УДК 681.12

**ВАСИЛИНА А. В.**

# СУЧАСНИЙ СТАН СПОСОБІВ ЗДІЙСНННЯ АТАК НА ІНФОРМАЦІЙНІ РЕСУРСИ

Вінницький національний технічний університет

**Анотація**

*У даній роботі проведено аналіз сучасних інструментів, які можуть бути використані для здійснення атак на інформаційні ресурси та зламу програмного забезпечення зловмисниками. Також наведено приклади популярних хакерських інструментів, які використовуються для цих цілей.*

**Ключові слова:** програмне забезпечення, види злому, хакерські інструменти, фішинг, криптоджекінг, атаки з використанням штучного інтелекту (AI) і машинного навчання, сталкерське ПЗ, DoS-атака, EtherHiding.

**Abstract**

*This article analyzes modern tools that can be used to carry out attacks on information resources and hacking software by attackers. Examples of popular hacking tools used for these purposes are also given.*

**Keywords:** software, types of hacking, hacking tools, phishing, cryptojacking, attacks using artificial intelligence (AI) and machine learning, stalker software, DoS attack, EtherHiding.

## Вступ

Кібербезпека є найважливішим елементом сучасного цифрового світу. Зі зростанням залежності суспільства від інтернету та цифрових технологій зростає і кількість потенційних загроз. Зловмисники постійно розробляють нові та вдосконалені методи атак, ставлячи під загрозу дані, фінанси та репутацію компаній і окремих осіб. Від фішингових атак до складних цільових порушень - сфера загроз кібербезпеки широка та різноманітна. Для того, щоб ефективно протистояти цим загрозам, важливо розуміти їх природу та механізми дії.

## Результати дослідження

Ризики, що пов`язані з інформаційними технологіями, виходять на новий рівень, оскільки з`являються різні лазівки в безпеці та потенційні вразливості, завдяки чому питання безпеки та конфіденційності даних мають дуже важливу роль. Кількість Інтернет-загроз і атак на інформаційні ресурси у сучасному інформатизованому суспільстві є дуже великою. Розглянемо найпопулярніші з них.

***Атаки з використанням штучного інтелекту (Artificial Intelligence, AI) і машинного навчання*** являють собою нове покоління кіберзагроз, де зловмисники використовують передові технології для посилення та оптимізації своїх нападів. Використовуючи алгоритми машинного навчання, хакери швидко аналізують величезні обсяги даних, виявляючи слабкі місця в системах безпеки, а також автоматично адаптуються до захисних заходів.

Крім того, за допомогою AI зловмисники створюють більш переконливі фішингові кампанії або маскують шкідливе програмне забезпечення (ПЗ) таким чином, щоб воно залишилося непоміченим для традиційних засобів виявлення. Ця тенденція робить важливим постійне оновлення та модернізацію систем безпеки для протидії сучасним загрозам.

***Криптоджекінг*** – зловмисники впроваджують майнінгові скрипти на чужі комп'ютери або веб-сайти, щоб використовувати їхні обчислювальні ресурси для видобутку криптовалюти. Таке незаконне використання чужих ресурсів не тільки уповільнює роботу інфікованих систем, а й призведе до збільшення рахунків за електроенергію для жертви. Крім фінансових збитків, довгострокове використання обладнання для майнінгу призведе до його зносу і несподіваних відмов, що ставить під загрозу надійність і довговічність пристрою.

***Фішинг*** – це атака, яка в основному використовує електронну пошту як вектор та в обманний спосіб змушує людей завантажувати шкідливі програми на свої пристрої. Зловмисники намагаються залучити користувачів до надання своїх особистих даних, таких як паролі або банківські дані, шляхом імітації офіційних листів. Це зловживання довіри призводить до розкриття конфіденційної інформації зловмисникам. Фішинг може проявлятись по-різному (табл. 1).

Таблиця 1 – Різновиди фішингу та техніки їх використання.

| Вид атаки | Мета | Техніка |
|---|---|---|
| spear-phishing | Цільові атаки на конкретних людей, наприклад, системних адміністраторів | Використання особистої інформації про жертву, щоб створити правдоподібний контент |
| whaling | Атаки на керівників вищої ланки | Використання інформації про жертву, щоб створити враження, що повідомлення надходить від офіційної особи |
| smishing | Атаки, що використовують текстові або SMS-повідомлення, щоб привернути увагу жертви | Використання повідомлень, які виглядають як повідомлення від легітимної організації, щоб заманити жертву на підроблений веб-сайт або завантажити шкідливе програмне забезпечення |
| search engine phishing | Атаки, які за допомогою SEO підвищують у пошуковій видачі позиції сайтів потрібних злочинцям | Використання SEO-технік для створення підроблених веб-сайтів, які з'являються у результатах пошуку для певних запитів |
| email phishing | Атаки через електронну пошту | Використання повідомлень, які виглядають як повідомлення від легітимної організації, щоб заманити жертву на підроблений веб-сайт або завантажити шкідливе програмне забезпечення |
| vishing | Атаки через голосову пошту | Використання телефонних дзвінків, які виглядають як дзвінки від легітимної організації, щоб заманити жертву на підроблений веб-сайт або завантажити шкідливе програмне забезпечення |

***Сталкерське ПЗ***, також відоме як шпигунське або службове програмне забезпечення, являє собою програми, розроблені для моніторингу та запису дій користувача на пристрої без його відома. Це охоплює відстеження дзвінків, текстових повідомлень, історії відвіданих веб-сайтів, місця розташування і навіть захоплення екрана в реальному часі.

Такі програми часто використовуються в комерційних або батьківських цілях для моніторингу дій дітей або співробітників. Однак у руках зловмисників сталкерське ПЗ стане інструментом порушення особистого життя, шантажу або інших шахрайських дій. Важливо регулярно перевіряти свої пристрої на наявність підозрілих додатків і забезпечувати їх адекватним захистом.

***Програми-вимагачі (ransomware)*** – це шкідливе ПЗ, яке блокує доступ користувачів до їхнього програмного забезпечення і вимагає заплатити викуп. Зазвичай ransomware поширюється за допомогою спаму або соціальної інженерії.

***DoS-атака*** (від англ. Denial of Service – відмова в обслуговуванні) - це вид кібератаки, метою якої є порушення нормальної роботи цільової системи, сервісу або мережі, роблячи їх недоступними для кінцевих користувачів. Це досягається шляхом перевантаження цільової системи великим обсягом непотрібних запитів, що призведе до тимчасового або навіть постійного припинення її роботи.

Існує також різновид цієї атаки, званий DDoS-атакою (Distributed Denial of Service), коли зловмисник використовує безліч заражених комп'ютерів (зазвичай об'єднаних у ботнет) для одночасного надсилання запитів до цільового ресурсу. Це робить DDoS-атаки потужнішими і складнішими для протидії, оскільки атака йде з безлічі джерел одночасно.

***EtherHiding*** **–** техніка представляє «новий поворот у обробці шкідливого коду» шляхом використання контрактів Binance Smart Chain (BSC) від Binance – одного з найбільших у світі криптовалютних сайтів – для розміщення частин ланцюжка шкідливого коду.

Атака починається, коли зловмисники використовують скомпрометовані сайти WordPress для вбудовування прихованого коду JavaScript, який впроваджується на сторінки, який отримує корисне навантаження другого етапу з сервера, контрольованого зловмисником. Звідти зловмисники псують

веб-сайти за допомогою «дуже правдоподібного накладення, яке вимагає оновлення браузера, перш ніж доступ до сайту буде доступним».

Хакерські атаки на програмне забезпечення постійно еволюціонують, і зловмисники постійно шукають нові методи для отримання несанкціонованого доступу та скомпрометування систем. Важливо розуміти основні методи атак та вживати заходів для забезпечення безпеки програмного забезпечення.

## Висновки

Сучасні хакінг-техніки та інструменти нагадують нам про важливість постійного вдосконалення кібербезпеки. Ці інструменти є лише кількома з багатьох, які використовуються хакерами для злому програмного забезпечення. Важливо пам'ятати, що використання цих інструментів без належних дозволів є незаконним і неправомірним. На сьогоднішній день, компанії та організації вкладають значні зусилля в підвищення безпеки свого програмного забезпечення, але хакери постійно шукають нові способи для злому систем. Тому важливо бути обережними і вживати всі можливі заходи для захисту своєї системи та конфіденційної інформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. CYBER DIGEST Огляд подій в сфері кібербезпеки, березень 2023. Режим доступу: https://www.rnbo.gov.ua/files/2023/NKCK/%D0%BA%D0%B2%D1%96%D1%82%D0%B5%D0%BD%D1%8C/Cyber%20digest_March_2023_UA.pdf (дата звернення: 30.11.2023).
2. Найпопулярніші види кібератак у 2021. Режим доступу: https://10guards.com/ua/articles/the-most-common-types-of-cyber-attacks-in-2021/ (дата звернення: 30.11.2023).
3. Злом Darknet: методи та інструменти, які використовують кіберзлочинці. Режим доступу: https://ts2.space/uk/%D0%B7%D0%BB%D0%BE%D0%BC-darknet-%D0%BC%D0%B5%D1%82%D0%BE%D0%B4%D0%B8-%D1%82%D0%B0-%D1%96%D0%BD%D1%81%D1%82%D1%80%D1%83%D0%BC%D0%B5%D0%BD%D1%82%D0%B8-%D1%8F%D0%BA%D1%96-%D0%B2%D0%B8%D0%BA%D0%BE/#gsc.tab=0 (дата звернення: 12.11.2023).
4. Техніка блокчейну «Etherhiding» маскує шкідливий код на сайтах WordPress. Режим доступу: https://www.darkreading.com/cyberattacks-data-breaches/etherhiding-blockchain-technique-hides-malicious-code-wordpress-sites (дата звернення: 27.11.2023).
5. CyberNews дайджест №1 Серпень 2023. Режим доступу: https://my-itspecialist.com/cybernews-digest-1-august-2023 (дата звернення: 21.11.2023).



***Василина Анастасія Василівна*** – студентка групи 2БС-22б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: nstvsln@gmail.com.

Науковий керівник: ***Каплун Валентина Аполінаріївна*** - ст. викл. кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, e-mail: valuka8379@gmail.com.

***Vasylyna Anastasia Vasylivna*** - is a student of group 2BS-22b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia.

Supervisor: ***Kaplun Valentyna Apolinariivna*** - Lecturer of the Chair of Safety of Information and Communication Systems, NTU, Vinnytsia.