УДК 004.056.5:343.326 (045)
DOI https://doi.org/10.32782/2663-6170/2022.28.16

ВИДИ КІБЕРНЕТИЧНИХ АТАК РФ ТА ЇХ СОЦІАЛЬНО-ПОЛІТИЧНІ НАСЛІДКИ ДЛЯ УКРАЇНИ

TYPES OF CYBERNETIC ATTACKS OF THE RUSSIAN FEDERATION AND THEIR SOCIO-POLITICAL CONSEQUENCES FOR UKRAINE

Сунгурова С.Р.,
ад'юнкт кафедри військової політології
Військового інституту Київського національного університету імені Тараса Шевченка

У статті проведено аналіз основних видів кібернетичних атак, які використовує Російська Федерація проти України у інформаційно-цифровому просторі. Стверджується зростання актів кіберзлочинів з боку країни-агресора з моменту її вторгнення на українську територію 24 лютого 2022 року. Виявлено три групи найбільш уживаних кібернетичних атак: DDoS-атаки, пошкодження веб-сайтів та зараження зловмисним програмним забезпеченням шляхом фішингу. Розкрито специфіку кожної з цих груп. Так, у ході DDoS-атаки зловмисники перевантажують цільові веб-сайти запитами, що спричиняє збій у роботі служб веб-сайту та заважає легальним користувачам отримати доступ до цих сторінок. Пошкодження веб-сайтів передбачає злам веб-серверу та отримання адміністративного доступу для розміщення спотвореної інформації. Шкідливе програмне забезпечення знищує або деформує дані користувача, переважно, заражаючи систему вірусами. Доводиться, що відповідальні за кібернетичну безпеку державні структури вдало відбивають атаки ворога, підтримуючу критичну інфраструктуру країни у належному стані. Проаналізовано окремі заходи РФ з дезінформації за використання сфабрикованих фото, відео матеріалів, текстових новин тощо. Також визначено негативні наслідки кібернетичних атак у короткостроковій перспективі та обґрунтовано позитивний вплив на вітчизняну інформаційну та цифрову інфраструктури у більш тривалому часовому проміжку. Зокрема, кібератаки можуть чинити тимчасовий збій у роботі банківської та фінансової систем, енергетичної галузі, системах мобільного та стаціонарного зв'язку тощо, що у свою чергу, може негативно відбиватися на життєзабезпеченні населення, координованості дій різних гілок влади, комунікації між громадянами та з громадянами і т. д. У той же час, вони можуть сприяти удосконаленню вітчизняної системи цифрової та інформаційної безпеки, проактивній позиції держави, міжнародній співпраці у протистоянні агресору, обізнаності населення у технологіях цифрової та інформаційної боротьби, гігієні українських соціальних мереж тощо.

Ключові слова: кібератаки, шкідливе програмне забезпечення, пошкодження веб-сайтів, дезінформація, цифрова інфраструктура.

The article analyzes the main types of cyber-attacks used by the Russian Federation against Ukraine in the information and digital space. It is alleged that cybercrime acts on the part of the aggressor country have increased since its invasion of Ukrainian territory on February 24, 2022. Three groups of the most commonly used cyber-attacks have been identified: DDoS attacks, website defacement, and phishing software. The specifics of each of these groups are revealed. For example, in a DDoS attack, attackers overload targeted websites with queries, which disrupts website services and prevents legal users from accessing those pages. Website defacement involves hacking a web server and gaining administrative access to post distorted information. Malicious software destroys or deforms user data, mainly infecting the system with viruses. It appears that government agencies responsible for cyber security are successfully repelling enemy attacks, maintaining the country's critical infrastructure in good condition. Some measures of the Russian Federation on disinformation for the use of fabricated photo and video materials, text news, etc. are analyzed. The negative consequences of cyber-attacks in the short term have also been identified and the positive impact on the domestic information and digital infrastructure over a longer period has been substantiated. In particular, cyber-attacks can temporarily disrupt the banking and financial systems, energy sector, mobile and fixed systems, etc., which in turn can negatively affect the livelihoods, coordination of various branches of government, communication between citizens and with citizens. etc. At the same time, they can contribute to the improvement of the domestic system of digital and information security, proactive position of the state, international cooperation in combating the aggressor, public awareness of digital and information technology, hygiene of the Ukrainian social networks and more.

Key words: cyber-attacks, phishing software, website defacement, misinformation, digital infrastructure.

Постановка проблеми. З моменту вторгнення армії РФ на територію України у лютому 2022 року боротьба на інформаційному «фронті» суттєво масштабувалася. Зросла частота кібернетичних атак та інформаційних провокацій з боку супротивника. Українській стороні довелося активно захищатися та контратакувати силами СБУ, Міністерства цифрової трансформації, кіберполіції, РНБО, ЗСУ тощо. Лави кібервійська стрімко поповнюються небайдужими спеціалістами з IT царини приватного сектору, які хочуть використати свої знання та вміння у боротьбі з агресором в інформаційно-цифровому просторі. І якщо у січні 2022 року біля 70 українських веб-сайтів зазнали атак з боку Росії (включаючи Міністерство освіти і науки України, Міністерство закордонних справ тощо), то за перший місяць військової агресії РФ у 2022 році було здійснено понад 3000 кібернетичних атак. Рекордною була кількість 275 – на день.

Аналіз останніх досліджень і публікацій. Загалом боротьба у інформаційно-кібернетичному просторі, методики, інструменти, теоретичні засади і багато інших наукових аспектів цієї проблематики вивчаються широким колом як вітчизняних, так і зарубіжних пошуковців. У цьому контексті принагідно згадати таких експертів, як Б. Брейк, О. Буров, І. Валюшко, Л. Веселова, Дж. Гулд, С. Колінз, М. Лібіцкі, П. Паганіні, Р. Стендіш, О. Трофіменко, Г. Форос тощо.

Виділення невирішених раніше частин загальної проблеми. Однак, аналітик, присвячених деталізації кібернетичних інструментів, якими оперує РФ від моменту вторгнення на українські землі в лютому 2022 року, поки що бракує.

Формулювання цілей статті (постановка завдання). Саме тому мета статті полягає у дослідженні основних видів кібернетичних атак, до яких активно вдається Росія з моменту широкомасштабного нападу. Це дозволить вивчити кібернетичну поведінку супротивника, його провідні інструменти та проаналізувати можливі соціально-політичні наслідки їх застосування для України.

Виклад основного матеріалу дослідження. «Хакери насамперед атакують фінансову, державну та телекомунікаційну інфраструктуру. Попри це, всі сервіси працюють і доступні для користувачів. Провайдери і оператори справляються з кібератаками на свої мережі. Більшість проблем у роботі мереж пов'язана з фізичними пошкодженнями, які також вдається швидко усувати» [1], – зазначив Віктор Жора, заступник Голови Держспецзв'язку з питань цифрового розвитку, цифрових трансформацій та цифровізації.

Загалом кібератаки, які використовує Росія проти України, можна класифікувати за трьома типами: DDoS-атаки, пошкодження веб-сайтів та зараження зловмисним програмним забезпеченням шляхом фішингу. Перші два інструменти точніше описуються як кібер-зриви, тоді як останній більш спрямований на кібершпигунство для збору розвідданих і підготовки поля бою до подальших кінетичних наступів або кібератак [2, с. 121].

Під час DDoS-атаки зловмисники перевантажують цільові веб-сайти запитами, що спричиняє збій у роботі служб веб-сайту та заважає легальним користувачам отримати доступ до цих сторінок. Цей метод вимагає використання кількох комп'ютерів, заражених бот-мережами, або координації роботи великої кількості користувачів. Зловмисники контролюють такі комп'ютери, скомпрометовані ботнетами, щоб надсилати запити до цільової мережі, про що користувачі заражених комп'ютерів навіть не здогадуються. DDoS-атаки також можуть відволікати увагу, щоб монополізувати увагу екстреної служби цільової установи. Поки вона зайнята боротьбою з DDoS-атакою, зловмисники можуть здійснювати інші шкідливі дії у відповідній мережі, наприклад, встановити бекдор або шкідливе програмне забезпечення з метою крадіжки даних [3, с. 4].

Пошкодження веб-сайту також спостерігається як інструмент кібернетичних активностей, задіяних проти українських цифрових ресурсів. Ця техніка передбачає, що хакер зламує веб-сервер за допомогою ін'єкції SQL, щоб отримати адміністративний доступ. Такий вид кібератаки вважається кібер-версією вандалізму. Після проникнення в систему зловмисник змінює зовнішній вигляд веб-сайту або замінює сторінки своїми матеріалами. Зазвичай, цю техніку використовують для поширення політичних меседжів.

Різні шкідливі програми також активно використовуються у інформаційному протистоянні. Серед останніх превалює використання трьох груп шкідливих програм, зокрема BlackEnergy, Snake та Operation Armageddon.

BlackEnergy – це сімейство шкідливих програм, які часто використовуються кіберзлочинцями. Перша версія BlackEnergy використовувалася для отримання доступу до мереж з метою запуску DDoS-атак. Друга версія, BlackEnergy2, була оновлена функціями, які дозволяють красти дані. Остання версія, BlackEnergy3, була оновлена для націлювання на системи контролю та збору даних (SCADA) і додала нову функцію KillDisk, яка зробила заражені комп'ютери непридатними для використання. Ця версія була використана для атаки на українську енергосистему ще в грудні 2015 року [4].

Зловмисники використовують фішингові електронні листи зі зламаним вкладенням, щоб заразити комп'ютери. Потім зловмисне програмне забезпечення встановлює бекдор, щоб надати хакерам доступ до мережі. Останні дві версії зловмисного програмного забезпечення були розгорнуті для збору інформації та імплантовані в конкретні цілі, такі як український уряд та українська енергосистема.

Шкідливе програмне забезпечення Snake було виявлено у 2014 році, але було активним принаймні з 2010 або 2011 року. Воно схоже на більш стару зловмисну програму Agent.btz. Жертви заражалися або відкриваючи фішингові електронні листи, або шляхом відвідування веб-сайтів водопою, тобто веб-сторінок, заражених шкідливим програмним забезпеченням. Після того, як зловмисне програмне забезпечення заражає комп'ютер, воно чекає, поки користувач відкриє веб-браузер, а потім одночасно відкриває бекдор для спілкування зі зловмисниками без відома користувача [5]. Цей засіб призначений для копіювання та видалення файлів, підключення до заражених серверів, а також для завантаження та виконання інших шкідливих програм. Зловмисне

програмне забезпечення Snake складається з двох елементів: руткіта і драйвера. Перший бере контроль над комп'ютером і приховує його діяльність від користувача, щоб вкрасти дані та захопити мережевий трафік. Драйвер вводить код у веббраузер, щоб приховати обмін інформацією з серверами зловмисників, і створює прихований файл для зберігання конфігурації та вкрадених даних [6]. З початку Євромайдану в Україні зросла кількість комп'ютерів, заражених саме Snake.

Operation Armageddon – це інструмент віддаленого адміністрування або доступу, був спрямований на український уряд, правоохоронні органи та військові мережі. Його виявила у вересні 2014 року американська охоронна фірма LookingGlass. Експерти з безпеки та українські чиновники підозрюють Росію у створенні та використанні цього шкідливого програмного забезпечення [7]. Його метою є збір інформації про своїх противників, можливо, щоб отримати перевагу на полі бою. Ця практика демонструє, що кібершпигунство можна використовувати як інструмент для підтримки фізичної війни. Вважається, що ця шкідлива програма була активна щонайменше з 2013 року, коли Україна почала обговорювати Угоду про асоціацію з ЄС. Вона заражала машини через фішингові електронні листи зі скомпрометованим вкладенням Microsoft Word. Було відзначено, що деякі вкрадені документи були введені зловмисним програмним забезпеченням і надіслані новим цілям фішингових листів [8].

15 березня 2022 року в Україні фахівцями компанії ESET було виявлене нове зловмисне програмне забезпечення – вірус-вейпер CaddyWiper. За свідченням експертів, CaddyWiper знищує дані юзера та інформацію про розділи з будь-яких накопичувачів, які підключені до ураженої системи. Спеціалісти зазначають, що програма-шкідник деформує файли на накопичувачі у спосіб перезапису символами нульового байта, в результаті чого їх неможливо відновити.

«Раніше дослідники виявили два інших штами шкідливого програмного забезпечення Wiper, націленого на комп'ютери в Україні. Перший штам під назвою HermeticWiper був виявлений 23 лютого, за день до того, як Росія розпочала військове вторгнення в Україну. Версія IsaacWiper була розгорнута в Україні 24 лютого. При цьому в ESET припускають, що IsaacWiper і HermeticWiper перебували в розробці за кілька місяців до їх появи. Їхні перші зразки були виявлені у жовтні та грудні 2021 року, відповідно» [9].

Росія також інвестує багато ресурсів у скоординовані кампанії з дезінформації, а не лише у відкриті хакерські операції. Росія просуває неправдиві наративи про вторгнення в Україну як на власній території, так і в українському та світовому інформаційному полях, включаючи підроблені відео (зустріч В. Путіна зі співробітницями авіаційної галузі, коли його рука магічним чином проходить крізь мікрофон), фото (Р. Кадиров у молитві на колінах в Україні, але на російській заправці) та новини (катування російських полонених, обстріли українськими військами своїх же населених пунктів, вербування українськими посольствами по всьому світу іноземних найманців та терористів, пропагування ненависті до мешканців Донбасу в українських підручниках). Російські чиновники заблокували доступ до соціальних мереж у країні, щоб запобігти поширенню інформації, яка не відповідає внутрішнім наративам.

Цілком зрозуміло, що вище описані злочинні активності хакерів від РФ у короткостроковій перспективі є деструктивними для державної та інформаційної інфраструктури України. Зокрема, такі дії можуть чинити тимчасовий збій у роботі банківської та фінансової систем, енергетичної галузі, системах мобільного та стаціонарного зв'язку тощо, що у свою чергу, може негативно відбиватися на життєзабезпеченні населення, координованості дій різних гілок влади, комунікації між громадянами та з громадянами і т. д.

Значний обсяг кібератак на українські державні інституції може підірвати віру людей в ці інституції та посилити загальне відчуття незахищеності. DDoS-атаки та пошкодження підривають довіру людей до їхніх інституцій та їхню здатність захищати власне населення. Пошкодження недержавних веб-сайтів передбачає переспрямування відвідувачів на інший веб-сайт, цільові веб-сторінки можуть втратити клієнтів, поки пошкодження зберігається. Такі пошкодження додатково спричиняють втрату довіри у власників зіпсованих веб-сайтів. Ці атаки виявляють слабкі місця в безпеці веб-сторінки, що може вказувати на подальшу вразливість і, таким чином, зробити сайти та власників сайтів ненадійними. Але в умовах воєнного стану такі нетривалі перепони (адже як доводить практика державний та приватний сектори оперативно вирішують створені ворогом цифрові проблеми), не є першорядними і не завдають непоправної шкоди цифровій критичній інфраструктурі України.

Якщо ж оцінювати кібернетичні атаки агресора більш далекоглядно, стає зрозумілим, що вони сприяють удосконаленню вітчизняної системи цифрової та інформаційної безпеки, проактивній позиції держави, міжнародній співпраці у протистоянні агресору, обізнаності населення у технологіях цифрової та інформаційної боротьби, гігієні українських соціальних мереж, відповідальній поведінці користувачів комп'ютерами, телефонами та планшетами тощо.

Висновки та перспективи подальших розвідок у цьому напрямі. Низка соціально-полі-

тичних наслідків може бути вичленована з кібератівності, яка має місце в російській кампанії інформаційної війни проти України. Досвід нашої держави може стати у нагоді для багатьох інших країн, які бажаючи лишатися відкритими та демократичними, мають дбати про безпеку власного інформаційного поля. Зокрема, вони повинні активно намагатися зміцнити свою позицію, щоб їхня держава не стала жертвою пропагандистських кампаній. Крім того, вони повинні підвищити кібербезпеку державних онлайн-інфраструктур від атак розподіленої відмови в обслуговуванні та пошкодження веб-сайтів. Також покращення кібербезпеки може бути пов'язане з обмеженням залежності від іноземних технологій та наданням рекомендацій приватному сектору щодо того, як реагувати на кібератаки. Демократичні держави повинні уважно стежити за тим, як розвивається україно-російське протистояння у інформаційному просторі, і сприяти заходам зміцнення довіри на міжнародному рівні. Майбутні наукові розвідки в контексті проблематики статті можуть бути спрямовані на аналіз нових видів атак, які можуть з'явитися з часом у кібернетичному протистоянні проти РФ, компаративних студій різних видів кібератак, а також дослідження дієвих засобів протидії та контрнаступу у інформаційно-цифровому просторі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Держспецзв'язку: Від 15 лютого Україна зазнала понад 3000 DDoS-атак. URL: https://www.kmu.gov.ua/news/derzhspeczvyazku-vid-15-lyutogo-ukrayina-zaznala-ponad-3-000-ddos-atak.

2. Torruella R.A., Determining Hostile Intent in Cyberspace. Jt. Force. 2014.Q. 75. P. 114–121.

3. NSFocus Inc. Distributed Denial-of-Service (DDoS) Attacks: An Economic Perspective (Whitepaper). NSFocus Inc. Santa Clara. CA. 2016.

4. FireEye Inc. FireEye Industry Intelligence Report cyber attacks on the Ukrainian grid: what you should know. FireEye Inc. Milpitas. CA. 2016.

5. Paganini P. BAE Systems Applied Intelligence has disclosed a Russian cyber espionage campaign codenamed as SNAKE that targeted Governments and Military Network. URL : http://securityaffairs.co/wordpress/22875/intelligence/snake-cyber espionagecampaign.html.

6. Paganini P. Crimea – The Russian Cyber Strategy to Hit Ukraine. URL : http://resources.infosecinstitute.com/crimearussian-cyber-strategy-hit-ukraine/.

7. Witty R. LookingGlass Cyber Threat Intelligence Group Links Russia to Cyber Espionage Campaign Targeting Ukrainian Government and Military Officials. URL : https://www.lookingglasscyber.com/pressrelease/lookingglass-cyber-threat-intelligencegroup-links-russia-to-cyber-espionagecampaign-targeting-ukrainian-governmentand-military-officials/.

8. Hackett R. Russian cyberwar advances military interests in Ukraine, report says. URL : http://fortune.com/2015/04/29/russiancyberwar-ukraine/.

9. ESET виявила в Україні новий вірус-вайпер CaddyWiper, який знищує дані на накопичувачах. URL : https://itc.ua/ua/novini/eset-viyavila-v-ukrayini-novij-zlovred-caddywiper-yakij-znishhuye-dani-na-nakopichuvachah/.