категорії громадян, послідовність, логічне викладення, злагодженість, переконливість, аргументованість із посиланням на різні факти доказів, правові норми, відповідність морально-етичним нормам поведінки, наявність достатньої інформації для досягнення цілей спілкування.

Всі ці навички спілкування необхідно розвивати працівникам правоохоронних органів для досягнення високого рівня мовної культури, оскільки професійне спілкування є важливою компонентою освіти поліцейських, яка дає їм можливість виконувати свої службові обов'язки на вищому рівні.

Одержано 29.05.2022

Вадим Анатолійович КОРШЕНКО,
завідувач науково-дослідної лабораторії з проблем інформаційних технологій та протидії злочинності у кіберпросторі Харківського національного університету внутрішніх справ

Захар Георгійович ДЕМИДОВ,
старший науковий співробітник науково-дослідної лабораторії з проблем інформаційних технологій та протидії злочинності у кіберпросторі Харківського національного університету внутрішніх справ

DDOS-АТАКИ: АНАЛІЗ ПЕРШОГО КВАРТАЛУ ПОТОЧНОГО РОКУ ТА ПЕРСПЕКТИВИ

DDoS-атаки, як і раніше, займають значну частину загроз для безпеки в IT-сфері. На ландшафт цих атак у першому кварталі 2022 року суттєво вплинула агресія Росії у бік України. Значна частина новин щодо атак на ресурси стосувалась саме Росії та України. У середині січня мішенню DDoS став сайт мера Києва Віталія Кличка, а низка веб-ресурсів українських міністерств зазнала дефейсу. У середині лютого DDoS-атаки торкнулися сайту Міністерства оборони України, онлайн-сервісів Ощадбанку та ПриватБанку, а також хостинг-провайдера Mirohost. Приблизно водночас клієнти ПриватБанку отримували підроблені SMS про непрацюючі банкомати, імовірно націлені на те, щоб посіяти паніку. Ще одна хвиля DDoS прокотилася по урядових ресурсах України 23 лютого, а Державна служба спеціального зв'язку та захисту інформації України повідомляла про безперервні атаки наприкінці лютого та на початку березня.

На початку березня дослідники з компанії Zscaler опублікували аналіз [1] атак на українські ресурси, які проводив один із операторів DanaBot. Цей банківський троянець поширюється за моделлю «зловред як послуга» (MaaS). Покупець використав DanaBot для завантаження на заражені пристрої DDoS-бота, єдина функція якого – атакувати жорстко прописаний у коді домен. Спочатку метою був поштовий сервер Міністерства оборони України. Атаки на цей ресурс тривали з 2 по 7 березня, після чого зловмисник перейшов на сайт Ради національної безпеки і оборони України, присвячений інформації про російських військовополонених.

Інформаційний ресурс LiveUAMap, що дозволяє в реальному часі відстежувати розвиток російсько-української війни, також став мішенню DDoS[2]. Цей сайт журналісти та благодійні організації використовують, як джерело актуальної інформації. Крім того, атакам зазнавали українські ЗМІ та інформаційні видання країн НАТО. Зокрема, від DDoS постраждав український портал Еспресо. Загалом, за даними українських провайдерів, DDoS-атаки на ті чи інші ресурси доводилося відбивати весь березень[3].

Починаючи з 24 лютого, шквал DDoS-атак у відповідь обрушився на російські сайти. Ціллю стали ЗМІ, державні органи регіонального (наприклад, у Югрі) та федерального рівня, Роскосмос, РЗ, Держпослуги, телеком-провайдери та інші організації. Наприкінці березня DDoS-атака торкнулася російського реєстратора доменів Ru-Center, через що сайти клієнтів компанії деякий час були недоступні. За даними РБК, як мінімум, частина атак на ЗМІ здійснювалася з веб-ресурсів, на яких був опублікований заклик припинити дезінформацію. За деякі атаки, наприклад, за DDoS телеканалу Russia Today, відповідальність на себе взяло хактивістське угруповання Anonymous, яке оголосило Росії війну у зв'язку з російською агресією.

Anonymous - не єдині хактивісти, які виступили на підтримку України. Уряд країни закликав волонтерів[4] вступати в IT-армію, у завдання якої входять у тому числі і DDoS-атаки. Координувалися такі атаки, зокрема через канал у Телеграмі, куди організатори постили списки цілей. Крім того, в мережі з'явилося багато сайтів, що пропонують користувачам будь-якого ступеня IT-грамотності приєднатися до DDoS проти російських організацій. Достатньо було відкрити сайт у браузері, щоб той почав відправляти запити на заданий список веб-ресурсів. Щоб користувач не нудьгував, на сайті можна було, наприклад, пограти в онлайн-гру.

Також, хактивісти розповсюджували програми, що атакують ресурси із заданого списку від імені користувача. Як і у випадку з сайтами, творці програм рекламували їх, як засоби для атаки на

російські ресурси. За даними компанії Avast, лише одне з них завантажили щонайменше 900 користувачів з України. При цьому програми не просто проводять атаку від імені користувача, а збирають дані про нього: IP-адресу, приблизне місце розташування, ім'я користувача, дані про систему, тимчасову зону, мову і т.п.

На ландшафт DDoS-атак у першому кварталі сильно вплинула геополітична ситуація: з кінця лютого спостерігався сплеск хактивістської активності та поява великої кількості стихійних ботнетів, до яких користувачі підключалися доброю волею. Хактивістські атаки відрізнялися великою тривалістю, навіть якщо сміттєвий трафік успішно фільтрувався захисними рішеннями. При цьому активність відомих ботнетів з кінця лютого помітно знизилася, а з точки зору тривалості з минулого звітного періоду зросла кількість довгих і дуже коротких атак цих ботнетів.

Окремо варто відзначити ситуацію із захистом від DDoS, яка спостерігалася у Росії у першому кварталі. Вал нових клієнтів перевантажив усі сервіси захисту від DDoS у Росії. В результаті їх просто не встигали підключати, що призвело до тривалої недоступності багатьох ресурсів.

Прогнозувати щось у поточних умовах дуже складно. Упевнено можна стверджувати лише одне: стан ринку DDoS у другому кварталі залежатиме насамперед від геополітичної ситуації у світі. Вкрай малоймовірно, що буде спад DDoS-активності до кінця бойових дій на території України. З іншого боку, зростання у другому кварталі теж не очікується. Прогнозовано, що для сплеску DDoS-активності, аналогічній тій, яка спостерігалася наприкінці лютого та на початку березня, потрібне нове потрясіння світового масштабу.

Список бібліографічних посилань

1. Schwarz D., Stone-Gross B. DanaBot Launches DDoS Attack Against the Ukrainian Ministry of Defense. URL: https://www.zscaler.com/blogs/security-research/danabot-launches-ddos-attack-against-ukrainian-ministry-defense (дата звернення: 02.06.22).

2. Bonifacic I. Ukrainian mapping tool taken offline by DDoS attack. URL: https://www.engadget.com/liveuamap-ddos-213225248.html (дата звернення: 17.05.22).

3. Mingas M. Data published on Ukraine DDoS attacks. URL: https://www.capacitymedia.com/article/29w6ghrh06rwvjbwsg35s/news/scale-of-ddos-attacks-on-ukraine-confirmed (дата звернення: 24.05.22).

4. Burgess M. Ukraine's Volunteer 'IT Army' Is Hacking in Uncharted Territory. URL: https://www.wired.com/story/ukraine-it-army-russia-war-cyberattacks-ddos/ (дата звернення: 02.06.22).

Одержано 09.06.2022