НІСД НАЦІОНАЛЬНИЙ ІНСТИТУТ СТРАТЕГІЧНИХ ДОСЛІДЖЕНЬ NATIONAL INSTITUTE FOR STRATEGIC STUDIES NISS

ЦЕНТР БЕЗПЕКОВИХ ДОСЛІДЖЕНЬ
CENTER FOR SECURITY STUDIES

Огляд російських кібератак проти України

Д. Дубов, *д-р. політ. наук, с.н.с., завідувач відділу інформаційної безпеки та кібербезпеки центру безпекових досліджень*

27 квітня 2022 р. компанія Microsoft оприлюднила підготовлений її підрозділом з кібербезпеки (Digital Security Unit) спеціальний звіт з оглядом російської кіберактивності під час широкомасштабної збройної агресії проти України[1]. Це результат співпраці Microsoft з представниками українських державних установ, що опікуються питаннями кібербезпеки, та українського приватного сектора.

Згідно з матеріалами документа діяльність російських хакерів переважно спрямовано на компрометацію об'єктів у всій Україні. Такі дії здебільшого реалізують у дві фази:

- фішингові атаки з метою отримати доступ до внутрішніх систем цілей, а після цього
- зосередження на знищенні (чи модифікуванні) даних або проведення кібершпигунських операцій.

Наголошено, що в період з 23 лютого по 8 квітня 2022 р. зафіксовано щонайменше 40 результативних кібератак, унаслідок яких знищено файли в сотнях систем десятків українських організацій. Для цього використано принаймні 8 різних сімейств вірусів, які дають змогу перезаписувати та видаляти дані, виводити з ладу комп'ютери та навіть впливати на системи управління промисловими процесами (*Industrial Control Systems*). 40 % деструктивних атак спрямовано на об'єкти критичної інфраструктури (ОКІ), що могло мати опосередкований негативний вплив на уряд, військову сферу, економіку та громадян. 32 % інцидентів стосувались українських державних установ на національному, регіональному та місцевому рівнях.

Microsoft відзначає, що ворожі хакерські угруповання активно адаптуються до умов ведення протиборства, швидко модифікуючи віруси для ускладнення їх виявлення. Наголошено, що коли зловмисники зможуть підтримувати такий темп адаптування, то в міру розвитку конфлікту буде виявлено дедалі руйнівніше шкідливе програмне забезпечення.

Американська компанія ідентифікувала хакерські групи, що пов'язані з усіма трьома ключовими безпековими структурами РФ:

- ФСБ (ACTINIUM/Gamaredon, Unit 71330/EnergeticBear та KRYPTON/Turla);
- ГУ ГШ ЗС РФ (Unit 26165/APT 28, Unit 74455/Sandworm та DEV-0586/Ghostwriter);
- СЗР РФ (NOBELIUM/UNC2452/2652).

[1]Special Report: Ukraine. An overview of Russia's cyberattack activity in Ukraine. Microsoft Digital Security Unit. 2022. 27April. URL: https://cutt.ly/nGKYY4s

Важливим висновком звіту є те, що російські хакери готувалися до воєнної агресії проти України щонайменше з березня 2021 р. Наведено приклади такої підготовки. Так, уже з березня 2021 р. одна з груп розпочала фішингову кампанію з метою ускладнити отримання Україною міжнародної допомоги для відбиття російської агресії. У середині 2021 р. російські хакерські угруповання робили численні спроби провести кібератаки методом «атака через ланцюжок постачання» (*supply-chain attack*). Наприклад, скомпрометовано мережу ІТ-компанії, яка розробляла систему управління ресурсами для Міністерства оборони України, а також програми для організацій транспортного й комунікаційного секторів. Інша хакерська група здійснила схожі кібератаки проти ІТ-компаній, які надавали такі самі послуги державним замовникам у країнах НАТО. У серпні 2021 р. проведено фішингову кампанію для отримання доступу до акаунтів українських іноземних військових радників та гуманітарних працівників. Приблизно тоді ж російські хакери намагалися створити позиції в українських ІТ-системах ОКІ для проведення supply-chain attacks. Зокрема, скомпрометовано системи компанії Kitsoft та деяких інших постачальників послуг з метою створити позиції для кібератак проти їхніх клієнтів (нерідко – з числа ОКІ чи державних установ).

Звіт Microsoft також містить низку візуалізацій, що ілюструють часову залежність між ключовими політичними подіями навколо України та кібератаками, з якими стикнулася наша держава протягом січня – лютого 2022 р. Зазначено, що кібератаки актуалізувалися щоразу після чергових заяв російського керівництва про «ігнорування інтересів РФ». Протягом лютого – квітня 2022 р. Росія піддала кібератакам майже всі основні сектори критичної інфраструктури України, і ці напади майже завжди збігалися в часі з наземними воєнними операціями РФ. На додаток, кібератаки часто географічно збігались не лише зі спрямованістю воєнних дій ворога, а й навіть з конкретними об'єктами в регіонах України, по яких завдавались збройні удари.

Базуючись на здійсненому аналізі, фахівці Microsoft дійшли низки висновків щодо перспектив кіберпротистояння в середньостроковій та стратегічній перспективі:

- що інтенсивніше розвиватиметься конфлікт, то ймовірнішим стає використання резервних можливостей (*highly reserved capabilities*), як-от вразливості «нульового дня», атаки на ОКІ чи supply-chain attacks;
- підвищення ефективності кібердопомоги Україні може призвести до того, що російські хакери використають приступні їм вразливості «нульового дня», які згодом застосують інші зловмисні групи. Це в перспективі створить нові кіберзагрози для організацій в усьому світі;
- скоріше за все, ворожа кіберактивність зростатиме й дії російських хакерів дедалі більше концентруватимуться на телекомунікаційному секторі України, передусім – інтернет-провайдерах;
- РФ розширюватиме сферу кібероперацій, щораз частіше концентруючись на країнах, які надають всебічну допомогу Україні. Такі операції стосуватимуться не лише традиційної сфери кібершпигунства, але й кібердиверсій.

Документ також пропонує перелік типових тактик і методів зловмисної діяльності російських хакерів, надає практичні рекомендації командам кібербезпеки з метою зменшити загрози від такої деструктивної діяльності.