвитком технологій інструментів, прийомів і технологій, які використовують зловмисники, експлойти теж еволюціонують.

Згідно з опитуванням аналітичної компанії CheckPoint Research, освіта та наукові дослідження є галуззю, яка найбільше постраждала від кібератак у 2021 році: у середньому 1605 атак на заклад на тиждень, що на 75% більше, ніж у 2020 році. [3]

Інші сектори, такі як уряд/військові, зазнають 1100 атак на тиждень у 2021 році, що на 47% більше, ніж у 2020 році. Крім того, галузь зв'язку спостерігала 1079 кібератак на тиждень, що на 51 відсоток більше, ніж у 2020 році. Крім того, у 2021 році в Африці було зафіксовано найбільшу кількість атак, у середньому 1582 атаки на тиждень, що на 13% більше, ніж у 2020 році. [3]

Експлойти за останні роки набули популярності у зловмисників і використовуються майже у всіх атаках на вразливі ПЗ.

Як можна побачити з Рис.1.1, експлойти для вразливостей ОС та ПЗ також є досить поширеними, оскільки зловмисники можуть використовувати вразливості, які не були відомі розробникам програмного забезпечення.

Найчастіше зловмисники компанують експлойти в паки, так називаємі Exploit Kit (EK). [1]. Перший задокументований випадок набору експлойтів був знайдений на російських підпільних форумах наприкінці 2006 року під назвою MPack. З самого початку автори наборів експлойтів створювали свою програму

як комерційний пакет, який часто включав підтримку та надання регулярних оновлень. Паки можуть використовувати експлойти, спрямовані на різне програмне забезпечення, включаючи Adobe Flash Player, Adobe Reader, Internet Explorer, Oracle Java і Sun Java.

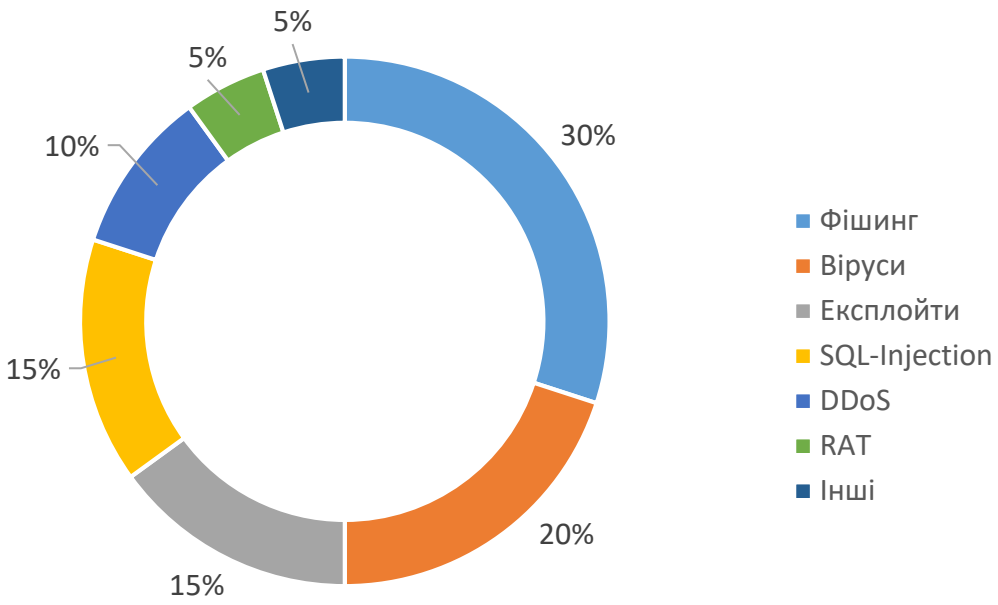


Рисунок 1.1 – Розподіл експлойтів при здійсненні атак

За останні 5 років на ринку експлойтів та ЕК відбулися значні зміни. Зокрема, багато відомих EKs, таких як Angler, Nuclear, Neutrino, та Magnitude, були закриті, що спричинило зменшення кількості EKs на ринку. Однак, деякі EKs, такі як RIG, GrandSoft та Fallout, залишилися активними і продовжували використовувати вразливості в програмному забезпеченні для здійснення атак. Ще одна причина зменшення прибутку від торгівлі експлойтів можна пов'язати зі зростанням виплат за програмами Bug Bounty - полювання на баги. Можливість легально отримати велику винагороду призводить до часткової декриміналізації ринку експлойтів і робить його мізернішим і мінливішим.

На рис1.2 можна побачити тенденцію змін вискористання експлойт-паків. Так, RIG EK є одним із популярних наборів експлойтів навпротязі 5 років, який широко поширюється через рекламні кампанії, такі як Fobos. RIG Exploit Kit

переживає свій найуспішніший період, щодня роблячи приблизно 2000 спроб вторгнень і вдаючись приблизно в 30% випадків, що є найвищим показником за довгу історію його роботи. [4] Використовуючи відносно старі вразливості Internet Explorer, RIG EK поширювала різні сімейства зловмисних програм, зокрема Dridex, SmokeLoader і RaccoonStealer. Цей EK залишається популярним завдяки постійним оновленням свого внутрішнього складника, тобто оновлюються експлойти, що використовуються. У останньому екземплярі RIG набір експлойтів містить два блискучі нові експлойти: CVE 2021-26411 і CVE-2020-0674 [4-5]. Завдяки цьому новому технічному прогресу його успішне використання різко зросло й досягло історичного максимуму в 30% у 2022 році.

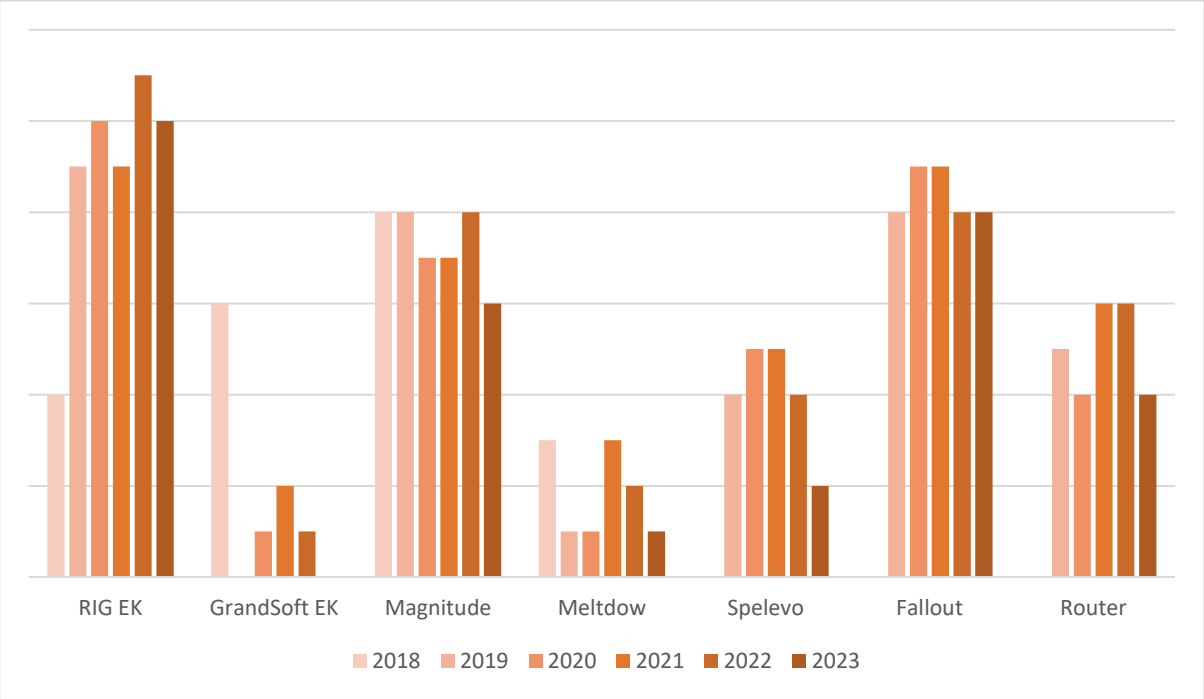


Рисунок 1.2 – Динаміка змін у використанні експлойт-паків

Набір експлойтів Magnitude, спочатку відомий як PopAds, існує принаймні з 2012 року, що є надзвичайно довгим терміном служби для набору експлойтів. Однак сьогодні це не той набір експлойтів, який був на початку. Відтоді практично кожна частина Magnitude змінювалася кілька разів. Змінилася інфраструктура, а також цільова сторінка, шелл-код, обфускація, корисне навантаження та, найголовніше, експлойти. Наразі Magnitude використовує вразливість Internet Explorer, яка може призвести до пошкодження пам’яті, CVE-

2021-26411, щоб забезпечити виконання шелл-коду всередині процесу візуалізації, і вразливість, яка може призвести до пошкодження пам’яті Windows, CVE-2020-0986, щоб згодом підвищити привілеї [5]. Повністю функціональний експлойт для CVE-2021-26411 можна знайти в Інтернеті, і Magnitude використовує цей загальнодоступний експлойт безпосередньо, лише з додаванням деякої обфускації зверху [5-6]. Цей CVE вперше був використаний у цілеспрямованій атаці на дослідників безпеки, яку Google Threat Analysis Group приписала Північній Кореї.

У період з 2018 по 2019 роки більшість експлойтів були націлені на вразливості в ПЗ браузерів, зокрема в Google Chrome та Firefox, а також на вразливості в ПЗ Adobe Flash Player та Microsoft Office. Ці вразливості залишалися основним об'єктом атак EKs, оскільки вони надавали можливість злочинцям отримати доступ до системи потенційної жертви та виконувати код з підвищеними привілеями. CVE-2018-8174 Internet Explorer і CVE-2018-15982 Flash Player є найпоширенішими уразливими місцями, тоді як старіша CVE-2018-4878 (Flash) все ще використовується деякими EK [5, 7].

Вісім із десяти найпоширеніших вразливостей, використовуваних кіберзлочинцями в рамках фішингу, наборів експлойтів або атак троянів віддаленого доступу (RAT) протягом 2018 року, були спрямовані на програмні продукти Microsoft, продовжуючи тенденцію, розпочату в 2017 році. Microsoft продовжує залишатися головною мішенню для зловмисників після такого ж 2017 року, коли найбільше використовуваних уразливостей перейшли з Flash Player від Adobe. [7]

У 2020 році відбулася зміна фокусу злочинців на використання вразливостей в ПЗ VPN-клієнтів, таких як Pulse Secure та Fortinet. Це пов'язано з тим, що багато компаній та організацій переходять на роботу з віддалених місць через VPN, що робить такі вразливості особливо цінними для злочинців. Крім того, зловмисники все частіше використовують соціальну інженерію та спам для

надсилання шкідливих посилань і файлів, що дозволяє їм обходити захист периметра мережі та проникати в системи потенційних жертв [8-9].

Як згадувалося вище, експлойти, націлені на продукти Microsoft, є найбільш популярними (22%). Останніми роками цей вид нападу став більш поширеним. Лише 5% «покупців» прагнуть використовувати пристрої Інтернету речей (IoT) (рис. 1.3), це свідчить про те, що зі збільшенням кількості підключених пристроїв для зловмисників буде більш прибутково напрявляти свої атаки на цей сегмент, особливо з урахуванням того, що багато IoT-пристроїв важко піддаються виправленню, а на деяких встановлення оновлень не передбачено взагалі.

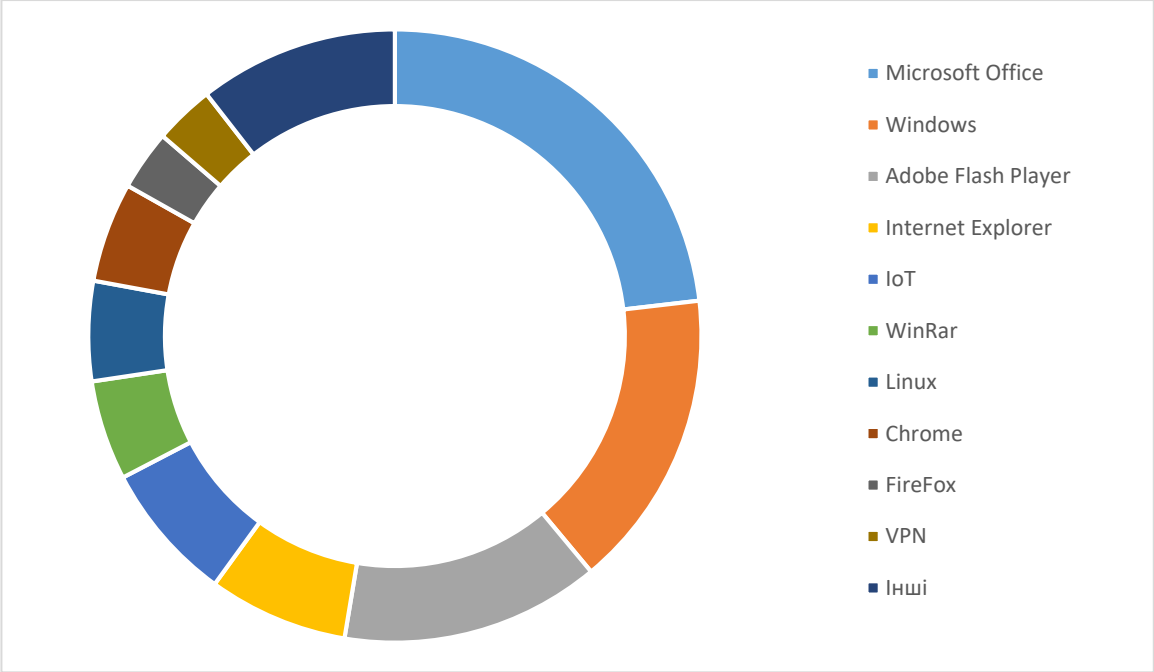


Рисунок 1.3 – Найпопулярніші експлойти на кіберфорумах

Загалом, на ринку EKs спостерігається тенденція до використання більш складних та раніше невідомих експлойтів, а також до комбінації різних методів атак для досягнення своїх цілей. Узагальнення звітів за 2021 рік показує, що було виявлено більше 29 тисяч різних зразків експлойтів, що є значним зростанням порівняно з попередніми роками. Більшість зразків були призначені для отримання несанкціонованого доступу (НСД) до пристроїв та даних

користувачів, а також для встановлення шкідливого ПЗ на ПК та мобільні пристрої жертв атаки. [10]

Серед найпоширеніших вразливостей, які використовувалися в експлойтах, були такі, які стосувалися веб-додатків, браузерів та операційних систем. Зокрема, найбільш націленими вразливостями стали такі, які стосувалися вразливостей:

- в ПЗ веб-серверів, таких як Apache та Nginx;
- в веб-додатках, таких як WordPress, Drupal та Joomla;
- в браузерах, зокрема Google Chrome, Firefox та Microsoft Edge;
- в операційних системах, зокрема Windows та Android.

Під час атак, зловмисники часто використовують такі експлойти для отримання доступу до пристроїв користувачів та для встановлення різних типів шкідливого ПЗ: - троянській кінь, шпигунські програми, розширення для браузерів та ін. Ці атаки можуть мати серйозні наслідки для користувачів та компаній, так як можуть призвести до втрати та/або порушення конфіденційності даних, викрадення грошей, перехвату управління ОС та інших шкідливих наслідків.

З початку 2020 року серед кіберзлочинців набула популярності пропозиція підписки на щомісячне оновлення експлойтів, що дозволяє зловмисникам легко і регулярно здійснювати атаки.[11] Ця підписна модель стала прибутковою як для вендорів програмного забезпечення, так і для кіберзлочинців, які пропонують передплату на свіжі експлойти за певну щомісячну плату, що варіюється від 60 до 2000 доларів США.

Один з таких продавців пропонував місячну підписку на збірник експлойтів за ціною від 60 доларів США [12]. Його сервіс включав кілька категорій експлойтів, таких як експлойти для Microsoft Word, Microsoft Excel і JavaScript, і гарантував повну невиявленість (FUD - Full UnDetectable) цих експлойтів, а також щотижневе оновлення. Крім того, передплатник мав

можливість вибрати конкретні експлойти для використання в своїх файлових атаках як корисні навантаження.

Інший продавець пропонував конструктор шкідливого програмного забезпечення за ціною 1150 доларів США на місяць. [13] Цей конструктор включав експлойти для вразливостей CVE-2017-11882, CVE-2017-8570 та CVE-2018-0802, і також гарантував їх невиявленість під час виконання, а також щомісячне оновлення [5]. Послуги, що пропонувалися у рамках таких підписок, сприяли швидкому доступу недосвідчених користувачів до кіберзлочинної діяльності, оскільки більшість процесів були автоматизовані, що значно знижувало бар'єри для вступу у світ кіберзлочинності. Частота використання експлойтів залежить від багатьох факторів, таких як поширеність вразливості, наявність публічної інформації про неї, складність експлойтування та багато іншого.

В Табл.1 перераховані кілька зразків вразливостей, які були найбільш часто використовувалися в експлойтах протягом останніх років [5]:

Табл. 1 – Найбільш поширені вразливості за 5 років

CVE	Компанія	Продукт	Ekploit Kit	CVSS	Опис
CVE-2017-11882	Microsoft	Microsoft Office	Exploit Kits	Високий (9.8)	Вразливість у Microsoft Office, яка дозволяє виконання коду з підвищеними привілеями.

Продовження таблиці 1 – Найбільш поширені вразливості за 5 років

CVE	Компанія	Продукт	Ekploit Kit	CVSS	Опис
CVE-2018-8174	Microsoft	Internet Explorer	RIG, Fallout	Високий (9.8)	Вразливість дозволяє виконання коду з підвищеними привілеями. Зловмисники можуть створити спеціально створений веб-сайт і переконати користувача відвідати його. При цьому використовується вразливість, що дозволяє виконувати шкідливий код на комп'ютері потенційної жертви з правами користувача.
CVE-2018-4878	Adobe	Adobe Flash Player	Magnitude, GrandSoft	Високий (9.8)	Вразливість яка дозволяє виконання коду з підвищеними привілеями. Зловмисники можуть вбудовувати шкідливий код у веб-сторінки або відправляти його через електронну пошту з метою виконання коду на комп'ютері потенційної жертви з правами користувача.
CVE-2019-11510	Pulse Secure	Pulse Connect Secure	RIG EK	Високий (9.8)	Вразливість яка дозволяє отримати доступ до системи потенційної жертви. Зловмисники можуть використовувати цю вразливість для отримання доступу до конфіденційної інформації або виконання інших шкідливих дій.

Продовження таблиці 1 – Найбільш поширені вразливості за 5 років

CVE	Компанія	Продукт	Ekploit Kit	CVSS	Опис
CVE-2019-19781	Citrix	Citrix Application Delivery Controller, Citrix Gateway	RIG EK	Високий (9.8)	Вразливість яка дозволяє отримати доступ до системи потенційної жертви. Зловмисники можуть використовувати цю вразливість для отримання доступу до конфіденційної інформації або виконання інших шкідливих дій.
CVE-2020-1472	Microsoft	Microsoft Active Directory	RIG EK	Критичний (10.0)	Вразливість яка дозволяє отримати повний доступ до доменного контролера без автентифікації. Зловмисники можуть використовувати цю вразливість для отримання контролю над мережею та виконання шкідливого коду.

Варто зауважити, що це лише деякі зразки вразливостей, які найчастіше всього використовувалися у експлойтах в останні роки. Нападники постійно шукають нові вразливості та способи їх практичної експлуатації, тому вкрай важливо своєчасно забезпечувати захист та оновлення прикладного ПЗ забезпечення та ОС, щоб зменшити ризики відповідних атак.

Очевидно, що без існування вразливостей не буде експлойта, оскільки саме вони і є умовною «точкою входу» для експлойтів в систему (апаратний пристрій), що атакується. Відповідно, логічно класифікувати експлойти за типом уразливості, яку вони використовують, наприклад : - переповнення буферу; міжсайтовий скриптинг; підробка міжсайтових запи- тів; SQL-ін'єкція; атака повернення до бібліотеки та інші. [2]

[2]Існують Загальна система оцінки вразливостей 2.0 (CVSS – з англ. Common Vulnerability Scoring System) та рівень загрози експлойту, за допомогою яких можна дізнатися ступінь небезпеки для пристрою, що атакується. На рис. 1.4 – 1.5 приведені відомості CVSS та рівень загроз експлойту, станом на 2019–2022 р. Як можна помітити 34% відомих експлойтів мають високий рівень загрози (CVSS ≥ 7), а 54% експлойтів мають середній рівень (CVSS < 7 та CVSS ≥ 4). Тобто, 88% загальнодоступних експлойтів розроблені для вразливостей середнього чи високого ступеня небезпеки. [2]

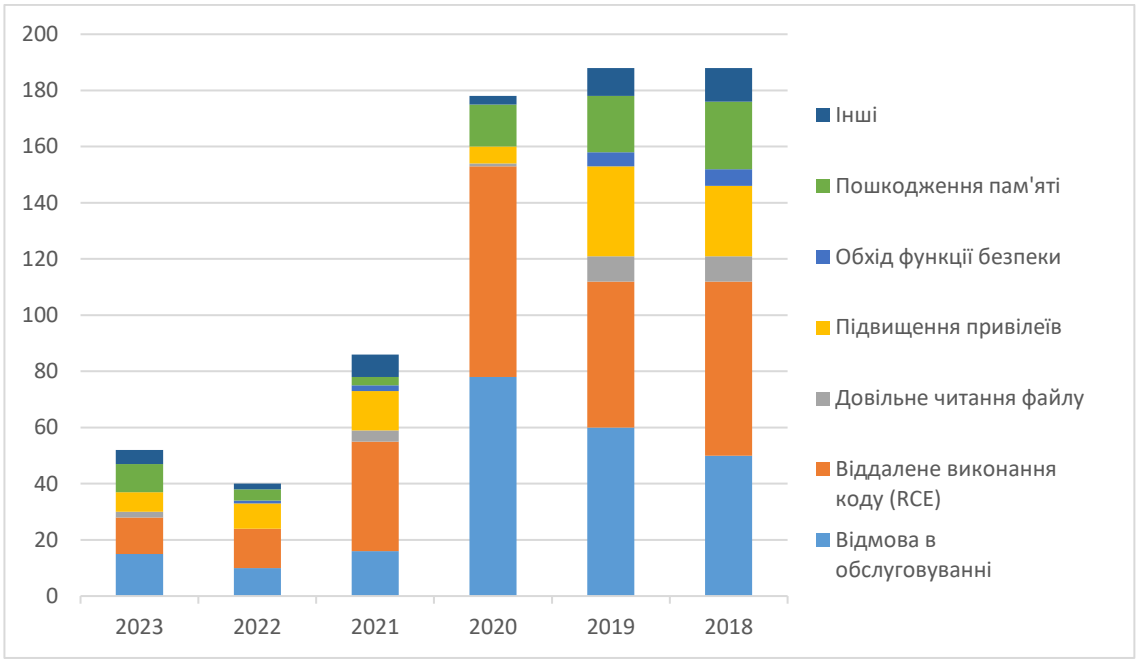


Рисунок 1.4 – Використання та розподіл експлойтів за частотою використання вразливостей, що експлуатуються. (за даними CVE)

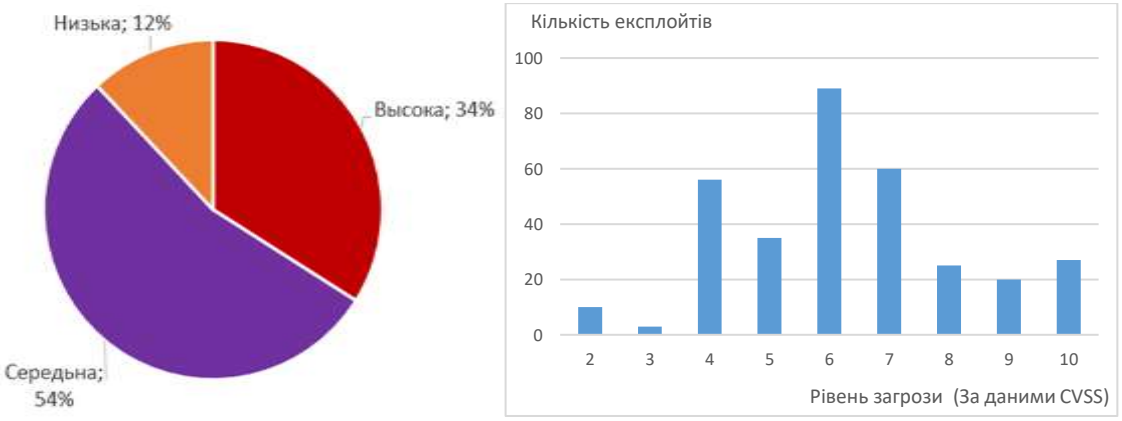


Рисунок 1.5 – Розподіл експлойтів за рівнем за- грози вразливості

2 УЗАГАЛЬНЕННЯ ПИТАНЬ ВИКОРИСТАННЯ ЕКСПЛОЙТІВ

Останні тенденції у практичному використанні експлойтів можна поділити на кілька категорій:

1) Використання штучного інтелекту (AI - *Artificial Intelligence*) та машинного навчання (ML - *Machine Learning*) в розробці нових та модифікації існуючих експлойтів. Зловмисники використовують ці технології для пошуку та експлуатації вразливостей у існуючому ПЗ та мережевих протоколах, та використовують ML для створення нових типів експлойтів.

2) Використання вразливостей "нульового дня" (zero-days) [2, 12] - це випадок експлуатації вразливості, про які відомо тільки зловмисникам, але не розробникам ПЗ. Такі вразливості дозволяють кіберзлочинцям ефективно проникати в системи та отримувати доступ до конфіденційної інформації. У 2021 році були виявлені декілька серйозних вразливостей zero-days, зокрема в Microsoft Exchange та VMware;

3) Використання SE-атак - зловмисники активно використовують прийоми і техніки соціального інжинірингу для отримання доступу до систем [9, 13]. Наприклад, вони можуть надіслати фішингові електронні листи, які містять посилання на шкідливі веб-сторінки, або надіслати відомості для входу на фальшиві веб-сайти;

4) Підтримка атак на хмарні сервіси - зростає кількість компаній, які переходять на хмарні рішення, тому зловмисники активно шукають відповідні вразливості в хмарних сервісах та використовують експлойти для здійснення атак. У 2021 році були виявлені кілька серйозних вразливостей в хмарних сервісах, зокрема в сервісах Microsoft Azure та Amazon Web Services; [10]

5) Витік конфіденційної інформації - зловмисники можуть використовувати експлойти, щоб отримати доступ до конфіденційної інформації [12], такої як логіни та паролі, кредитні картки та інша особиста інформація. Пізніше ця інформація може бути використана для крадіжки грошей, викрадення

особистої ідентичності на різних комунікаційних майданчиках та ресурсах [8, 9] або здійснення інших шахрайських дій.

6) Використання експлойтів для шпигунства - зловмисники можуть використовувати експлойти, щоб отримати доступ до ПК та інших пристроїв, щоб надалі здійснювати шпигунські операції. Наприклад, вони можуть здійснювати прослуховування, відстеження дій користувачів та витік конфіденційної та/або персоніфікованої інформації [14].

7) Використання експлойтів для кібершантажу [13] - зловмисники можуть використовувати експлойти для завдання шкоди ПК та іншим пристроям жертви атаки, з метою компрометації їх користувача та/або отримання викупу (фінансової винагороди) за повернення контролю над атакованими системами . Наприклад, розробники вірусів-вимагачів часто використовують експлойти для злому систем та заблокування доступу до них, після чого вимагають викуп за повернення доступу. [4]

8) Розширення використання експлойтів для атак на мобільні пристрої. Зараз на ринку присутні десятки мільярдів смартфонів та інших мобільних пристроїв. Зловмисники можуть використовувати різноманітні вразливості в ОС та додатках, що працюють на цих пристроях, для отримання доступу до конфіденційної інформації користувачів.

Насамперед, сам експлойт не надає шкоди вразливому ПЗ або системі. Загально кажучи, способи застосування експлойтів залежать від конкретної вразливості та цілей зловмисника.

Зловмисники використовують експлойти з метою злому або атаки на систему чи мережу з незаконними намірами. Вони шукають вразливості у програмах, операційних системах, мережевих протоколах або апаратному забезпеченні, і використовують експлойти для отримання несанкціонованого доступу, виконання шкідливого коду, отримання конфіденційної інформації або зламу системи.

Зловмисники можуть використовувати готові експлойти, які вони знаходять в публічних базах даних, форумах чи інших джерелах. Вони також можуть самостійно розробляти свої експлойти, використовуючи знання про вразливості та методи їх експлуатації.

Експлойти для переповнення буферу, міжсайтовому скриптингу, ін'єкціяї SQL, заперечення обслуговування та умови змагання можуть бути використані зловмисниками для введення системи в некоректний стан, що може призвести до відмови системи або несправностей в її роботі. [15]

Експлойти Reverse Shell та Backdoor використовуються для встановлення зворотного з'єднання з цільовою системою. Це може дозволити зловмисникам виконувати команди на цільовій системі з віддаленої локації. [15]

Також вище перечисленні експлойти можуть бути застосовані для деанонімізації користувачів, тобто для визначення їхньої ідентичності або місцезнаходження в Інтернеті. Зловмисники завдяки цим експлойтам використовують вразливості в браузерах, мережевих протоколах та сервісах, щоб отримати доступ до інформації про користувача, включаючи їхню IP-адресу, місцезнаходження або ідентифікатори сесій, тобто займаються незаконним збором інформації про цільову систему, її налаштування та конфігурацію. Ця інформація може допомогти зловмисникам пізніше здійснити таргетовані атаки на цю систему.

З іншого боку, тестувальники можуть використовувати експлойти в контексті етичного хакінгу або тестування на проникнення для виявлення потенційних вразливостей у системі та оцінки їх наслідків [16]. Використання експлойтів тестувальниками допомагає виявити слабкі місця і недоліки в безпеці системи перед тим, як вони можуть бути зловживанні зловмисниками.

Тестувальники можуть використовувати різноманітні експлойти для перевірки системи на наявність вразливостей. [2, 12]. Це можуть бути вразливості в ПЗ, ОС, мережевих протоколах або апаратному забезпеченні. Вони

можуть використовувати наявні знання про вразливості та спеціально створені або доступні експлойти для реалізації спроб НСД до системи-жертви, виконання шкідливого коду та/або зламу інших рівнів захистів [14].

Використання експлойтів тестувальниками вимагає знань і експертизи в області безпеки, а також відповідального підходу. Тестувальники повинні дотримуватись етичних принципів та правил, не завдаючи шкоди системі або зловмисниками. їх мета полягає в ідентифікації вразливостей та наданні рекомендацій щодо їх виправлення.

Пентестери або інженери з ІБ можуть використовувати ЕК як засіб швидкого та простого виявлення та використання вразливостей у цільовій системі та для аналізу мережі. Використовуючи попередньо упаковані експлойти, пентестери можуть заощадити час і ресурси, які в іншому випадку знадобилися б для розробки експлойтів для кожної вразливості. Завдяки відомим експлойт-пакам як Metasploit яка є платформою з відкритим вихідним кодом, або Canvas чи Core Impact, які є комерційними ЕК, можна підбирати/створювати/модифікувати експлойти під різні види вразливостей завдяки їхній великій бібліотеці експлойтів для різних платформ та додатків [17].

З погляду дослідницької діяльності, експлойти використовуються для виявлення нових вразливостей в програмному забезпеченні та системах. Дослідники з безпеки виконують аналіз програм, операційних систем, мереж та інших компонентів, щоб ідентифікувати можливі слабкі місця і вразливості. [15]

Дослідники можуть розробляти власні експлойти або використовувати вже існуючі, які були розкриті в межах відкритої інформації. Вони аналізують програми та системи, шукають уразливості і розробляють спеціальні кодові фрагменти, що використовують ці уразливості. Ці кодові фрагменти, можуть бути використані для виконання контрольованої атаки з метою перевірки та демонстрації уразливості.

Систематизація роботи з аналізу відомих експлойтів допомагає виробникам ПЗ і розробникам мережевого устаткування завчасно передбачити та врахувати появу нових вразливостей. Такі дослідження надають цінну інформацію про потенційні ризики та «слабкі» місця, що дозволяє покращити безпеку програм та систем. В межах цієї роботи дослідники можуть, також, спілкуватися з виробниками та постачальниками послуг, повідомляючи їх про виявлені вразливості та пропонуючи рекомендації щодо їх виправлення, що сприяє підвищенню фактичного рівня безпеки використовуваних ІС.

Важливо зауважити, що дослідники з безпеки повинні дотримуватися певних етичних принципів та встановлених правил поведінки, наприклад таким, як *Responsible Disclosure* (відповідальне повідомлення про вразливості). Це означає, що вони повинні повідомляти виробників про виявлені вразливості та надавати достатній строк для виправлення перед розкриттям деталей глобально [2]. Це дозволяє виробникам вчасно виправити проблему та запобігти можливим зловживанням з їх використанням.

3 ОСОБЛИВОСТІ АНАЛІЗУ ЕКСПЛОЙТІВ ЇХ ПОБУДОВА ТА РІЗНОВИДИ

3. 1 Методи аналізу експлойтів

До найбільш поширених методів і способів аналізу експлойтів, які успішно застосовуються для дослідження розвитку й використання експлойтів, слід віднести наступні:

Реверс-інженерія (англ. reverse engineering) - це процес аналізу ПЗ або пристроїв з метою з'ясування їхньої структури та принципів функціонування. Цей процес часто застосовується для виявлення вразливостей у програмах та пристроях, включаючи експлойти. В цьому разі для аналізу експлойтів можуть використовуватися наступні способи реверс-інженерії [18]:

- Дизасемблюція: цей метод полягає в перетворенні машинного коду експлойту на асемблерний код для дослідження його структури та функціонування.
- Декомпіляція: цей метод зазвичай застосовується для аналізу вихідних кодів програм. Він полягає в перетворенні машинного коду на вихідний код програми для аналізу та зрозуміння її функціоналу.
- Відладка: цей метод застосовується для аналізу експлойту під час його виконання. Він дозволяє досліджувати поведінку програми та виявляти вразливості в процесі її виконання.
- Аналіз пам'яті: цей метод використовується для аналізу пам'яті, що використовується програмою. Він дозволяє досліджувати дані, що зберігаються в пам'яті програми, та виявляти вразливості.
- Дослідження вразливостей - пошук вразливостей у програмному забезпеченні, що можуть бути використані для створення експлойтів.

Моніторинг вразливостей - це процес виявлення та аналізування вразливостей в наявному ПЗ, ОС та інших складових обчислювальної

інфраструктури [19]. Моніторинг вразливостей може бути використаний як спосіб аналізу експлойтів, оскільки дозволяє виявляти та виправляти вразливості ще до того, як зловмисники можуть їх використати для атаки.

Під час моніторингу вразливостей зазвичай використовуються спеціалізовані програми, такі як сканери вразливостей, що сканують системи на наявність вразливостей та звітують про їх наявність. Сканери використовують бази даних вразливостей для порівняння знайдених проблем зі списком відомих вразливостей. Аналіз експлойтів, як правило, містить наступні кроки:

- Сканування систем на вразливості з використанням сканерів вразливостей. Формує звіти про сканування та визначає вразливості, які необхідно виправити;
- Аналіз знайдених вразливостей, що дозволяє з'ясувати, які з них можуть бути використані для атаки та яким чином;
- Виправлення вразливостей дозволяє зменшити ризик атаки. Виправлення вразливостей, також, можна проводити шляхом встановлення оновлень, видалення або відключення непотрібних компонентів, використання захисних ПЗ та інших способів;
- Повторне сканування, дозволяє переконатися, що знайдені вразливості були виправлені та усунути передумови для появи інших, нових вразливостей.

Також можна використовувати автоматизовані інструменти для моніторингу вразливостей, які дозволяють проводити сканування систем на вразливості автоматично та безперервно. Такі інструменти можуть надсилати сповіщення про виявлення вразливостей та допомагають в управлінні процесом виправлення знайдених проблем.

Аналіз трафіку – є корисним методом аналізу експлойтів, так як трафік включає в себе інформацію про те, якими програмами використовується мережа, які порти відкриті, яка інформація передається та інше [20]. Ці дані використовуються для виявлення зловмисних атак, а також для аналізу

експлойтів. Для аналізу трафіку зазвичай використовуються програми, які збирають дані про трафік і аналізують його з точки зору безпеки. Наприклад, програма Wireshark є потужним інструментом для аналізу трафіку, який може допомогти виявити вразливості та атаки на систему.

Аналіз журналів подій - забезпечує виявлення незвичайної активності або спроб атак на систему [20]. Журнали подій - це записи, які створюються системою під час виникнення подій, таких як вхід в систему, зміна конфігурації, запуск програми та інші. Журнали подій містять значну кількість інформації про те, що відбувається в системі та можуть допомогти виявити зловмисну та/або недекларовану діяльність. Для аналізу журналів подій, зазвичай, використовуються спеціальне ПЗ, таке як Windows Event Viewer, ELK Stack, або Splunk, що збирають та аналізують дані про події в ОС. Ці програми можуть допомогти виявити незвичайну або підозрілу діяльність в ОС, яка може свідчити про наявність проблем, котрі є наслідком роботи експлойтів.

Дослідження коду - надає уточнюючу інформацію про те, як саме атака виконується та допомагає завчасно встановити потрібні заходи безпеки. Як було зазначено вище, для дослідження коду експлойтів використовуюся різні методи, включаючи декомпіляцію, дизасемблювання та аналіз пам'яті. Декомпіляція полягає в перетворенні вихідного коду з мови високого рівня на мову низького рівня, щоб зрозуміти, як саме працює експлойт. Дизасемблювання полягає в перетворенні бінарного коду у більш зрозумілий вигляд, щоб дослідити дії, які виконує експлойт. Аналіз пам'яті виявляє ресурсозатратні дії, які виконує експлойт, та маркує процеси взаємодії експлойту з іншими процесами в системі. Дослідження коду може також допомогти виявити, як саме експлойт був впроваджений в систему, якщо він був скомпільований з вихідного коду. Наприклад, дослідження коду може продемонструвати, яким чином був скомпільований експлойт, які опції були використані та які залежності були встановлені тощо.

Однак, слід мати на увазі, що процес дослідження коду може бути важким завданням, особливо якщо експлойт складено спеціалістом високого рівня, який

використовував складний код та різні методи обфускації. Крім того, дослідження коду може вимагати великої кількості часу та знань зі сторони аналітиків з ІБ. Не всі фахівці можуть мати необхідні навички та досвід для розуміння складного коду експлойту, тому може виникнути необхідність залучати експертів з цієї галузі. Крім того, дослідження коду може вимагати відповідних програмних інструментів й обладнання, таких як дизасемблери, декомпілятори, дебагери та інші, що є додатковою витратою для організації, яка має намір або вже проводить аналіз експлойтів. Також, процес дослідження коду експлойтів може бути обмеженим, якщо експлойт використовує вразливість, яка вже добре відомою та є вивченою [2]. У такому випадку може бути більш ефективним використання інших методів, таких як моніторинг мережі та системних журналів, для виявлення та запобігання можливим атакам.

Всі ці методи і засоби можуть використовуватись, як окремо, так і в поєднанні для більш детального аналізу експлойтів та вдосконалення існуючих стратегій й методик для покращення протидії новим зразкам експлойтів.

3. 2 Внутрішня побудова та сутність функціонування експлойтів

Внутрішня побудова експлойтів може бути досить складною і варіюватися в залежності від цілей та вразливостей, які в них використовуються [2, 17]. Проте, основні компоненти більшості відомих експлойтів залишаються незмінними. Зловмисний код є основною частиною експлойту, який використовує вразливість, щоб отримати доступ до системи або даних. Цей код може бути написаний на різних мовах програмування, найчастіше це Java/Java Script або C/C++, залежно від вразливості та системи (устаткування), яку має намір атакувати зловмисник.

Наступна частина експлойту – це спосіб взаємодії (адаптер) з вразливістю шляхом використання спеціально створеного коду або відповідної техніки (*послідовності маніпуляцій*), які використовують «слабкі» місця в ПЗ або конфігурації цільової системи та/або пристрою [21]. Наприклад, експлойти можуть впроваджувати шкідливий код в систему, використовуючи вразливість.

Це можна зробити, наприклад, шляхом переповнення буферу, введення коду або виконання команд на віддалених системах тощо. Іншим прикладом є використання недостовірних або некоректних даних, завдяки яким експлойт може порушити роботу (зламати) або обійти контроль безпеки вразливої системи. Також, експлойт може використовувати вразливість для маніпулювання *(тобто прихованого здійснення нештатної послідовності дій/процедур)* системними ресурсами, такими як пам'ять, файлова система або мережеві з'єднання. Це може призводити до зміни конфігурації системи, витоку інформації або порушення нормального функціонування системи. Крім того, експлуатована вразливість може бути використана для підвищення привілеїв доступу та реалізації цілої послідовності НСД, які недоступні звичайному користувачеві (наприклад, зміну конфігурації мережевого устаткування та/або параметрів маршрутизації трафіку [14]).

Ще однією важливою частиною експлойту є інструменти для подолання та/або обходу захисту систем безпеки, таких як фаєрволи [14], антивірусні програми тощо. Це може бути код, який змінює значення певних параметрів, щоб обійти захист, або код, який виконується від імені користувача з високими привілеями, щоб отримати доступ до системи. Завдяки уразливостям нульового дня (*zero-day*) [2], експлойти можуть довго існувати і обходити захист вразливих систем. Також експлойти можуть використовувати недостатньо захищені мережеві підключення, такі як відкриті Wi-Fi мережі або недостатньо захищені VPN-з'єднання [14], для злому системи.

Після того, як експлойт успішно використав вразливість та отримав доступ до системи-жертви, зловмисники можуть встановлювати додатковий зловмисний код (*т.з. корисне навантаження*) для контролю над скомпрометованою системою. Цей код розширює функціональні можливості зловмисникам та надавати йому доступ до файлів і конфіденційної інформації, створювати нові облікові записи та/або знищувати/шифрувати дані .

Інші можливі складові експлойтів можуть включати шифрування та/чи обфускацію коду. Тобто код експлойту може бути зашифрований або

перетворений за допомогою різних технік обфускації (наприклад, фрагментація коду, зміна коду, сеансовий поліморфізм та/або вбудовування в незловмисний код тощо), що робить його важчим для виявлення та наступного аналізу [21].

Також, замість або в доповнення до технічних методів атак, зловмисники можуть використовувати атаки соціальної інженерії (SE), щоб отримати доступ до системи. Ці техніки можуть одночасно поєднувати *Site parsing, Sniffing, Vishing, Phishing, Spoofing*, різні різновиди *DDoS* тощо [15]. Наприклад, вони можуть переконати користувача цільової системи надіслати їм свій пароль або відкрити заразливий документ. Відомі кілька векторів атаки, з яких зловмисники можуть вибрати. Одним із них є використання SE-атак та заманювання потенційних жертв на шкідливий веб-сайт, який містить заздалегідь підготовлений набір експлойтів. У цьому сценарії набір експлойтів непомітно сканує цільовий пристрій на наявність будь-яких невиправлених вразливостей і застосовує відразу кілька експлойтів. При цьому, кожний експлойт може бути націлений на будь-яку конкретну вразливість або навіть на кілька вразливостей одночасно, та може бути реалізовано у формі фрагмента коду або набору спеціально створених інструкцій.

Характерна атака з використанням експлойтів зазвичай відбувається наступним чином (див. Рис 3.1)[2, 15, 21]:

- Пошук вразливостей – зловмисники шукають у доступному коді або експериментують із популярними програмами та апаратними засобами, шукаючи вразливості. Вони також можуть купувати вразливості на відповідних ресурсах (докладніше про *zero-day* буде розглянуто нижче);
- Синтез коду експлойту – зловмисники створюють шкідливу програму або інші технічні засоби (базис) для використання вразливості;

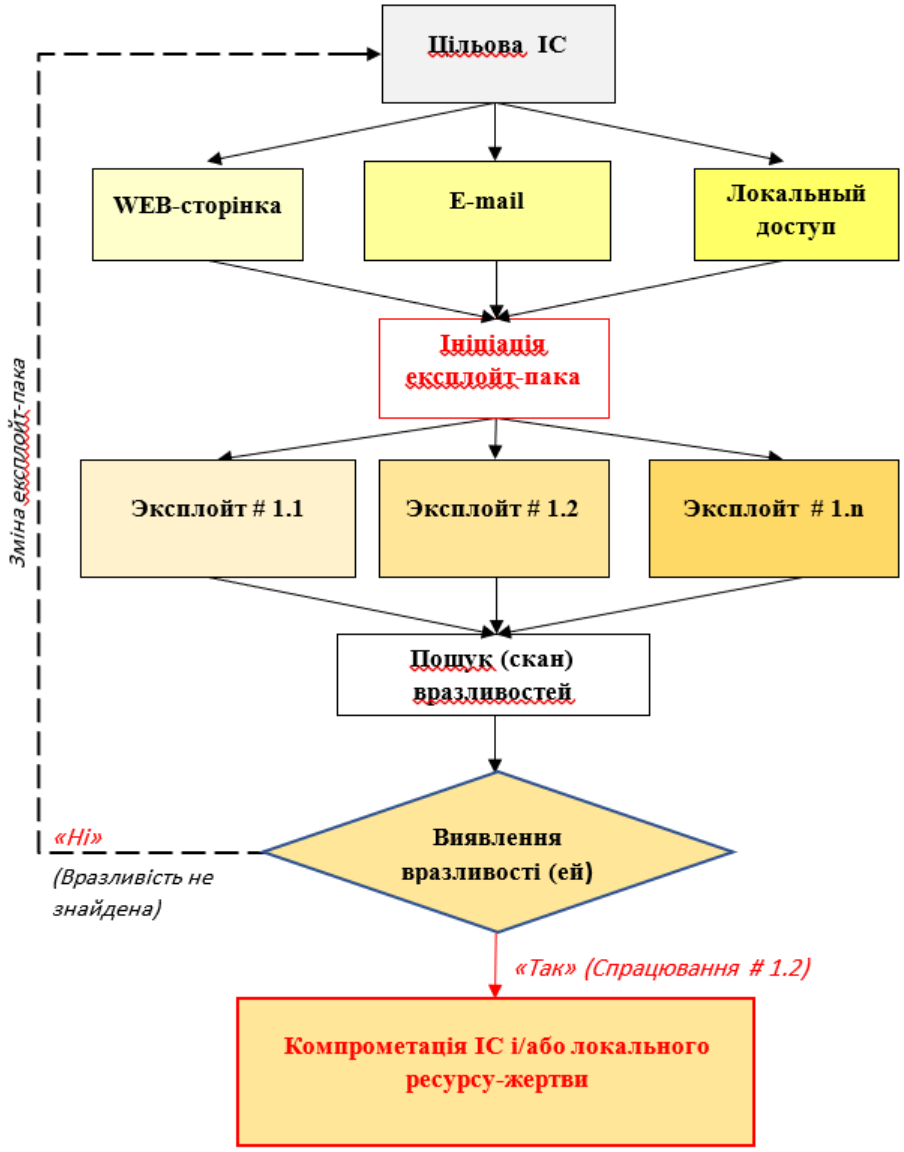


Рис. 3.1 - Принцип роботи експлойт-паку в цільовій ІС

- Пошук цільових систем й вразливого устаткування – зловмисники можуть використовувати ботів, автоматичні сканери та інші засоби для ідентифікації систем та/або пристроїв, які мають потрібні уразливості;
- Планування атаки – під час цілеспрямованої атаки на певну організацію/ресурс зловмисники можуть провести детальну попередню розвідку з використанням всіх можливих векторів атак [9, 14], щоб визначити найкращий спосіб проникнення в уразливу систему. Під час нецільової атаки (т.з. полювання) зловмисники зазвичай використовують ботів або масові фішингові кампанії, щоб спробувати проникнути в якомога більше вразливих систем;

- Проникнення – зловмисник обходить або деактивує захисні інструменти/функції периметра безпеки організації або персонального пристрою жертви;
- Ініціація експлойту нульового дня – забезпечує можливість віддалено виконувати код в скомпрометованій системі/пристрої.

Створювані набори (збірки) експлойтів здатні отримувати широкий діапазон інформації про пристрій, наприклад використовувані плагіни браузера, встановлено ПЗ та навіть ОС, запущену на пристрої [21]. Ці набори (кіт-набори) невпинно перевіряють усі компоненти цільового пристрою в пошуках уразливості для використання. Як тільки вони знаходять вразливість для зламу, вони можуть легко розгорнути зловмисне ПЗ локально на «слабкому» цільовому пристрої та/або ОС.

Ще один відомий спосіб (стратегія) здійснити атаку з використанням експлойту – розповсюдити код по мережі. Завдання коду теж саме – шукати вразливі місця системи (наприклад, такі як уразливості EternalBlue і BlueKeep) [15]. В цьому разі вони працюють повністю автономно, тобто не потрібна взаємодія з користувачем взагалі. Переваги цього вектора атаки для зловмисників досить прості – це дуже ефективний спосіб розвитку та розширення ботнетів [14] у рамках підготовки до більш масштабної розподіленої атаки, наприклад типу «відмова в обслуговуванні» проти мобільних або веб-додатків. Одним з таких ботнетів є відомий Mirai [22].

На жаль, основними кандидатами на атаки експлойтів є такі популярні системи, як Java, Adobe Flash Player, MS Silverlight і Runtime Environment. Іншою мішенню для кіт-наборів експлойтів є будь-яке застаріле ПЗ. Хоча постійні оновлення ПЗ і здаються «неприємними», вони, як правило, спрямовані на усунення існуючих недоробок у безпеці, тому ніколи не слід ігнорувати важливість їх встановлення [2, 17].

Після створення експлойту зловмисникам потрібно приховати його таким чином, щоб користувачі, навмисно (SE-атака) або випадково відвідавши певний

веб-сайт, та/або необачно запустили на виконання запропонований ним файл, автоматично інфікувалися, не підозрюючи нічого. Зловмисники використовують різні підходи для досягнення цієї мети, ось кілька прикладів:

1) Використання спаму: - зловмисники розсилають спамові повідомлення, що містять посилання на зловісний веб-сайт. Ці повідомлення намагаються привернути увагу та залучити користувачів до переходу на сайт, часто за допомогою підроблення DNS-імен або застосування SE [9, 13, 14].

2) Створення заражених сайтів: - зловмисники створюють багато заражених веб-сайтів з назвами, що нагадують легітимні. Вони можуть зареєструвати доменні імена, що мають непомітні відмінності у написанні від популярних сайтів (наприклад, *microsooft.com* замість *microsoft.com*) для введення необачних користувачів в оману.

3) Компрометація веб-сайтів легітимних компаній: - зловмисники зламують веб-сайти, що належать реально існуючим компаніям, і впроваджують шкідливий код до того, як власник сайту виявить та заблокує цю підміну та/або модифікацію контенту [23].

4) Впровадження пасток у посилання на файли, що розміщуються на сайтах соціальних мереж та ін., які вказують на зовнішній код, що використовує вразливості у сторонніх модулях, необхідних для виконання цього зловмисного коду.

Безвідносно підходів до реалізації атаки з експлойтами, зловмисники обов’язково виконують маскування основного «тіла» програмного коду експлойту за допомогою наступних методів [21, 23, 24]:

- Обфускація: - що перетворює експлойт у важкозрозумілий і заплутаний код. Це робить важким аналіз і виявлення шкідливого змісту;
- Використання шифрування - щоб уникнути виявлення та ідентифікації. При виконанні експлойту шифрований код розшифровується і виконується в пам'яті, що ускладнює виявлення атаки;

- Впровадження технології поліморфізму - забезпечує зміну структури та/або властивостей експлойту при кожному циклі виконанні. Т.ч. зловмисники можуть генерувати різні варіації експлойту, що унеможливлює його виявлення на основі сигнатур антивірусних програм та іноді навіть IDS [14];
- Впровадження інструментів/технік анти-аналізу: - протидіють й ускладнюють аналіз коду, наприклад такі як, виявлення віртуальних середовищ тощо. Спрямовано на ускладнення аналізу експлойту в дослідницькій лабораторії при спробах отримати його опис та зрозуміти принцип дії;

Усі ці методи спрямовані на унеможливлення виявлення експлойту та збереження його функціональності, щоб зловмисники могли успішно інфікувати системи без виявлення.

Подібно до експлойтів і зловмисного ПЗ, експлойти та вразливості виявляються тісно пов’язаними, але хоча вони і пов’язані між собою, проте не є одним і тим же. Вразливість – це «слабке» місце або помилка програмного коду, якими можна зловживати для «доставки» зловмисного корисного навантаження в цільову комп’ютерну систему/пристрій [21]. Однак не всі вразливості можна використати – навіть якщо вразливість ще не виправлено, так як вона (вразливість) може бути заблокована іншими засобами/системами безпеки. В обчислювальній техніці експлойт зазвичай відноситься до атаки, яка використовує відому вразливість, щоб викликати несподівані наслідки в цільовій системі через доставку зловмисного ПЗ або підвищення діючих привілеїв атакуючого. При цьому існування вразливості не обов’язково означає безпосередню небезпеку, рівно до того часу, поки для неї не буде створено відповідний експлойт, що буде експлуатувати цю вразливість, і тому, в цілому, немає аж ніяких сумнівів, що це рано чи пізно, але все одно станеться.

3. 3 Аналіз відомих різновидів експлойтів

Час від часу в ПЗ та мережевому устаткуванні сучасних ІС виявляються нові вразливості. Ці вразливості являють собою умовні «потайні канали» в контурі безпеки ПЗ та обладнання, які дозволяють зловмисникам на 1-му етапі,

отримати несанкціонований доступ до них, а згодом (відповідно до свого задуму) пошкодити або скомпрометувати. Відомі вразливості задокументовані в публічних базах даних, таких як Національна база даних уразливостей (NVD). Як постачальники ПЗ, так і незалежні дослідники ІБ постійно шукають нові вразливості в нових та діючих програмних продуктах. Станом на сьогоднішній день, відомі 2 основних класи експлойтів: - т.з. *N-day* експлойти та експлойти нульового дня (або інакше *zero-day*, зеродеї) [2].

Експлойт нульового дня – це варіант реалізації загрози безпеки при якому зловмисник використовує вразливість нульового дня для атаки на систему [23]. Ці експлойти особливо небезпечні, тому що вони з більшою ймовірністю будуть успішними, ніж атаки на встановлені/відомі вразливості. В цьому разі у т.з. «нульовий день, коли вразливість вже оприлюднена, а інструментів щодо її виправлення поки ще не існує, є всі передумови для «успішної» реалізації відповідних атак з використанням *zero-day* експлойту.

Те, що робить експлойти нульового дня ще більш небезпечними, полягає в тому, що деякі активні групи кіберзлочинців використовують *zero-day* для здійснення планових багатошарових й багатоступеневих атак. Ці групи заздалегідь навмисно «резервують» потрібні їм *zero-day* для використання з певними цілями і проти конкретних (таргетованих) жертв, наприклад - атака на фінансові установи або конкретний зразок ПЗ та/чи обладнання тощо [21]. Така стратегія дій атакуючої сторони суттєво зменшує ймовірність того, що вразливість (або одразу декілька вразливостей у разі ЕК) буде виявлена жертвою атаки, що в свою чергу, збільшує тривалість життя експлойту (-тів). В даному випадку, навіть після розробки виправлення користувачі все одно повинні оновлювати свої системи, і якщо вони цього не зроблять, то зловмисники можуть з «успіхом» продовжувати користуватися цим або іншим *zero-day* експлойтом (зі складу ЕК), доки атаковану систему не буде виправлено в повному обсязі. Таким чином, атака нульового дня, це вразливість ПЗ, яку зловмисники використовують до того, як про це дізнається розробник цього ПЗ. Вочевидь, що

на цей момент (*zero-day*) виправлення не існує, тому зловмисники можуть відносно легко експлуатувати цю вразливість, знаючи, що захисту від неї практично немає. Тобто цю загрозу можна лише декілька нівелювати за рахунок правильних налаштувань в роботі наявних засобів проактивного захисту [14], що є дуже серйозною загрозою безпеці.

Коли зловмисники виявляють вразливість нульового дня, їм потрібен відповідний механізм гарантованої доставки зловмисного програмного коду до вразливої системи. У багатьох випадках механізмом доставки виступає, наприклад електронний лист або інше повідомлення, яке нібито надійшло від відомого чи законного кореспондента, але насправді від зловмисника. Таке повідомлення намагається переконати (SE атака) користувача виконати потрібну дію, наприклад відкрити файл або відвідати шкідливий веб-сайт, т.ч. активуючи цільовий експлойт.

Зловмисники, які здійснюють атаки нульового дня, належати до кількох категорій [24-25]:

Кіберзлочинці – хакери, основним мотивом яких є фінансова діяльність.

Хактивісти – нападники, котрі мотивовані певною ідеологією, тому вони зазвичай хочуть, щоб атаки були помітними.

Корпоративне шпигунство – зловмисники, які мають на меті незаконне отримання приватної (чутливої) інформації від інших організацій.

Кібервійна – реалізація певних дій, с залученням відповідних спеціалістів, в межах котрих національні держави та/або органи національної безпеки та окремі підрозділи приватних компаній й організацій, вдаються до кіберзагроз проти інфраструктури іншої країни або організацій в іншій країні, які представляють критичну інфраструктуру (наприклад, атака Stuxnet).

Цільові *zero-day* атаки можуть бути спрямовані на конкретні компанії і установи, урядові структури, критичну інфраструктуру *(енергетичні системи, телекомунікаційні мережі, транспортні системи тощо)*, або індивідуальних користувачів та дослідників безпеки, з метою викрадення конфіденційної

інформації й отримання несанкціонованого доступу і виведення з ладу відповідних систем та ресурсів [25].

Нецільові (розосереджені) атаки нульового дня зазвичай здійснюються проти великої кількості приватних або бізнес-користувачів, які використовують вразливу систему чи устаткування (наприклад ОС або маршрутизатор з вразливістю). Часто метою зловмисника є скомпрометувати ці системи та використовувати їх для створення масштабних ботнетів. Нещодавнім прикладом цього вектобру подій є атака WannaCry, яка використовувала експлойт EternalBlue у файловому протоколі Windows SMB [25].

На противагу *zero-day*, експлуатація вже відомих вразливостей (*N-day)*, нажаль, є набагато більш масштабною проблемою безпеки для багатьох сучасних організацій. *N-day* експлойт - це вразливість, яка вже відома і більш того, для неї вже доступне відповідне виправлення. Тобто після публікації патчу безпеки та CVE (від англ. *Common Vulnerabilities and Exposures*), експлойт *zero-day* стає *N-day* експлойтом (див. Рис.3.2) [2, 5, 11].

[2]Теоретично, «застарілі» експлойти не повинні були б загрожувати безпеці пристроїв та ПЗ, проте вони, нажаль, продовжують використовуватися для атак і продовжують набирати популярності. Певною мірою це зумовлено тим, що зловмисники можуть дізнаватися про подробиці існуючих вразливість все, що їм потрібно, шукаючи відповідні виправлення (*т.з. «бінарне порівняння»*), або переглядаючи загальнодоступні документи на наявність активних експлойтів. Також є можливість, що постачальники ПЗ та/або мережевого обладнання, не надають оновлення безпеки для своїх попередніх рішень, навіть якщо вони випускають відповідне виправлення ПЗ, або ж самі користувачі не встановлюють своєчасно патчі безпеки. Прикладом може бути відомий *N-day* експлойт *«EternalBlue»*, який був досить активним (як інструмент для здійснення атак), навіть через три роки після випуску відповідного патчу безпеки (з 2017 по 2020 рр.). Серед іншого, він був використаний програмою-вимагачем WannaCry, а за даними Shodan, понад 650000 підключених до Інтернету пристроїв все ще залишаються вразливими для нього. [2]

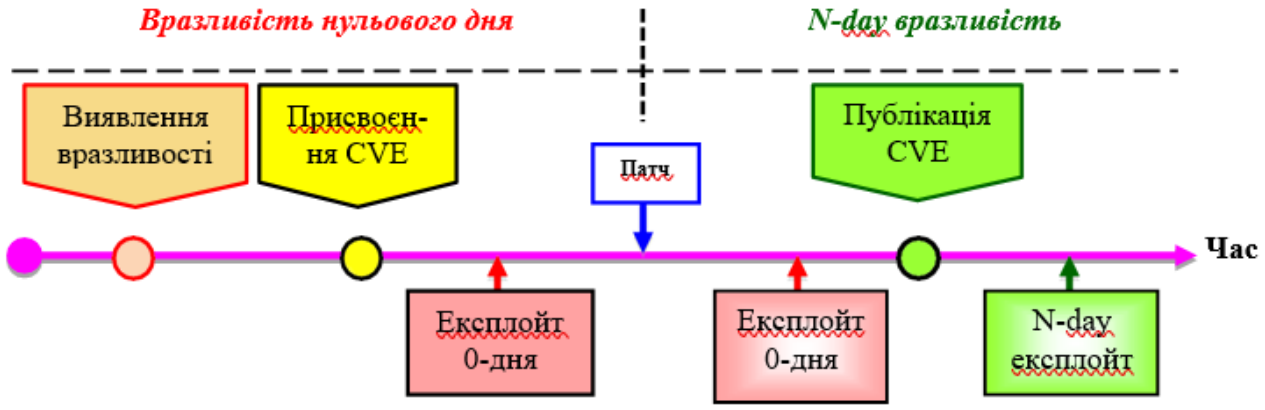


Рис. 3.2 – Алгоритм реагування на вразливості та публікації експлойтів

[2]Залежно від способу отримання доступу до вразливого ПЗ, існуючи експлойти умовно поділяються на віддалені (*англ. remote*), локальні (*local*) та експлойти підставного серверу [2].

[2]Віддалений експлойт, використовуючи вразливість без попереднього доступу до вразливої системи (пристрою), дозволяє зловмиснику отримати доступ до неї через мережу. В залежності від того, який сервіс експлуатується, атакуючий отримує права користувача або *root* на сервері, що атакується. Після того, як зловмисник сканує сервер на наявність будь-яких відомих локальних експлойтів, якщо такі знаходяться, він використовує їх для отримання root-доступу на сервері. В разі, коли зловмисник отримує root-доступ, то він може встановити руткіти (та/або бекдори), які дозволять йому несанкціоновано увійти в скомпрометовану їм систему, та почати «працювати» на цільовому сервері без загрози його відс теження з боку адміністратора та/або інших користувачів. Найбільш поширеними різновидами віддалених експлойтів є переповнення буферу (використання вразливості CVE-2015-0311, тобто переповнення буфера *Adobe Flash Player*, яка дозволяє зловмисникам віддалено вико- нувати довільний код через невідомі вектори атак) та інші атаки з неперевіреним введенням. Вони виконуються або для загальнодоступних служб (таких, як *HTTP* та *FTP*), або під час входу до захищених служб (*таких, як POP та IMAP*) [2].

Локальний експлойт — це тип експлойта, який використовує вразливість або слабкість у локальній системі чи пристрої [21]. Зазвичай він порушує безпеку системи зсередини, використовуючи недоліки програмного забезпечення або конфігурації. На відміну від віддалених атак на системи через мережу, локальні експлойти вимагають прямого доступу до цільового пристрою чи системи. Він може бути виконаний зловмисником, який має фізичний доступ до машини, або користувачем із підвищеними привілеями в локальній системі. Локальні вразливості можна використовувати для отримання неавторизованого доступу, підвищення привілеїв, виконання шкідливого коду або маніпулювання конфігураціями пристрою чи системи. Вони часто розробляються дослідниками безпеки для виявлення вразливостей і підвищення безпеки системи.

[2]Експлойти підставного серверу - це вразливість по відношенню до існуючих клієнтських додатків, що зазвичай включають змінені сервери, які розсилають експлойти при отриманні доступу до клієнтського додатку. Ця вразливість з «успіхом» працює в парі із SE атаками, наприклад: - фішинг та ланч-фішинг (*для розповсюдження рекламного ПЗ*) [2].

Відомі експлойти можна класифікувати за різними ознаками, такими як:

- Тип вразливості: деякі експлойти використовують певні типи вразливостей, наприклад, переповнення буфера, SQL-ін'єкції, Cross-Site Scripting (XSS) та інші;
- Платформа: експлойти можуть бути специфічними (таргетовані) для певної цільової платформи, наприклад: ОС або веб-серверу;
- Призначення: експлойти можуть мати різні цілі, такі як отримання доступу до системи, виконання коду на вразливій машині, зміна налаштувань системи та інші;
- Метод виконання: деякі експлойти потребують безпосереднього фізичного доступу до цільових ПК та/або мережі, тоді як інші можуть бути виконані з віддаленого місця;

- Рівень доступу: деякі експлойти вимагають адміністративних привілеїв для їх виконання, тоді як інші можуть бути виконані з обмеженими привілеями для їх «користувача»;
- Комплексність: експлойти можуть бути як відносно простими, так і дуже складними та вимагати «розуміння» специфіки роботи ПЗ та/чи наявних вразливостей.

4 УЗАГАЛЬНЕННЯ МОЖЛИВОСТЕЙ ВИКОРИСТАННЯ ЕКСПЛОЙТІВ ДЛЯ ЦІЛЕЙ ПОПЕРЕДЖЕННЯ АТАК НА ІНФОРМАЦІЙНІ РЕСУРСИ

Розробники антивірусної індустрії особливо усвідомлюють складності сучасних кібератак і прагнуть забезпечити комплексний захист своїх продуктів, умовно відтворюючи відповідні «програмний комплекс із забезпечення ІБ» на стороні клієнта. На жаль, розвиток так званої "Advanced Persistent Trouble" (APT) тепер загрожує і кінцевим користувачам [26]. І, як показала практика, реалізація будь-якої техніки, навіть невідомої зараз, для атаки на цільової ІС починається саме з експлуатації вразливості «нульового дня». Отже, у цьому сенсі слід мати на увазі, що:

По-перше, антивірусні програми можуть мати *zero-day* вразливість. При цьому людський фактор є і в розробці будь-якого серйозного продукту, а це означає, що всі відповідні загрози притаманні антивірусу та другому захисному програмному забезпеченню.

По-друге, ідея реалізації краудсорсингу (*краудсорсинг – рішення складної задачі необмеженим кругом осіб*) в антивірусній індустрії, веде за собою супутні наслідки: - проблеми передачі даних в «хмари» від кожного клієнта; - оцінки репутаційної системи тощо. Наприклад, тенденція довіряти інформації відносно підозрілих файлів, яку розсилають (а в деяких продуктах і самостійно оцінюють) користувачі, може мати серйозні наслідки для розробників ПЗ.

Тому, для звичайних користувачів слід виконувати наступні дії, щоб зменшити ймовірність атак з використанням експлойтів [15, 21, 23 – 25]:

- Регулярно оновлювати всі програмні додатки, що використовуються, в тому числі ОС, браузер та антивірусні програми. Оновлення включають в себе виправлення вразливостей, що можуть бути використані для атаки;

- Використовувати мережеві засоби міжмережевого захисту (брандмауери), які можуть заблокувати певну кількість атак, включаючи ті, що використовують експлойти;
- Не відкривати та/чи запускати на виконання підозрілі файли та посилання, які приходять від невідомих або недовірених джерел;
- Для захисту від атак, які використовують перехоплення трафіку, слід використовувати VPN або інші захисти, які шифрують трафік;
- Постійно навчитися впізнавати підозрілі повідомлення, веб-сайти та інші елементи, які можуть приховувати шкідливе ПЗ;
- Використовувати складні паролі, які складаються з комбінації букв, цифр та символів. Це зробить систему менш вразливою до атак «перебором» (*брутфорс*), котрі використовують експлойти.

Також слід використовувати та всіляко впроваджувати, деякі інші, додаткові заходи, які можуть захистити від впливу експлойтів:

- вимкнути автовідтворення медіа в налаштуваннях інтернет браузерів, щоб уникнути проникнення експлойтів, які використовують відповідні вразливості через механізм автовідтворення медіа контенту;

- намагатися використовувати ПЗ з блокування реклами, так як деякі експлойти використовують рекламні банери, щоб провести атаку;

- регулярно проводити резервне копіювання даних.

При цьому, для спеціалістів з ІБ, котрі проводять дослідження та тести на проникнення в ІС (петнестерів), постають зовсім інші проблеми, які обумовлені існуванням експлойтів. В даному випадку, одна з головних проблем – це проблема визначення пріоритетності вразливостей, тобто в визначенні, які з них потрібно перевіряти та вирішувати в першу чергу [17]. Цей процес є досить суб’єктивним, та залежить від профільного досвіду експертів. Основними факторами, які впливають на встановлення пріоритетів, є наступні:

1) Важливість вразливостей: Оцінюється потенційний вплив вразливостей на систему та дані, що обробляються. Вразливості, які можуть

призвести до серйозних наслідків(на думку експерта), таких як втрата конфіденційності, цілісності або доступності, мають вищий пріоритет [2].

2) Ймовірність використання: Оцінюється ймовірність відповідної атаки з боку зловмисників. Вразливості, що можуть бути використані безпосередньо та з найменшими зусиллями, мають вищий пріоритет [2].

3) Розповсюдженість: Оцінюється, наскільки поширена вразливість у системах і якщо вразливість є широко поширеною, то вона може мати вищий пріоритет, оскільки зловмисники вже можуть бути знайомі з нею та використовувати її [2].

4) Складність використання: Оцінюється складність розробки й використання експлойту для вразливості. Вразливості, що вимагають складних технік або розробки складного коду, можуть мати нижчий пріоритет, оскільки їх використання вимагатиме більше зусиль.

5) Доступність наявних заходів захисту: Оцінюється, наскільки доступні та ефективні існуючи заходи захисту від певної вразливості. Якщо існують ефективні засоби для запобігання цієї вразливості, то вона має нижчий пріоритет.

Пінтестери повинні аналізувати всі ці фактори та враховувати ризики і контекст системи (критичність до компрометації), щоб визначити пріоритети у вирішенні вразливостей та виконанні тестування експлойтів.

Організація системи ІБ повинна втілювати комплексний підхід, що включає в себе різноманітні заходи та технології для захисту від різних типів загроз, включаючи експлойти. В цьому контексті слід виділити три етапи реагування на проблематику експлуатації вразливостей [27]:

1) Превентивний - комплекс дій щодо усунення вразливостей перед входом до публічних мережевих (тобто не довірених) просторів;

2) Профілактичний - на протязі всього існування сервісу проводиться серія перевірок, тестів та аудиту безпеки з метою завчасного виявлення вразливостей.

3) Реактивний - команда експертів реагує та вивчає всі дії та наслідки, стосовно виявлених вразливостей (*інцидентів*) і швидко випускає (встановлює) відповідні виправлення (патчі) оновлень для усунення цієї проблеми.

У сучасному кіберпросторі існує велика різноманітність та динамічність кіберзагроз. Тому базові захисні засоби вже недостатні для побудови повністю захищеної інфраструктури, особливо з урахуванням вразливостей нульового дня [23]. Щоб ефективно протидіяти цим загрозам, необхідно вживати профілактичних заходів та підходів, що дозволяють завчасно виявляти спроби підготовки та проведення атак, а також зменшувати можливості атакуючого, щодо їх «успішного» завершення. Успіх протидії полягає у ретельному аналізі даних, пошуку значущих подій, виявленні інцидентів та їх розслідуванні. Це дозволяє відповідальним особам, таким як розробники та спеціалісти з ІБ, завчасно виправляти вразливості та захищати власні інформаційні ресурси.

У випадку *zero-day* найбільш ефективні є системи та інструменти, які здатні комплексно аналізувати поведінку атакуючої сторони (*проактивні засоби безпеки - IDS, Honeypot, брандмауери рівня Next Generation (NGFW), XDR платформи тощо*), виявляти ланцюжки атак та аномалії трафіку у корпоративній інфраструктурі [28, 29]. Слід зауважити, що *Deception*-технології є ефективним інструментом у таких випадках [28]. Вони спрямовані на приманювання зловмисників до вчинення демонстративних дій, використовуючи звичайні людські слабкості, які є характерними для хакерів будь-якого рівня кваліфікації.

Щодо регламентів та тренування дій на «імітаторах інцидентів», то їх головна перевага полягає в розірванні непередбачуваності та неочевидності, які часто супроводжують вразливість саме нульового дня. Хоча неможливо змоделювати алгоритм дій для кожної конкретної ситуації, проте тренування допомагає знизити ризик помилок, як для користувачів, так і персоналу з ІБ.

Коротко розглянемо організацію системи ІБ проти експлойтів нульового дня, як головної загрози безпеки з точки зору можливих наслідків, масштабів та термінів існування/реалізації відповідних атак.

4.1 Особливості превентивного захисту від експлойтів

Забезпечення превентивного захисту починається з розуміння того, що жоден цифровий продукт не може бути повністю безпечним. Існує завжди певний ризик вразливостей, особливо в компаніях, які використовують багато різних сервісів. Кожен додаток або сервіс може мати потенційні вразливості нульового дня, що створює великі ризики для безпеки.

Превентивна боротьба з експлойтами спрямована на попередження використання вразливостей та захист системи від атак [30]. Основною метою є зниження ймовірності успішного використання експлойтів шляхом виявлення, усунення та запобігання вразливостям. Це означає активне виявлення і патчінг вразливостей у програмному забезпеченні, встановлення захисних механізмів, які утруднюють експлуатацію вразливостей, і практикування кращих методів безпеки.

Превентивний захист також включає усвідомлення ризиків та навчання персоналу компанії щодо безпекових практик. Це може включати навчання про соціальну інженерію, своєчасне оновлення паролів і застосування багаторівневої аутентифікації.

Основні підходи до превентивної протидії з експлойтами включають [27, 30]:

1) Правильне планування та проектування системи: Забезпечення безпеки повинно бути враховано на початкових етапах проектування системи. Це означає врахування найкращих практик безпеки, вибір безпечних технологій та архітектурних рішень.

2) Використання безпечних програмних рішень: Розробники повинні дотримуватись безпечних програмувальних практик, використовувати безпечні функції та бібліотеки. Це включає перевірку введення даних, управління пам'яттю, обробку помилок та інші аспекти, що можуть запобігти вразливостям.

3) Захист периметра: Використання файрволів, веб-фільтрації, інтрузійного виявлення та запобігання може допомогти уникнути вразливостей, обмежити доступ до системи та виявляти потенційно шкідливий трафік.

4) Система контролю доступу: Встановлення і правильна конфігурація системи контролю доступу може забезпечити обмеження прав доступу до системи, що ускладнює можливість використання експлойтів.

5) Навчання та освіта: Підвищення рівня свідомості користувачів та персоналу про загрози безпеці та навчання їх безпечному поводженню в мережі може допомогти уникнути атак, які використовують експлойти.

Найважливішим засобом боротьби з вразливістями нульового дня та іншими проблемами інформаційної безпеки є впровадження практик безпечного життєвого циклу розробки програмного забезпечення (SSDLC-підхід).

SSDLC (Secure Software Development Lifecycle) - це підхід, який використовується для розробки безпечного програмного забезпечення та боротьби з експлойтами [31]. Основною метою SSDLC є виявлення, усунення та запобігання вразливостям на ранніх етапах розробки програмного продукту. Він включає в себе наступні етапи:

- Аналіз ризиків: Здійснюється аналіз потенційних загроз безпеці, включаючи ідентифікацію вразливостей та потенційних експлойтів. В результаті визначаються пріоритети заходів безпеки.
- Проектування безпеки: На цьому етапі виконується проектування системи з урахуванням заходів безпеки. Це включає в себе вибір безпечних архітектурних рішень, використання безпечних протоколів та алгоритмів, врахування механізмів аутентифікації та авторизації, та інші заходи.
- Реалізація та кодування: Розробники дотримуються безпечних програмувальних практик, використовують безпечні функції та бібліотеки, здійснюють перевірку введення даних та обробку помилок.
- Тестування та верифікація: Проводяться безпечні тестування, включаючи тестування вразливостей та експлойтів, для перевірки системи на наявність слабких місць та забезпечення її безпеки.

- Випуск та підтримка: Після успішного завершення попередніх етапів, програмний продукт випускається, а після випуску здійснюється підтримка та моніторинг для виявлення та усунення нових вразливостей.

SSDLC допомагає забезпечити, що безпека вбудовується в кожен етап розробки програмного забезпечення, що сприяє запобіганню експлойтам та зменшенню вразливостей.

4.2 Узагальнення заходів з протидії загрозі застосування експлойтів

Профілактична складова з протидії впливу *zero-day* уразливостям, частково перетинається з превентивною складовою цих заходів. В цьому напрямку слід виділити наступні головні аспекти [15, 21, 27]:

- Регулярні оновлення та патчі: Важливо регулярно оновлювати ПЗ та ОС, встановлюючи всі доступні патчі безпеки. Це допомагає усунути виявлені вразливості та запобігти їх використанню.
- Багатовекторне тестування - передбачає регулярний внутрішній та зовнішній аудит безпеки і широке залучення пентестерів.
- Використання складних паролів автентифікації: Слід використовувати складні паролі для всіх передбачених етапів автентифікації облікових записів і забезпечувати їх регулярну зміну. «Складні» паролі зменшують ризик неавторизованого доступу до системи та можливість роботи експлойтів при реалізації модулю перебору.
- Безпека мережі: Впровадження та активна робота з засобами безпеки на рівні мережі (файрволів, віртуальних приватних мереж (VPN), мережевих моніторів тощо [14, 28, 29]), може допомогти уникнути атак, що використовують експлойти.
- Антивірусне ПЗ та захист від шкідливих програм: Встановлення та регулярне оновлення антивірусного ПЗ, що містять не сигнатурні модулі поведінкового моніторингу, частково допомагають виявляти та блокувати діяльність експлойтів.

- Використання безпечних програмних рішень: Перед використанням будь-якого ПЗ або додатків слід переконатися, що вони походять з надійних джерел і не містять вразливостей, які можуть бути використані експлойтами.
- Контроль доступу: Впровадження принципу найменших привілеїв користувачів та обмеження доступу до системи та/або приладу і мережевого устаткування для зниження ризику передумов НСД.
- Постійне підвищення рівня особистої обізнаності з питань ІБ: Підвищення рівня компетенцій користувачів/персоналу про загрози ІБ сприяє уникненню сценаріїв атак, які використовують експлойти.

До цих аспектів треба додати ще моніторинг «внутрішньої» поведінки процесів в пошуках можливих аномалій (*Internal Process Behavior Monitoring*). Це метод аналізу й відстеження активності мережевих процесів, з метою виявлення незвичайних або підозрілих дій (в т.ч. є елементом IPS [14]). Цей підхід передбачає постійний моніторинг активності процесів, включаючи їхній доступ до файлів, мережеву комунікацію, системні запити, споживання ресурсів та інші параметри. За допомогою спеціальних аналітичних алгоритмів та методів машинного навчання, моніторинг внутрішнього поведінки процесів може виявити аномалії, які вказують на можливі зловживання або кібератаку.

Штатна поведінка процесів визначається на основі накопичених даних та вивчених моделей (*поведінкових сигнатур*), що дозволяє виявити незвичайні відхилення в реальному часі. Це можуть бути незвичайні системні виклики, доступ до конфіденційних файлів, незрозуміла мережева активність, спроби підняття привілеїв або зміни конфігураційних параметрів.

Моніторинг внутрішнього поведінки процесів є важливою складовою кібербезпеки, оскільки дозволяє вчасно виявляти та реагувати на потенційно шкідливу або небезпечну активність всередині системи [20]. Цей підхід гармонічно доповнює класичні заходи безпеки, такі як антивірусне ПЗ та брандмауери, забезпечуючи додатковий рівень виявлення і захисту. Важливо не ігнорувати можливостей технології створення безпечного мережевого

середовища т.з. «пісочниці», що емулює інфраструктуру клієнта та допомагає перевірити, поведінку надісланих файлів.

4.3 Варіанти реагування на експлуатацію вразливостей класу zero-day

За результатами проведеного аналізу причин та наслідків експлуатації *zero-day* вразливостей, слід виділити наступні три аспекти [17, 24, 27]:

1) Проінформованість. Фахівці компанії повинні бути постійно інформованими про наявність 0-day вразливостей. Якщо вони не слідкують за останніми новинами або не отримують повідомлень від постачальника програмного забезпечення, то дані про такі вразливості можуть їх не досягти.

2) Управління патчами: Важливо розуміти, що перше випущене оновлення від постачальника може або закрити вразливість, або бути неефективним. Навіть може стати причиною появи нових проблем або збоїв у роботі системи. Ефективне управління патчами вимагає обережності та випробування перед впровадженням.

3) Готовність. Досвід реагування, що отримано під час тренінгів, чіткі регламенти та наявність необхідних інструментів є важливими складовими з протидії загрозам класу zero-day. Це допомагає фахівцям з ІБ мінімізувати потенційну шкоду та швидко реагувати на вразливості, які з'являються.

4) Ранжування пріоритетів вразливостей. Алгоритм присвоєння пріоритетності експлойтам повинен варіюватися в залежності від конкретної системи, організації та контексту даних що обробляються. При цьому, загальний алгоритм дій повинен використовувати наступні критерії для визначення пріоритетності експлойтів:

- Вразливість: Оцінюється ступінь небезпеки вразливості, включаючи потенційні наслідки її використання та можливий вплив на систему.
- Поширеність: Аналізується інформація, наскільки поширений або відомий експлойт, що детектовано. Чим більше систем піддаються ризику через дану вразливість, то тим вищий пріоритет слід бути наданий.

- Інформованість: Враховує ступінь інформованості профільних фахівців, щодо цього експлойту. Якщо є публічна інформація про експлойт і його використання, то це привід до вищого пріоритету.
- Вплив: Визначається потенційний вплив експлойту на конфіденційність, цілісність і доступність ІС. Експлойти, що можуть призвести до серйозних наслідків, повинні отримати вищий пріоритет.
- Наявність виправлень (патчів): Оцінюється наявність відповідного виправлення. Якщо виправлення вже існує або може бути швидко розроблене, то це може вплинути на пріоритетність експлойту.

Зважаючи на ці критерії, експерти з ІБ повинні встановлювати пріоритети для виправлення вразливостей та застосовувати відповідні заходи безпеки для зменшення рівнів потенційного ризику атаки zero-day експлойтів.

Реактивна парадигма протидії впливу експлойтів орієнтована на фактичне виявлення та реагування на вже реалізовані атаки. Тобто цей підхід спрямований на негайне реагування на атаки, запобігання їх поширенню та зменшення можливих наслідків. За рядом ознак та характерних властивостей [14] до засобів реактивного захисту від впливу експлойтів можна віднести наступні:

1) Системи виявлення вторгнень (IDS): IDS виявляють аномалії та підозрілу активність в мережі або системі. Вони відслідковують мережевий трафік та системні події з метою виявлення потенційних атак, включаючи використання експлойтів [20]. При виявленні підозрілого зловмисного активу IDS сповіщають про це адміністратора або ініціюють автоматичні заходи щодо припинення атаки.

2) Системи попередження вторгнень (IPS): IPS включають в себе функціонал IDS та додаткову здатність реагувати на виявлені атаки. Вони можуть автоматично блокувати атакуючий трафік та/або виконання процедур програмних модулів ескплойту, застосовуючи для цього наявні поведінкові сигнатури [20].

3) Антивірусне ПЗ виявляє та блокує відомий шкідливий програмний код, включаючи той, який використовують експлойти. Використовують бази даних відомих вразливостей та експлойтів для розпізнавання й блокування дій шкідливого ПЗ [27].

4) Використання декількох міжмережевих екранів (файрволів) та правил фільтрації трафіку може сприяти блокуванню трафіку, який містить відомі експлойти. Це дозволяє зменшити ризик експлуатації вразливостей системи.

5) Патчі та оновлення: - регулярне оновлення прикладного ПЗ, ОС та додатків дозволяє «закрити» відомі вразливості. Важливо постійно слідкувати за оновленням виправлень безпеки та вчасно встановлювати їх.

В цілому, реактивний захист проти експлойтів є важливою складовою загальній системи безпеки, оскільки дозволяє виявляти та припиняти атаки в реальному часі (тобто по факту інцидентів). Однак, слід чітко розуміти, що кращим підходом є комплексний захист, який поєднує обидві складові, тобто проактивні та реактивні заходи безпеки.

Розглянуті рекомендації можуть допомогти в організації системи ІБ для захисту від експлойтів. Проте, важливо пам'ятати, що захист від експлойтів є лише однією складовою системи ІБ і комплексний підхід до безпеки повинен включати в себе заходи для захисту від різноманітних типів загроз. В цілому, найкращий спосіб захисту від експлойтів - це поєднання відразу кількох методів захисту, які були розглянуто вище, та неперервне підтримання усього ПЗ в актуальному стані їх поточних релізів. Крім того, користувачам слід бути пильними та уважними при отриманні невідомих повідомлень та посилань від недовірених відправників, оскільки це може бути тільки першим кроком SE атак для підготовки умов використання експлойтів.

ВИСНОВКИ

В роботі проведено огляд інцидентів безпеки, що пов’язані з практикою застосування експлойтів. Узагальнення інформації стосовно відомих сценаріїв проведення атак з експлуатацією експлойтів свідчить про те, що зловмисники використовують стратегію «групових» (або кумулятивних) атак, основною ідеєю яких є, об'єднання відразу кількох експлойтів у складі одного мультивекторного експлойт-паку Exploit Kits). Така реалізація стратегії атаки забезпечує має більше шансів на «успіх» так як реалізує одночасно кілька напрямків компрометації цільової системи, шляхом виявлення та експлуатації всіх наявних уразливостей ПЗ. Найбільш «популярні» Exploit Kits, це ті, що впродовж свого використання підлаштовувались під нові вразливості та, відповідним чином, оновлювали свій склад новими експлойтами (наприклад, RIG EK та Magnitude). За результатами узагальнення тенденцій використання експлойтів можна стверджувати, що чисельність та склад найбільш «популярних» Exploit Kits, безпосередньо залежить від популярності (кількості використань чи масштабів інсталяції) того чи іншого ПЗ. Так наприклад, найбільш експлуатовані вразливості знаходяться в продуктах Microsoft та Adobe, а після 2020 року до них стрімко додались IoT-рішення, що пов’язано з значним переводом персоналу на дистанційну форму роботу (в наслідок пандемії COVID) та масовим впровадженням технології Інтернету речей.

В ході досліджень розглянуті питання практичного використання експлойтів. Підкреслено, що експлойти, здебільшого, використовуються зловмисниками для проведення акцій кібершантажу, несанкціонованого вилучення даних, шпигунства та перехвату функцій управління у легітимних користувачів. Також зловмисники частіше всього застосовують експлойти сумісно з SE атаками у зв'язці з іншим шкідливим ПЗ. Пентестери та спеціалісти з ІБ, також, можуть використовувати експлойти в контексті концепції «етичного

хакінгу» або тестування на проникнення з метою виявлення вразливостей у системах і надання рекомендацій щодо їх виправлення та покращення поточного рівня безпеки ПЗ. Однак, в обох випадках (напад та захист), використання експлойтів вимагає специфічних знань, зі сторони тих, хто з ними «працює».

За результатами проведених аналітичних досліджень встановлено, що існує декілька методів аналізу експлойтів, а саме реверс-інженерія та дослідження коду. Обидва ці методи розглядають внутрішню побудову експлойтів та надають інформацію про них. Інші методи, наприклад такі, як «аналіз трафику» й «аналіз журналу подій», сканують та оцінюють поведінку експлойтів в момент атаки на вразливу систему і зберігають інформацію для складання подальшого плану протидій цим атакам.

Спираючись на огляд профільних наукових публікацій, можна констатувати, що внутрішня побудова експлойтів доволі варіативна, оскільки їх різновидів доволі багато, то і їх «корисне навантаження» відрізняється залежно від мети застосування (та/або властивостей існуючих уразливостей). Основні компоненти більшості відомих експлойтів залишаються незмінними, це: - зловмисний код, котрий використовує вразливість, щоб отримати доступ до системи або даних; - спосіб взаємодії з вразливістю; - інструменти для подолання та/або обходу захисту систем безпеки. При цьому, код експлойту може бути прихований, бути змінним та/або зашифрований для ускладнення процесу його виявлення та дизассемблірування.

В роботі була запропонована узагальнена схеми цільової атаки на вразливу ІС умовним експлойт-паком та виконано їх класифікацію. Встановлено, що існує два основних класи експлойтів, це Zero-Day експлойти та N-експлойти. Крім того, експлойти можна класифікувати залежно від способу отримання доступу до вразливого ПЗ: - віддалені, локальні та експлойти підставного серверу. По-третє, експлойти поділяють за типом вразливості, призначенням та платформою, на яку буде націлена ця атака.

В межах робот сформульовано пропозиції, стосовно дій звичайних (приватних) користувачі, які можуть допомогти зменшити ризики атак експлойтами. Підкреслено що, діюча організація системи ІБ повинна втілювати виключно комплексний підхід, який складається з трьох етапів реагування на атаки експлойтами: превентивний, профілактичний, реактивний. Ці етапи були розглянуті на прикладі zero-days експлойтів та надані варіанти реагування на такий тип атак.

Отже, за результатами проведених досліджень можна зробити висновок, що експлойти є дуже серйозною загрозою для ІБ і вимагають постійного моніторингу, аналізу та застосування відповідних заходів протидії цій загрозі. Розробка та своєчасне впровадження ефективних методів захисту від впливу експлойтів є критичним напрямом діяльності для забезпечення безпеки ІС приватних користувачів та інформаційних ресурсів корпоративних мереж.

ПЕРЕЛІК ВИКОРИСАННИХ ДЖЕРЕЛ

1 Богданова, Е., & Малахов, С. (2022). Обобщение специфики применения эксплойтов. Збірник наукових праць SCIENTIA, (Vol.2), 28-32. URL: https://ojs.ukrlogos.in.ua/index.php/scientia/issue/view/24.06.2022/759 Available at: DOI 10.36074/scientia-24.06.2022 (дата звернення 20.05.2023)

2 Богданова, Є., Чорна, Т., & Малахов, С. (2022). Огляд поточного стану загроз, що обумовлені впливом експлойтів. Комп'ютерні науки та кібербезпека, (2), 35-40. URL: https://periodicals.karazin.ua/cscs/article/view/21039/19745 (дата звернення 22.04.2023)

3 2022 security report: software vendors saw 146% increase in cyber attacks in 2021, (2022) marking largest year-on-year growth. URL: https://research.checkpoint.com/2022/2022-security-report-software-vendors-saw-146-increase-in-cyber-attacks-in-2021-marking-largest-year-on-year-growth/ (дата звернення 15.03.2023)

4 A Deep Dive Into RIG Exploit Kit Delivering Grobios Trojan. (2022) URL: https://www.mandiant.com/resources/blog/deep-dive-into-rig-exploit-kit-delivering-grobios-trojan (дата звернення 25.04.2023)

5 Search CVE List. URL: https://cve.mitre.org/cve/search_cve_list.html (дата звернення 29.05.2023)

6 Magnitude Exploit Kit: Still Alive and Kicking. (2021) URL: https://decoded.avast.io/janvojtesek/magnitude-exploit-kit-still-alive-and-kicking/ (дата звернення 27.04.2023)

7 Top Exploit Kit Activity Roundup – Spring 2018. (2018) URL: https://www.zscaler.com/blogs/security-research/top-exploit-kit-activity-roundup-spring-2018 (дата звернення 27.04.2023)

8 Гайкова, В., & Малахов, С. (2021). Суть аналогий кибербуллинга и эксперимента Милгрэма. Збірник наукових праць ΛΌГОΣ. URL: https://doi.org/10.36074/logos-14.05.2021.v1.39 (дата звернення 12.04.2023)

9 Погоріла, К., Лєсная, Ю., Богданова, Є., & Малахов, С. (2022). Соціальний інжиніринг, як фактор реалізації інсайдерських загроз. Scientific Collection «InterConf», (111): with the Proceedings of the 1st International Scientific and Practical Conference «Scientific Community: Interdisciplinary Research» (June 6-8, 2022). Boston, USA; pp. 494-501. URL: https://archive.interconf.center/index.php/conference-proceeding/issue/view/6-8.06.2022 (дата звернення 05.05.2023)

10 Kaspersky Security Bulletin 2021. Statistics. (2021) URL: https://securelist.com/kaspersky-security-bulletin-2021-statistics/105205/ (дата звернення 02.04.2023)

11 The Rise and Imminent Fall of the N-Day Exploit Market in the Cybercriminal Underground. (2021) URL: https://documents.trendmicro.com/assets/white_papers/wp-the-rise-and-imminent-fall-of-the-n-day-exploit-market-in-the-cybercriminal-underground.pdf (дата звернення 10.04.2023)

12 Bogdanova, E., Pavlova, L., & Pohorila, K. (2022). A concise overview of the specific features of using exployts. Комп'ютерні науки та кібербезпека, (1), 15-19. URL: https://doi.org/10.26565/2519-2310-2022-1-02 (дата звернення 28.04.2023)

13 Гайкова, В., & Малахов, С. (2021). Аналіз факторів і умов реалізації кібербулінгу з урахуванням можливостей сучасних інформаційних систем. *Комп'ютерні науки та кібербезпека*, (1), 50-59. URL: https://periodicals.karazin.ua/cscs/article/view/17435/16040 (дата звернення 01.05.2023)

14 Джон Маллери, & Джейсон Занн (2007). *Безопасная сеть вашей компании.* (Е. Линдеманн, пер. с англ.). Москва: НТ Пресс.

15 What Is an Exploit? We Look at How It Works & How to Mitigate It. (2021) URL: https://websitesecuritystore.com/blog/what-is-exploit-how-does-it-works/ (дата звернення 11.05.2023)

16 Секрети кібербезпеки: Що таке пентест і навіщо він потрібен компаніям? (2021) URL: https://eba.com.ua/sekrety-kiberbezpeky-shho-take-pentest-i-navishho-vin-potriben-kompaniyam/ (дата звернення 13.05.2023)

17 Богданова, Є., Чорна, Т., Азаров, С., & Малахов, С. (2023). Особливості проблематики використання експлойтів. Scientific Collection «InterConf», (144), 540-544. URL: https://archive.interconf.center/index.php/conference-proceeding/issue/view/26-28.02.2023/154 (дата звернення 19.05.2023)

18 Що таке реверс-інжиніринг? Інструменти, процеси та приклади. (2022) URL: https://gridinsoft.ua/reverse-engineering (дата звернення 01.04.2023)

19 What is Vulnerability Scanning? [And How to Do It Right] (2021) URL: https://www.hackerone.com/vulnerability-management/what-vulnerability-scanning-and-how-do-it-right (дата звернення 11.05.2023)

20 Жилін А. В., Шаповал О. М., Успенський О. А. Технології захисту інформації в інформаційно-телекомунікаційних системах : навчальний посібник. Київ, 2022. URL: https://ela.kpi.ua/bitstream/123456789/45723/1/NP_TZI_ITS.pdf (дата звернення 22.05.2023)

21 Exploit in Cyber Security. URL: https://www.wallarm.com/what/what-is-exploit (дата звернення 17.05.2023)

22 Що таке ботнет Mirai і як я можу захистити свої пристрої? (2021) URL: https://techukraine.net/що-таке-ботнет-mirai-і-як-я-можу-захистити-св/ (дата звернення 14.05.2023)

23 Zero-Day Exploits: Examples, Prevention and Detection. URL: https://www.cynet.com/zero-day-attacks/zero-day-exploit-recent-examples-and-four-detection-strategies/ (дата звернення 20.05.2023)

24 What Is an Exploit in Computer Security? URL: https://www.avg.com/en/signal/computer-security-exploits (дата звернення 20.05.2023)

25 Zero-Day Attacks, Exploits, and Vulnerabilities: A Complete Guide. URL: https://www.cynet.com/zero-day-attacks/zero-day-vulnerabilities-exploits-and-attacks-a-complete-glossary/ (дата звернення 22.05.2023)

26 Advanced Persistent Threat (APT) Attacks. URL: https://www.cynet.com/advanced-persistent-threat-apt-attacks/ (дата звернення 01.05.2023)

27 Zero-Day Attack Prevention: 4 Ways to Prepare. URL: https://www.cynet.com/zero-day-attacks/zero-day-attack-prevention/ (дата звернення 01.05.2023)

28 Рузудженк, С., Погоріла, К., Кохановська, Т., & Малахов, С. (2020). Особливості захисту корпоративних ресурсів за допомогою технології Honeypot. Комп'ютерні науки та кібербезпека, (4), 22-29. URL: https://periodicals.karazin.ua/cscs/article/view/15751/14600 (дата звернення 12.05.2023)

29 Погоріла К.В., Богданова Є.С., Колованова Є.П. Огляд можливостей та узагальнення специфіки реалізації XDR-технології, як засобу комплексної протидії актуальним загрозам інформаційної безпеки. Технології, інструменти та стратегії реалізації наукових досліджень: матеріали IV Міжнародної наукової конференції, м. Суми, 07.10.2022 р. / МЦНД. □ Вінниця: Європейська наукова платформа, 2022. - 142 с. DOI 10.36074/mcnd-07.10.2022

30 Automatic Exploit Prevention Technology. URL: https://media.kaspersky.com/pdf/kaspersky-lab-whitepaper-automatic-exploit-prevention.pdf (дата звернення 22.05.2023)

31 Secure Software Development Lifecycle. URL: https://www.aquasec.com/cloud-native-academy/supply-chain-security/secure-software-development-lifecycle-ssdlc/ (дата звернення 25.05.2023)

ДОДАТОК А

COLLECTION OF SCIENTIFIC PAPERS
SCIENTIA

24 June, 2022

Helsinki, Republic of Finland

SCIENCE OF XXI CENTURY: DEVELOPMENT, MAIN THEORIES AND ACHIEVEMENTS

II International Scientific and Theoretical Conference

VOLUME 2

Helsinki, 2022

Science of XXI century: development, main theories and achievements | Volume 2

Богданова Елизавета Сергеевна
студентка III курса, факультета компьютерных наук
Харьковский национальный университет имени В.Н. Каразина, Украина

Молков Сергей Витальевич
канд. техн. наук, старший научный сотрудник,
доцент кафедры безопасности информационных систем и технологий
Харьковский национальный университет имени В.Н. Каразина, Украина

ОБОБЩЕНИЕ СПЕЦИФИКИ ПРИМЕНЕНИЯ ЭКСПЛОЙТОВ

Вступление.

За последние 20 лет, в сфере обеспечения информационной безопасности, эксплойты (*фр. exploit - эксплуатировать*) продолжают оставаться одной из скрытых проблем [1]. Причин данного обстоятельства практически в равной мере являются, как разработчики ПО и различных защитных решений, так и сотрудников подразделений информационной безопасности (ИБ) компаний, и организаций. При этом среди профильных специалистов, до сих пор сохраняется неоднозначность в определении фактической роли и места эксплойтов. В прежде всего, в части того, может ли эксплойт, самостоятельно нанести вред информационной системе (ИС) и/или ее информационным ресурсам, или же его следует рассматривать, как некий инструмент (*средство*) для проникновения и последующего запуска другого вредоносного кода.

С учетом стремительной информатизации всех сфер деятельности современного общества и его критической зависимости от уровня и масштабов реализации сетевых технологий, в безусловном приоритете остаются вопросы обеспечения ИБ современных ИС и онлайн сервисов. Данное обстоятельство обусловило непрерывный эволюций инструментов, приемов и технологий, используемых злоумышленниками, в ходе поиска и эксплуатации различных уязвимостей ПО, и шлюзах безопасности программно-аппаратных средств ИС. Одним из таких инструментов, позволяющих преодолеть контур безопасности атакуемых ИС, являются эксплойты. Так их «популярность» приходится на минувших десятилетие, однако они до сих пор рассматриваются злоумышленниками, как эффективное «проникновенное» средство для проникновения в современные ИС (*например, отчет вируса WannaCryptor*). При этом эксплойты становятся все более изощренными, учитывая особенности как атакуемого ресурса, так и его системы безопасности.

Основная часть.

ПО создается людьми, а как известно, человеку свойственно ошибаться. В результате, даже наличие этапа тестирования кода, разрабатываемого ПО, не устраняет вероятность сохранения уязвимостей в создаваемом программном коде. Более того, нельзя исключать и угрозу умышленного внедрения в создаваемые программные продукты, тех или иных уязвимостей. При этом, мотивация подобных действий (по внедрению уязвимостей) может быть довольно широкой – от желания внутреннего аналайзера нанести «ожог» компании репутационный вред, или же с целью личной наживы, пытаясь впоследствии, реализовать скрытые уязвимости данного ПО на специальных онлайн ресурсах. В любом случае, безотносительно побуждающего мотива, эксплуатирующий эксплойтом уязвимость пользователь (в т.ч. и умышленно отдаленный), потенциально способен обеспечить контроль над целевой ИС и/или получить несанкционированный доступ к «чувствительным» данным.

Используя существующую уязвимость системной или прикладной программы и/или «онлайн сервиса», эксплойт создает необходимые предпосылки для

Рисунок А.1 – Наукове видання [1], сторінка 28

COLLECTION OF SCIENTIFIC PAPERS
SCIENTIA

CERTIFICATE OF PARTICIPATION

Yelyzaveta Bohdanova

participated in the II International Scientific and Theoretical Conference

SCIENCE OF XXI CENTURY: DEVELOPMENT, MAIN THEORIES AND ACHIEVEMENTS

June 24, 2022
Helsinki, Republic of Finland

The conference is included in the Academic Resource Index ResearchBib catalog

Head of the European Scientific Platform
Chairman of the Organizing committee
MARIIA HOLDENBLAT

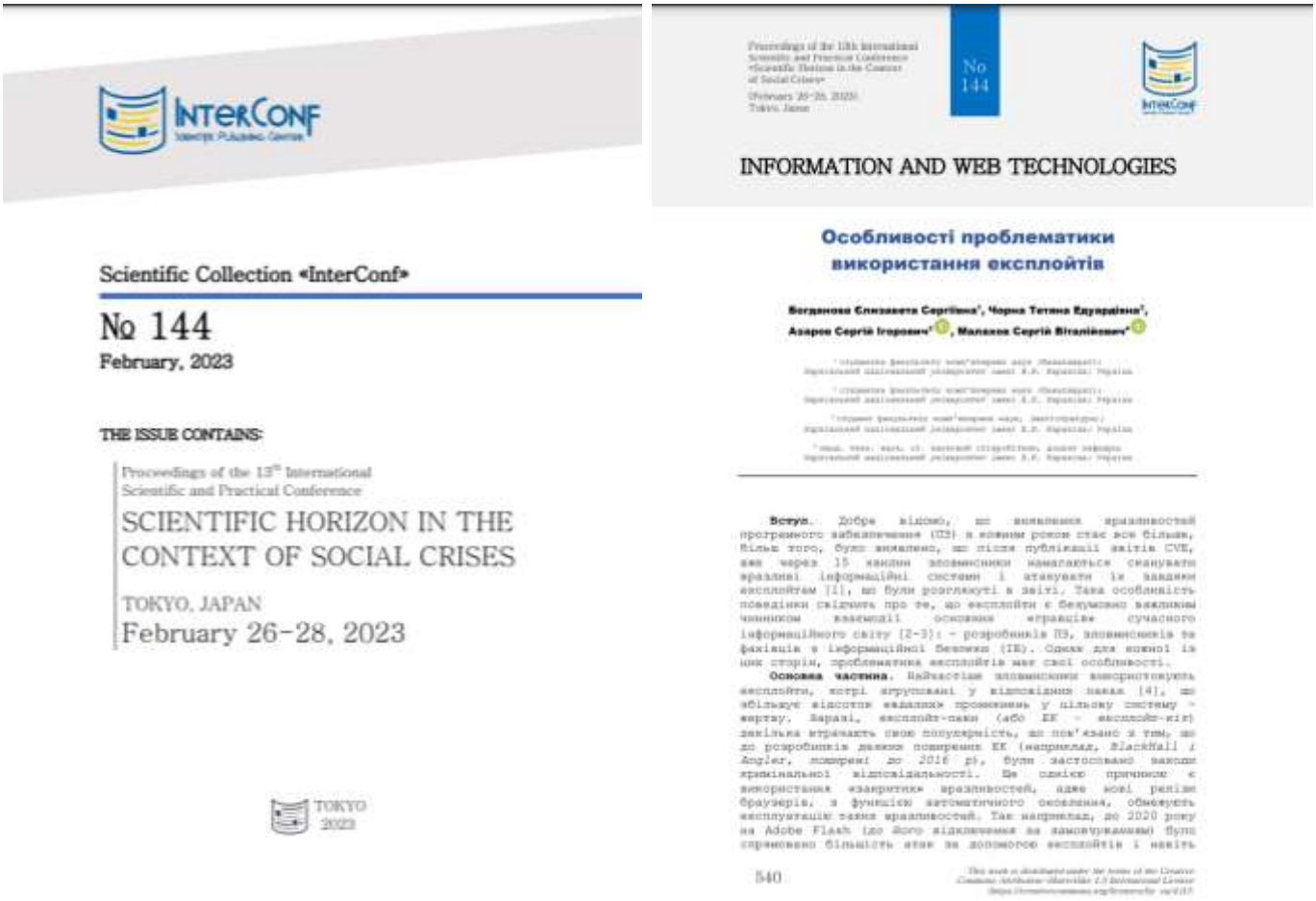
EUROPEAN SCIENTIFIC PLATFORM

Conference proceedings are publicly available under terms of the Creative Commons Attribution 4.0 International License (CC BY 4.0)

Рисунок А.1 – Сертифікат участі для роботи [1]

Рисунок А.2 – Наукове видання [12], сторінка 15

Рисунок А.3 – Наукове видання [2], сторінка 35



Scientific Collection «InterConf»

№ 144

February, 2023

THE ISSUE CONTAINS:

Proceedings of the 13th International Scientific and Practical Conference

SCIENTIFIC HORIZON IN THE CONTEXT OF SOCIAL CRISES

TOKYO, JAPAN

February 26-28, 2023

TOKYO 2023

Proceedings of the 13th International Scientific and Practical Conference «Scientific Horizon in the Context of Social Crises» (February 26-28, 2023) Tokyo, Japan

№ 144

INFORMATION AND WEB TECHNOLOGIES

Особливості проблематики використання експлойтів

Рисунок А.4 – Наукове видання [17], сторінка 540

Certificate Number: Fb-2326121

Certificate of Participation

We are honored to present this certificate to

Yelyzaveta Bohdanova

For participation in the XIII International Scientific and Practical Conference SCIENTIFIC HORIZON IN THE CONTEXT OF SOCIAL CRISES held on February 26-28, 2023 in Tokyo, Japan.

and for publishing a scientific paper

ОСОБЛИВОСТІ ПРОБЛЕМАТИКИ ВИКОРИСТАННЯ ЕКСПЛОЙТІВ

Рисунок А.4 – Сертифікат участі для роботи [17]