УДК 004.056.5

А.Є. Москаленко

Методи та засоби кібератак у віртуальному середовищі

Вінницький національний технічний університет

Анотація

У цій статті розглянуто інструменти, які використовують кібершахраї для здійснення своїх атак. Розглянуті методи включають вразливості програмного забезпечення, фішинг, шкідливе програмне забезпечення, DDoS-атаки.

Ключові слова: інструменти, кібершахраї, атаки, викрадення даних, вразливості, ПЗ, фішинг, DDoS-атаки.

Abstract

This article examines the tools that cybercriminals use to carry out their attacks. Techniques covered include software vulnerabilities, phishing, malware, DDoS attacks.

Keywords: tools, cyber crooks, attacks, data theft, vulnerabilities, software, phishing, DDoS attacks.

Вступ

Кіберзлочинність визначається як незаконна діяльність, спрямована проти будь-якої особи, яка використовує комп'ютер або його системи, онлайн або офлайн додатки. Це відбувається, коли інформаційні технології використовуються для вчинення або приховування злочину. Однак діяння вважається кіберзлочином лише тоді, коли воно є навмисним, а не випадковим. Перехід з офлайну в онлайн майже в усіх сферах нашого життя призвів до відродження кіберзлочинності, особливо в останні роки: за оцінками експертів Statista, глобальні втрати від кібершахрайства зростуть з 1,2 трильйона доларів США у 2019 році до 7,1 трильйона доларів США до 2022 року. Водночас, за даними Chainalysis, у 2021-2022 роках зростає кількість зломів та атак з боку великих міжнародних хакерських угруповань [1].

Результати досліджень

Кібершахраї використовують широкий спектр інструментів для здійснення своїх злочинів. Пропонується розглянути атаки до яких вони можуть призвести. Перш за все однією загроз для користувачів мережі Інтернет є фішинг. Фішинг— це одна з найпоширеніших кібератак, фішинг в основному складається з шахрайських повідомлень електронною поштою. Зазвичай метою такої практики є викрадення конфіденційної інформації, наприклад, кредитних карток або персональних даних. Також до загроз віднесено шкідливе програмне забезпечення, таке як шпигунське програмне забезпечення, програми-вимагачі, віруси та черв’яки. Потрапивши в систему, хакер може блокувати доступ до ключових компонентів мережі, отримувати інформацію, інсталювати додаткове шкідливе програмне забезпечення тощо [2]. Злом також відноситься до атак, які спричинюють зловмисники, тобто це отримання несанкціонованого доступу до комп’ютерної системи чи мережі. Також ще можна віднести до загроз спричиненими шахраями спуфінг— це акт змусити одну комп’ютерну систему або мережу прикинутися ідентичністю іншого комп’ютера. Здебільшого він використовується для отримання доступу до ексклюзивних привілеїв, якими користується ця мережа чи комп’ютер [3]. Для здійснення масштабного втручання або виведення компанії з роботи використовуються DDoS атаки. Для здійснення відмови в обслуговуванні (DDoS) кібершахраї використовують інструменти, що дозволяють залучати велику кількість комп'ютерів або пристроїв до надсилання трафіку на цільовий сервер або мережу, з метою перевантаження та призводить до відмови в обслуговуванні для легітимних користувачів.

Проаналізуємо інструменти, що використовуються для кібератак. Їх існує велика кількість, але для кращого розуміння, розглянемо лише найвідоміші з них.

Kali Linux — це програмне забезпечення з відкритим кодом, яке підтримується та фінансується Offensive Security [3]. Це спеціально розроблена програма для цифрової експертизи та тестування на проникнення.

Ophcrack — цей програмний інструмент в основному використовується для злому хешів, які генеруються тими ж файлами windows. Він пропонує безпечну систему графічного інтерфейсу і дозволяє працювати на кількох платформах [3].

Інструмент віддаленого доступу (RAT) — це програма, яка після встановлення на комп'ютері жертви дозволяє дистанційно адміністративно керувати [4]. У зловмисному контексті вони можуть надати актору можливість завантажувати та завантажувати файли, виконувати команди, реєструвати натискання клавіш та/або записувати екран користувача [4]. Прикладом шкідливого RAT є JBiFrost. Цей RAT найчастіше надсилається як додаток до електронного листа, як правило, у вигляді повідомлення про рахунок-фактуру, запиту на участь у тендері, повідомлення про грошовий переказ, повідомлення про відвантаження, повідомлення про оплату або посилання на файловий хостинг-сервіс.

Веб-оболонки — це шкідливі сценарії, які завантажуються на цільовий хост після початкового злому та надають актору віддалений доступ до мережі [4]. Як тільки цей доступ буде встановлено, веб-оболонки можуть полегшити бічний рух у мережі. Прикладом широко використовуваної веб-оболонки є China Chopper , добре задокументована та загальнодоступна веб-оболонка, яка широко використовується з 2012 року.

Mimikatz — інструмент, який використовується кількома суб'єктами для отримання облікових даних із мереж, зазвичай використовується після отримання доступу до хосту, який бажає пересуватися внутрішньою мережею. Спостерігається широке використання цього інструменту серед організованої злочинності та фінансованих державою груп.

PowerShell Empire — легальний інструмент для тестування на проникнення, але широко використовується зловмисниками. Інструмент надає зловмисникам можливість підвищувати привілеї, збирати облікові дані, витягувати інформацію та переміщатися в мережі. Інструмент набуває все більшої популярності серед державних органів та організованих злочинних угруповань і нещодавно став об'єктом низки глобальних інцидентів у широкому спектрі секторів.

Висновок

Кіберзлочинність є серйозною загрозою в сучасному цифровому суспільстві. Кіберзлочинність проявляється у використанні інформаційних технологій для здійснення або приховування злочинів. Наше дослідження показує, що кіберзлочинці використовують різноманітні інструменти та методи для досягнення своїх цілей. Фішинг, шкідливе програмне забезпечення, системний злом, спуфінг і DDoS-атаки - це лише деякі з атак, які використовують кіберзлочинці. Їхні інструменти включають різноманітні програми та програмні платформи, такі як Kali Linux, Ophcrack, Remote Access Tool (RAT), Web Shell, Mimikatz та PowerShell Empire. Ці висновки вказують на необхідність посилення заходів безпеки в Інтернеті та підвищення обізнаності користувачів про потенційні загрози. Вони також відображають необхідність постійного вдосконалення кібербезпеки на рівні користувачів, корпорацій та урядів для забезпечення безпеки в Інтернеті та запобігання кіберзлочинності.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Кібершахраї стають активнішими в Україні та світі. Які інструменти вони використовують та як захиститися? [Електронний ресурс] – Режим доступу: https://fintechinsider.com.ua/kibershahrayi-stayut-aktyvnishymy-v-ukrayini-ta-sviti-yaki-instrumenty-vony-vykorystovuyut-ta-yak-zahystytysya/ (дата звернення 04.05.2024)
2. 8 Most Powerful Cybersecurity Tools in 2023 [Електронний ресурс] – Режим доступу: https://distantjob.com/blog/cybersecurity-tools/ (дата звернення 04.05.2024)
3. What is Cybercrime? Types, Tools, Examples [Електронний ресурс] – Режим доступу: https://www.guru99.com/cybercrime-types-tools-examples.html (дата звернення 04.05.2024)
4. Top 5 hacking tools: 5 Eyes report[Електронний ресурс] – Режим доступу: https://ngm.com.au/5-most-available-hacking-tools/ (дата звернення 04.05.2024)

Москаленко Аліна Євгеніївна- студентка групи 1БКС-22б, факультету інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: moskalenkoalina56@gmail.com

Moskalenko Alina Evgeniivna- student of group 1BKS-22b, faculty of information technologies and computer engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: moskalenkoalina56@gmail.com

Науковий керівник: ***Гарнага Володимир Анатолійович*** – к.т.н., доцент кафедри захисту інформації, факультету інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: garnaga.volodymyr@vntu.edu.ua.

Supervisor: ***Harnaha Volodymyr*** - Ph.D., Associate Professor of the Department of Information Protection, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia.