

[12] Гібридна війна: сутність, виклики та загрози: зб. матер. Круглого столу (Київ, 8 липня 2021 р.). [Електронне видання]. Київ: НА СБУ, 2021. 189 с URL: https://academy.ssu.gov.ua/uploads/p_57_28744724.pdf (дата звернення: 14.02.2023).

FEATURES OF USING SOCIAL NETWORKS TO ACHIEVE CYBERINFLUENCE

In the modern information society, such a type of virtual communities as social networks has become widespread. The task of such social Internet services is to provide users with all possible ways of interacting with each other. Social networks, in addition to fulfilling the functions of supporting communication, exchange of opinions, meet their professional needs, political ambitions, satisfaction of their interests in art, permission and preservation of information by members of the virtual community, increasingly become objects and use of informational and cybernetic influence. Monitoring of open sources, accounts, groups, application of social engineering methods and realization of cybernetic influences are considered the main stages of conducting cybernetic operations in social Internet services that use them. In the conditions of the Russian Federation's large-scale war against Ukraine, which has a largely hybrid component, digital means of mass communication and social Internet services are widely used by the enemy to exert destructive informational, psychological and cybernetic influence on the military-political leadership, personnel and population of the country as a whole. Therefore, it is

relevant to analyze the vulnerabilities of an individual user, depending on the information posted by him in social networks, and to develop methods of protection against destructive cybernetic influences, so that it is possible to create an effective system for detecting and countering them in the future.

Keywords: social network, social Internet service, virtual community, cyber influence, social engineering, vulnerabilities of social network users.

Самчишин Олексій Володимирович, кандидат технічних наук, старший дослідник, начальник кафедри захисту інформації та кібербезпеки Житомирського військового інституту імені С. П. Корольова.

Oleksii Samchyhsyn, Candidate of Technical Sciences (PhD), Senior Researcher, Head at the Chair of Information Protection and Cybersecurity of Korolov Zhytomyr Military Institute.

E-mail: samyj123@ukr.net.

Orcid ID: 0000-0002-1542-1065.

Носова Ганна Дмитрівна, начальник науково-організаційного відділення Житомирського військового інституту імені С. П. Корольова.

Hanna Nosova, Head of Research and Organizational Department of Korolov Zhytomyr Military Institute.

E-mail: hannanos@ukr.net.

Orcid ID: 0000-0003-3573-9828.

DOI: 10.18372/2410-7840.24.17380

УДК 004.49

ДОСЛІДЖЕННЯ МОЖЛИВОСТЕЙ ВИКОРИСТАННЯ ЧАТБОТІВ ЗІ ШТУЧНИМ ІНТЕЛЕКТОМ ДЛЯ ДОСЛІДЖЕННЯ ЖУРНАЛІВ ПОДІЙ

Іван Опірський, Віталій Сусукайло, Святослав Васишин

Дана стаття аналізує можливість використання чат ботів зі штучним інтелектом для аналізу інцидентів інформаційної безпеки. Вона визначає, як чатботи можуть допомогти організаціям покращити швидкість та точність реагування на інциденти, зменшити навантаження в групах безпеки та мінімізувати вплив інцидентів. У статті розглядаються виклики, що стоять перед організаціями в реагуванні на інциденти, включаючи все більший обсяг та складність загроз та дефіцит кваліфікованих спеціалістів безпеки. Також розглядається, як штучний інтелект може допомогти організаціям вирішити ці проблеми, автоматизуючи звичайні завдання, такі як аналіз журналів подій та визначення індикаторів компрометації систем. Пропонуються способи майбутнього реагування на інциденти та ролі автоматизації в розслідуванні кібербезпеки. Також, проведено аналіз важливості збалансування автоматизації з людським досвідом та судженням, а також необхідністю постійних інвестицій у технології та персоналу, щоб випереджати нові загрози. В цілому стаття надає інформацію про переваги використання штучного інтелекту для реагування на інциденти інформаційної безпеки та підкреслює необхідність організацій сприймати чат ботів з штучним інтелектом як ключовий компонент їх стратегії кібербезпеки.

Ключові слова: чатбот, Штучний Інтелект, кіберзлочини, кіберзагрози, кібербезпека, SIEM, інциденти, IDR, ChatGPT.

ВСТУП

Швидке зростання технологій створило для бізнесу як можливості, так і проблеми. Незважаючи на те, що технологічний прогрес призвів до підвищення ефективності та результативності операцій, він також призвів до збільшення загроз кібербезпеці. У цьому контексті системи виявлення вторгнень та керування подіями (SIEM) стали важливим інструментом для організацій для моніторингу своєї IT-інфраструктури та виявлення потенційних загроз безпеці. З появою штучного інтелекту (AI) і машинного навчання системи SIEM на основі штучного інтелекту стають новим рішенням, які допомагають організаціям виявляти загрози кібербезпеці та реагувати на них у реальному часі. У цій статті буде проаналізовано важливість використання чатботів на базі штучного інтелекту для кібербезпеки, висвітлено переваги та недоліки цієї технології та досліджено потенційний вплив на майбутнє кібербезпеки. Досліджуючи роль штучного інтелекту для дослідження кіберзлочинів, ця стаття має на меті забезпечити повне розуміння того, як штучний інтелект може підвищити ефективність і результативність операцій кібербезпеки для організацій.

Інструменти безпеки інформації та керування подіями розроблені, щоб допомогти організаціям контролювати свою IT-інфраструктуру та виявляти потенційні загрози безпеці проте не завжди організація має змогу використовувати технології для дослідження кіберзлочинів з Штучним інтелектом. Проте інструменти кібербезпеки без використання Штучного Інтелекту мають і свої переваги:

1. Рентабельність: інструменти без штучного інтелекту можуть бути дешевшими, ніж рішення на основі штучного інтелекту, що робить їх економічно ефективнішим варіантом для невеликих організацій або організацій з обмеженим бюджетом.

2. Простота використання: інструменти без штучного інтелекту можуть бути легшими для налаштування та використання, вимагаючи менше технічних знань для налаштування та обслуговування.

3. Налаштування: інструменти без штучного інтелекту можуть бути більш налагоджувальними, дозволяючи організаціям створювати власні правила кореляції та механізми виявлення, адаптовані до їхніх конкретних потреб безпеки.

4. Гнучкість: інструменти без штучного інтелекту можуть бути більш гнучкими, дозволяючи організаціям за потреби інтегрувати їх з іншими інструментами та процесами безпеки.

Тому для організацій які мають обмежений бюджет та ресурси може бути не доцільним використання Штучного Інтелекту. Проте для великих організацій з більшими можливостями Штучний інтелект може стати у нагоді так як має такі переваги:

1. Автоматизація: рішення на основі штучного інтелекту можуть автоматизувати багато завдань, зменшуючи робоче навантаження на команди безпеки та дозволяючи їм зосередитися на більш складних завданнях.

2. Розширене виявлення загроз: рішення на основі штучного інтелекту можуть аналізувати великі обсяги даних і виявляти складні загрози, які можуть бути пропущені традиційними інструментами.

3. Підвищена точність: рішення на основі штучного інтелекту можуть зменшити помилкові спрацьовування та помилкові негативні результати, підвищуючи точність виявлення загроз і зменшуючи втому від попереджень.

4. Моніторинг у режимі реального часу. Рішення на основі штучного інтелекту можуть забезпечувати моніторинг у режимі реального часу та сповіщення, що дозволяє командам безпеки швидко реагувати на потенційні загрози.

Загалом як інструменти без штучного інтелекту, так і рішення на основі штучного інтелекту мають свої переваги та недоліки, і найкращий варіант для організації залежатиме від її конкретних потреб і бюджету. У той час як рішення на основі штучного інтелекту пропонують розширені можливості виявлення загроз і автоматизації, інструменти SIEM без штучного інтелекту можуть бути економічно ефективнішими та адаптованими.

Постановка проблеми

Як можна ефективно використовувати технології штучного інтелекту, щоб допомогти в розслідуванні та запобіганні кіберзлочинам, одночасно вирішуючи потенційні етичні проблеми, пов'язані з конфіденційністю та упередженістю? Зокрема, як ШІ можна використовувати для виявлення та запобігання кіберзагрозам, виявлення та відстеження кіберзлочинців, а також аналізу вели-

ких обсягів даних, щоб виявити закономірності та тенденції, які можуть вказувати на злочинну діяльність? Крім того, як ці системи штучного інтелекту можна розробити та впровадити таким чином, щоб надавати пріоритет конфіденційності та справедливості даних і зменшувати ризик збереження упередженості чи дискримінації? Відповіді на ці запитання мають вирішальне значення для розробки ефективних і відповідальних інструментів ШІ для розслідування кіберзлочинів.

Аналіз останніх досліджень і публікацій

Штучний інтелект і машинне навчання стають дедалі популярнішими для аналізу журналів завдяки їхній здатності обробляти великі обсяги даних і виявляти закономірності, які людям може бути важко виявити. Для прикладу Мін Ду, Фейфей Лі, Гуйненг Чжен і Вівек Срікумар у своєму дослідженні «DeerLog: виявлення та діагностика аномалій із системних журналів за допомогою глибокого навчання» представляють DeerLog, модель глибокої нейронної мережі, яка вчиться виявляти аномалії в даних журналу, передбачаючи наступну подію журналу на основі історичних даних. Цей підхід показує багатообіцяючі результати у виявленні аномалій і діагностиці проблем у системах реального світу. Дослідження "Drain3: гнучкий і ефективний фреймворк аналізу журналів" проведене Едуардо Бланко, Вагеліс Атлідакіс та Родріго Фонсека представляє Drain3, оновлену версію алгоритму аналізу журналу Drain. Drain3 пропонує підвищену ефективність і гнучкість, що робить його більш придатним для обробки великомасштабних даних журналу. Автори демонструють ефективність Drain3 у визначенні шаблонів журналів і зменшенні ручних зусиль під час аналізу журналів. Ці публікації демонструють різноманітні застосування ШІ для аналізу журналів, включаючи виявлення аномалій, розбір журналів, безпеку та керування хмарою. Поточні дослідження в цій галузі спрямовані на подальше підвищення ефективності та результативності аналізу журналів за допомогою методів ШІ.

Метою статті є дослідження можливості використання чатботів зі Штучним Інтелектом для дослідження кіберзлочинів.

ОСНОВНА ЧАСТИНА

Підготовка середовища

Як потенційно вразливе середовище було використано додаток OWASP Juice Shop на сервері Ubuntu в Digital Ocean. Детальна схема налаштування середовища вказана на рисунку 1. Для підготовки середовища було проведено наступні дії: створено сервер Ubuntu в Digital Ocean, встановлено Owasp Juice Shop як контейнер та встановлено Nginx як Reverse Proxy для запису всіх запитів.

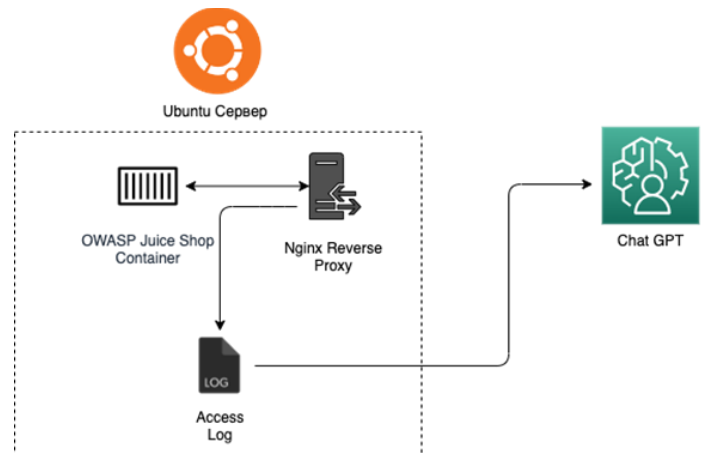


Рис. 1. Схема потенційно вразливого середовища

Для генерації журналів подій з потенційними атаками на налаштоване середовище використовувались наступні застосунки: Nessus, nmap, Burp Suite та Metasploit. Автоматизовані засоби пошуку вразливостей використовувались для того, щоб охопити якомога більше типів атак. Зокрема для даного експерименту було визначено, що автоматизовані рішення дають наступні переваги:

- реалістичні сценарії атак: сканери вразливостей створені для імітації реалістичних сценаріїв атак, які імітують поведінку зловмисників у реальному світі. Використовуючи ці інструменти для створення журналів, можна створити ряд сценаріїв атак, які можуть допомогти вам перевірити ефективність IDS у виявленні та реагуванні на різні типи атак;
- узгоджене тестування: інструменти автоматизованого сканування, такі як Nessus, можуть виконувати узгоджене тестування в кількох системах, що важливо, коли потрібно перевірити ефективність IDS у великому масштабі;

- комплексне тестування: сканери вразливостей можуть перевіряти широкий спектр вразливостей і векторів атак, включаючи вразливості мережі, веб-додатків і хостів;

- ефективне тестування: автоматичні сканери вразливостей можуть виконувати тестування набагато швидше, ніж тестування вручну;

Загалом використання автоматизованих інструментів сканування вразливостей для створення журналів є ефективним способом тестування можливостей систем виявлення вторгнень і виявлення потенційних вразливостей і слабких місць.

Дослідження кібератак за допомогою GPT-3.5

Для дослідження різних типів кібератак за допомогою GPT 3.5 було використано журнали подій згенеровані під час попереднього кроку. Перший тип атаки який було надано GPT-3.5 є атака обходу каталогу використовує недостатню перевірку безпеки або дезінфекцію наданих користувачем імен файлів. Атака на обхід каталогу, також відома як атака на обхід шляху або перехід на каталог, є типом кібератаки, яка використовує вразливі місця в механізмах обробки файлів веб-додатку. Зловмисник прагне отримати неавторизований доступ до файлової системи програми, дозволяючи читати, змінювати або видаляти конфіденційні файли та дані.

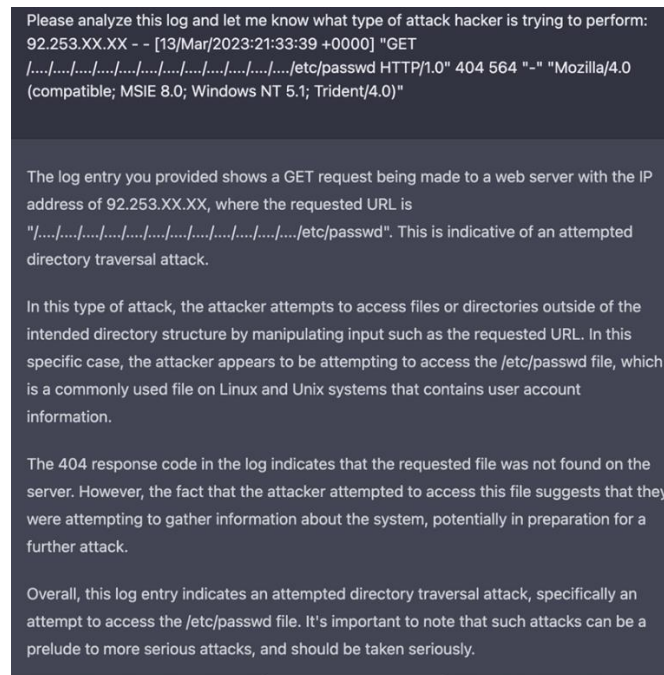


Рис. 2. Визначення атаки на обхід каталогу

Chat GPT було запропоновано два записи з журналу подій: запис що містить в собі інформацію про ймовірну атаку обходу каталогу та закодований варіант атаки обходу каталогу. Як бачимо ChatGPT зміг визначити тип атаки у обох випадках, як вказано на рисунках та описати запити, здійснені зловмисником. Запит без кодування ChatGPT розпізнав за 7 секунд, закодований за 8 секунд. Даний час є відносним так, як час реагування також залежить від мережевого з'єднання локально пристрою звідки запускається дослідження та параметрів локальної системи.

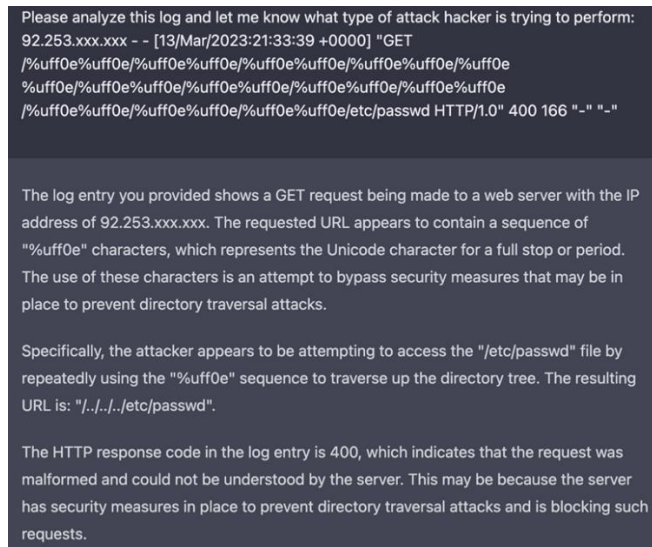


Рис. 3. Визначення атаки на обхід каталогу для закодованого фрагменту журналу подій

Наступний тип атаки який був запропонований для ChatGPT є XSS атака. Міжсайтовий скриптинг (XSS) – це тип уразливості веб-додатків, який дозволяє зловмисникам виконувати шкідливі сценарії на веб-сторінках, які переглядають інші користувачі. Атака відбувається, коли програма включає ненадійні дані (зазвичай дані, введені користувачем) на веб-сторінку без належної перевірки, екранування або кодування. У результаті шкідливий код зловмисника виконується в контексті браузера жертви, що потенційно може призвести до крадіжки даних, захоплення облікового запису або інших зловмисних дій.

Для аналізу XSS атаки було використано модель GPT-4.0. XSS. ChatGPT визначив тип атаки та описав принцип експлуатації XSS. Було визначено що зловмисник намагається вплинути на

додаток через JavaScript код та через параметри URL. Журнал подій вказує на запит GET до файлу "xmd79sr7.asp" з додатковим параметром URL, що містить вбудований JavaScript код: "<script>document.cookie=%022testmtbo=2804;%022</script>". Було визначено, що зловмисник провокує сервер відобразити цей код на веб-сторінці і, як результат, виконає його в браузері користувача. Також ChatGPT проаналізував відповідь серверу та вказав результат виконання запиту. Було визначено, що відповідь містить код 404, що означає "Не знайдено". Тому ChatGPT вказав, що може свідчити про те, що веб-сервер не відповів на запит або поточна конфігурація сервера перешкоджає виконанню таких атак. На проведення аналізу знадобилось 24 секунди. Доцільно відзначити, що запит сформовано українською мовою.

```
92.253.xx.xx - - [13/Mar/2023:21:33:53 +0000] "GET /xmd79sr7.asp
<script>document.cookie=%22testmtbo=2804;%22</script> HTTP/1.0" 404 564 "-"
"Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)"
```

За даними з журналу подій, здається, що зловмисник намагається виконати атаку на основі вбудованого скрипта, так званий "Cross-Site Scripting" атаку (XSS).

XSS атака полягає в тому, що зловмисник вставляє шкідливий код (зазвичай JavaScript) в сторінку веб-сайту з метою крадіжки даних користувача, модифікації вмісту веб-сайту або виконання інших дій від імені жертви. В даному випадку, зловмисник намагається вбудувати код JavaScript через параметри URL.

Журнал подій показує запит GET до файлу "xmd79sr7.asp" з додатковим параметром URL, що містить вбудований JavaScript код: "<script>document.cookie=%22testmtbo=2804;%22</script>". Зловмисник сподівається, що сервер відобразить цей код на веб-сторінці і, як результат, виконає його в браузері користувача.

Однак, у журналі подій вказано код 404, що означає "Не знайдено". Це може свідчити про те, що веб-сервер не відповів на запит або поточна конфігурація сервера перешкоджає виконанню таких атак.

Рис. 4. Визначення XSS атаки

Також в рамках даного дослідження було проаналізовано можливість виявлення сканування на вразливості та аналізу декількох записів журналів подій одночасно. Для даного дослідження було використано чат-бот ChatGPT версію моделі GPT 4.0. ChatGPT визначив, що надані журнали подій вказують на те, що зловмисник намагається знайти вразливі точки веб-сервера, використовуючи різні шляхи і методи запитів. Опрацювання журналів подій тривало 16 секунд. Також було опрацьовано та проаналізовано кожен запит індивідуально. Варто зазначити, що запити були опрацьовані та відповідь надана українською мовою.

```
92.253.xx.xx - - [13/Mar/2023:21:33:52 +0000] "POST /spipe?Source=nessus HTTP/1.0"
404 564 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)"
92.253.xx.xx - - [13/Mar/2023:21:33:52 +0000] "POST /cgi-bin/mainfunction.cgi
HTTP/1.0" 404 564 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)"
92.253.xx.xx - - [13/Mar/2023:21:34:07 +0000] "POST /flex2gateway/http HTTP/1.0" 404
564 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)"
```

Ці записи журналу подій вказують на те, що зловмисник намагається знайти вразливі точки веб-сервера, використовуючи різні шляхи і методи запитів. Така атака відома як "сканування" або "пробивання" веб-сервера.

1. Перший запис відображає спробу зловмисника виконати POST-запит на "/spipe?Source=nessus" з клієнта MSIE 8.0. "nessus" - це сканер безпеки, який може вказувати на спробу виявлення вразливостей.
2. Другий запис свідчить про спробу зловмисника виконати POST-запит на "/cgi-bin/mainfunction.cgi". Він може намагатися використати вразливості, пов'язані з CGI-скриптами.
3. Третій запис показує спробу зловмисника виконати POST-запит на "/flex2gateway/http". Це може вказувати на спробу атаки на вразливості Adobe Flex або AMF (Action Message Format) застосунків.

У всіх трьох випадках сервер відповідає кодом 404, що означає "Не знайдено". Це свідчить про те, що атакуючий не знайшов жодних існуючих ресурсів або вразливих елементів за наведеними шляхами. Загалом, сервер здається стійким до цих спроб атак.

Рис. 5. Виявлення сканування на вразливості

```
92.253.xx.xx - - [13/Mar/2023:21:39:23 +0000] "GET /wp-login.php HTTP/1.0" 404 162
"${jndi:ldap://log4shell-generic-8Vno2Ky4QW5hhAz16ZUW${lower:ten}.w.nessus.org/nessus}"
"${jndi:ldap://log4shell-generic-8Vno2Ky4QW5hhAz16ZUW${lower:ten}.w.nessus.org/nessus}"
92.253.xx.xx - - [13/Mar/2023:21:39:28 +0000] "GET /wwwadmin.cgi HTTP/1.0" 404 162
"${jndi:ldap://log4shell-generic-8Vno2Ky4QW5hhAz16ZUW${lower:ten}.w.nessus.org/nessus}"
"${jndi:ldap://log4shell-generic-8Vno2Ky4QW5hhAz16ZUW${lower:ten}.w.nessus.org/nessus}"
8Vno2Ky4QW5hhAz16ZUW${lower:ten}.w.nessus.org/nessus}"
"${jndi:ldap://log4shell-generic-8Vno2Ky4QW5hhAz16ZUW${lower:ten}.w.nessus.org/nessus}"
92.253.xx.xx - - [13/Mar/2023:21:39:23 +0000] "GET /wp-login.php HTTP/1.0" 404 162
"${jndi:ldap://log4shell-generic-8Vno2Ky4QW5hhAz16ZUW${lower:ten}.w.nessus.org/nessus}"
"${jndi:ldap://log4shell-generic-8Vno2Ky4QW5hhAz16ZUW${lower:ten}.w.nessus.org/nessus}"
92.253.xx.xx - - [13/Mar/2023:21:39:28 +0000] "GET /wwwadmin.cgi HTTP/1.0" 404 162
"${jndi:ldap://log4shell-generic-8Vno2Ky4QW5hhAz16ZUW${lower:ten}.w.nessus.org/nessus}"
"${jndi:ldap://log4shell-generic-8Vno2Ky4QW5hhAz16ZUW${lower:ten}.w.nessus.org/nessus}"
```

It seems like someone is attempting to exploit the Log4Shell vulnerability on your server. The Log4Shell vulnerability (CVE-2021-44228) is a critical security vulnerability found in the Apache Log4j library that allows remote code execution. It gained significant attention when it was discovered in December 2021.

In the logs you provided, the attacker is trying to access `wp-login.php` and `wwwadmin.cgi` endpoints with malicious payloads. They are using the `\${jndi:ldap://...}` syntax, which is specific to the Log4Shell vulnerability. The attacker is trying to make your server connect to their malicious LDAP server to execute arbitrary code.

Рис. 6. Виявлення експлуатації Log4j вразливості

Складність журналів подій поступово збільшувалась в ході даного дослідження. Для наступного аналізу було надано записи з журналів подій,

які були записані сервером під час спроби експлуатації Log4j вразливості. Вразливість Log4Shell (CVE-2021-44228) — це критична вразливість безпеки, виявлена в бібліотеці Apache Log4j, яка дозволяє віддалено виконувати код. ChatGPT з використанням GPT 4.0 успішно виявив експлуатацію CVE-2021-44228. На даний аналіз знадобилось 15 секунд. Варто зазначити, що отриманий результат надано англійською мовою.

Отож, у результаті даного дослідження можна зробити висновок, що з усіх наданих запитів ChatGPT опрацював усі та успішно виявив усі типи атак. Також у рамках даного дослідження були проведені експерименти з використанням масивів журналів подій з використанням декількох записів журналів подій, з якими модель успішно справилась.

ВИСНОВКИ

Чат-боти на основі штучного інтелекту, такі як ChatGPT, можуть революціонізувати спосіб розслідування кіберзлочинів, забезпечуючи швидке, масштабоване та економічно ефективне рішення для аналізу великих обсягів даних і виявлення потенційних загроз. Як показали дослідження, розглянуті в цій статті, чат-ботів на основі штучного інтелекту можна навчити виявляти моделі поведінки, позначати підозрілу активність і надавати персоналізовану підтримку жертвам кіберзлочинців.

Однак використання чат-ботів на основі штучного інтелекту для розслідування кіберзлочинів також викликає важливі етичні проблеми, пов'язані з конфіденційністю даних, упередженістю та можливістю чат-ботів підтримувати дискримінаційні практики. Щоб переконатися, що чат-боти на основі штучного інтелекту використовуються відповідально та ефективно в контексті розслідування кіберзлочинів, важливо, щоб майбутні дослідження були зосереджені на вирішенні цих проблем.

Існує кілька напрямків майбутніх досліджень щодо використання чат-ботів на основі ШІ для розслідування кіберзлочинів. Однією з важливих сфер уваги має бути розробка чат-ботів, призначених для захисту конфіденційності користувачів і пом'якшення ризику упередженості чи дискримінації. Це може включати вивчення нових підходів до анонімізації даних, впровадження суворого

контролю доступу до даних і використання передових алгоритмів для виявлення та пом'якшення упереджень у навчальних даних чат-бота.

Іншим важливим напрямком досліджень може стати розробка чат-ботів, здатних аналізувати нетекстові джерела даних, наприклад зображення та відео. Це може передбачати включення передових методів комп'ютерного зору та обробки природної мови в алгоритми чат-бота, щоб він міг ідентифікувати та аналізувати мультимедійний вміст, пов'язаний з кіберзлочинністю.

ЛІТЕРАТУРА

- [1] "AI and cybersecurity: The future of cyber defence" [Електронний ресурс]. Режим доступу до ресурсу: <https://www.forbes.com/sites/andrewrossow/2021/06/01/ai-and-cybersecurity-the-future-of-cyber-defence/>
- [2] "The role of AI in cybersecurity" by John Boitnot " [Електронний ресурс]. Режим доступу до ресурсу: <https://venturebeat.com/2018/03/31/the-role-of-ai-in-cybersecurity/>
- [3] Ду, М., Лі, Ф., Чжен, Г., і Срікумар, В. (2019). DeepLog: виявлення та діагностика аномалій із системних журналів за допомогою глибокого навчання. *ACM Transactions on Privacy and Security (TOPS)*, 22(4), 1-27. <https://doi.org/10.1145/3338501>
- [4] Бланко, Е., Атідакіс, В., Фонсека, Р. (2020). Drain3: гнучкий і ефективний фреймворк аналізу журналів. Матеріали конференції USENIX 2020 року з оперативного машинного навчання (OpML 20). <https://www.usenix.org/conference/opml20/presentation/blanco>
- [5] "How AI is transforming cybersecurity" by Gary Eastwood, " [Електронний ресурс]. Режим доступу до ресурсу: <https://www.information-age.com/how-ai-is-transforming-cybersecurity-123478294/>
- [6] Кларк, Дж., Джейкоб, Дж. (2018). ШІ та кібербезпека: загрози та рішення. *Журнал кібербезпеки*, 4(1), С. 1-14.
- [7] Ян, Дж., Чжан, Ю., Ван, Х., і Ву, В. (2017). Підхід глибокого навчання для виявлення вторгнень за допомогою рекурентних нейронних мереж. *IEEE Access*, 5, С. 21954-21961.
- [8] Чжу, Т., Лі, К., Рен, К., і Лу, В. (2019). Комплексне дослідження глибокого навчання для кібербезпеки. *ACM Computing Surveys (CSUR)*, 52(6), С. 1-39.
- [9] Ван, Х., Юань, Ю., Чжу, С. (2021). Опитування щодо глибокого навчання для виявлення

- мережових вторгнень. IEEE Communications Surveys & Tutorials, 23(1), С. 527-561.
- [10] Абрахам, А., Камарудін, С., і Чай, С. Т. (2020). Опитування щодо використання штучного інтелекту в кібербезпеці. Комп'ютери та безпека, 88, 101628 с.
- [11] Caviglione, L., Coccoli, M., Lops, C., & Nocerino, R. (2019). Застосування машинного навчання до кібербезпеки: вичерпний огляд. Прикладні науки, 9(10), 2038 с.
- [12] Poonia, P., Sharma, S.K., & Kumar, A. (2020). Система виявлення вторгнень на основі машинного навчання: комплексне дослідження. Journal of Ambient Intelligence and Humanized Computing, 11(9), С. 3963-3983.
- [13] Чжан, Х., Хуан, Х., і Чжан, Ю. (2019). Дослідження прогресу штучного інтелекту в кібербезпеці. Міжнародний журнал систем обчислювального інтелекту, 12 (1), С. 316-326.
- [14] Чжан Ю., Чен В., Ян Дж. та Сю В. (2019). Машинне навчання в кібербезпеці. IEEE Access, 7, С.108700-108707.
- [15] Опірський І.Р., С.І. Василюшин, В.А. Сусукайло . Розслідування кіберзлочинів за допомогою прийомок у хмарному середовищі. Безпека інформації, 27(1). 2021. С. 13-20. <https://doi.org/10.18372/2225-5036.26.15574>.

RESEARCH OF THE POSSIBILITIES OF USING CHATBOTS WITH ARTIFICIAL INTELLIGENCE FOR LOGS ANALYSIS

This article analyses the possibility of using chatbots with artificial intelligence to investigate information security incidents. It identifies how chatbots can help organizations improve the speed and accuracy of incident response, reduce the burden on security teams, and minimize the impact of incidents. The article examines the challenges organizations face in incident response, including the increasing volume and complexity of threats and the shortage of skilled security professionals. It also looks at how artificial intelligence can help organizations solve these problems by automating mundane tasks such as analyzing event logs

DOI: 10.18372/2410-7840.24.17381

УДК 004.946.5.056

МОДЕЛЮВАННЯ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ВПЛИВУ НА СУСПІЛЬСТВО

Володимир Артемов, Володимир Хорошко, Юлія Хохлачова

У статті дається визначення інформаційно-психологічних впливів (ІПВ) і основні шкали їх впливу на соціальні групи суспільства. Наведено опис моделі, що ведуть до форми нелінійного диференціального рівняння. В моделі враховано інформаційний вплив на масову свідомість міжособистісної інформаційної взаємодії, засобів масової інформації та ефект забування впливу ІПВ. Показано, що модель має рішення у вигляді узагальненої логістичної кривої. Наведено статистичне розподілення за часом окремих членів соціуму, які підтримують

and identifying indicators of system compromise. Future incident response methods and the role of automation in cyber security investigations are suggested. It also explores the importance of balancing automation with human experience and judgment and the need for continued investment in technology and personnel to stay ahead of emerging threats. Overall, the article provides insight into the benefits of using artificial intelligence to respond to information security incidents and highlights the need for organizations to embrace AI chatbots as a key component of their cybersecurity strategy.

Keywords: Chatbot, AI, cyberthreats, cybercrime, cybersecurity, SIEM, incidents, IDR, ChatGPT.

Опірський Іван Романович, д.т.н., проф., професор кафедри захисту інформації, Національний Університет "Львівська Політехніка", Львів, Україна.

Ivan Opriskyu, Dc.S., Professor, Professor of Information Security Department, Lviv Polytechnic National University, Lviv, Ukraine.

E-mail: ivan.r.opirskyi@lpnu.ua.

Orcid ID: 0000-0002-8461-8996.

Сусукайло Віталій Андрійович, аспірант кафедри захисту інформації, Національний університет «Львівська політехніка», м. Львів, Україна.

Vitalii Susukailo, Ph.D. student of Information Security Department, Lviv Polytechnic National University, Lviv, Ukraine.

E-mail: vitalii.a.susukailo@lpnu.ua.

Orcid ID: 0000-0003-4431-9964.

Василюшин Святослав Ігорович, аспірант кафедри захисту інформації, Національний університет «Львівська політехніка», м. Львів, Україна.

Sviatoslav Vasylyshyn, Ph.D. student of Information Security Department, Lviv Polytechnic National University, Lviv, Ukraine.

E-mail: swat2244@gmail.com.

Orcid ID: 0000-0003-1944-2979.