Кібератаки у сфері інформаційної безпеки: тенденції на євразійському просторі

Якубівська Ю.Є.
к.е.н., доцент кафедри фінансово-економічної безпеки та інтелектуальної власності Тернопільського національного економічного університету, м.Тернопіль

Особиста інформація, дані про місцезнаходження і технічні характеристики пристрїв потенційно можуть бути викрадені хакерами або ж законним чином придбані менеджерами інтернет-реклами, з метою наступного здійснення потужнішої реклами, поширення цільової стратегічно важливої інформації тощо. Як наслідок, виникає більш агресивний та шкідливіший метод під назвою «кібератака». Окремі загрозливі мобільні програми просто дублюють функціонал існуючих загроз, наприклад тих, котрі завдяки професійній роботі хакерів напряму крадуть інформацію з пристроїв.

Основними напрямками хакерської діяльності на світовому ринку у 2014 році були шпигунство і крадіжка даних, зокрема, польської енергетичної компанії, французької телекомунікаційної компанії та державних органів і адміністрації країн Західної Європи [4].

У 2014 році кібернапад було також здійснено на комп'ютери посольств, розташованих у Європі та Азії. Йдеться про посольства не менше дев'яти країн - у тому числі Німеччини, Китаю, Польщі та Бельгії, які містили конфіденційну дипломатичну інформацію. На сьогодні кібератака є нападом на урядові веб-сайти, банки, управління, підприємства та корпорації, що виступають об’єктами промислового шпигунства. Наприклад, згідно неофіційних джерел хакери отримали у 2014 році найбільшу кількість особистої інформації користувачів мережі Інтернет зі всього світу [3]: 1,2 млрд. вкрадених імен користувачів і паролів на сайти, і більш 500 млн. адрес електронної пошти. Це конфіденційна інформація, зібрана з 420 000 веб-сайтів, в тому числі великого і малого бізнесу.

Хакери орієнтувалися на «Fortune 500» («Fortune 500» є ранжуванням 500 найбільших американських компаній, класифікованих відповідно до рівня доходу). У грудні 2013 р. 40 млн. номерів кредитних карток і 70 млн. адрес, телефонів і додаткова інформація про персональні дані були вкрадені хакерами у Східній Європі [3]. У травні 2014 році бельгійський МЗС оголосило, що структура стала жертвою хакерської атаки, метою якого було отримання документів, пов'язаних з кризою в Україні: «...Міністерство закордонних справ, за допомогою військової розвідки, повідомляє, що комп'ютерна система отримала зараження вірусом, який скопіював інформацію і документи, що відносяться до питання української кризи...» - йдеться в заяві міністерства [5].

Особливо даний аспект пов’язаний з кібератаками російських хакерів на український інформаційний простір. На сьогодні Росія розглядається експертами як член так званої «Кібернетичної тріади», перебуваючи у одному ранзі разом із Китаєм та США. Саме ці країни диктують правила у кіберпросторі. У той же час Пекін і Москва поставили більший акцент на стратегії наступу, спрямованій, зокрема, на Вашингтон. Порушники кіберпростору не обмежується тільки оборонними діями, часто використовуючи активні дії хакерів у контексті здійснення як зовнішніх, так і внутрішніх атак, спрямованих проти цільових країн. Хоча інституційна структура українського бізнесу, прив’язаного до кіберпростору, не розвинена так, як, наприклад, в США, однак, Росія є однією з потенційних країн, котрі створюють загрози та активно реалізовують кібератаки в українському інформаційному середовищі.

Розглянемо детальніше парадигму формування та активності кібератак на євразійському просторі. Російське законодавство, наприклад, на виокремлює кіберпростір в якості окремого стратегічного поля інформаційної війни (поруч з повітряним, морським, наземним тощо). Замість слова «кіберпростір» використовується термін «інформаційний простір». Для Росії її кіберможливості є новим інструментом для діяльності в рамках інформаційної війни (розвідка, контррозвідка, дезінформація, пропаганда), радіоелектронної боротьби, що

порушують зв'язок та навігацію, для того щоб чинити психологічний тиск та з метою руйнування стратегічних ресурсів противника. Росія не має окремого стратегічного центру на кшталт американського «Cyber Command», хоча уже наявний план його створення в найближчому майбутньому. А відтак, основне російське вчення базується на трьох базових документах [2]:

- «Доктрина інформаційної безпеки» з 2000 року;
- «Конвенція Міжнародної інформаційної безпеки»;
- «Комплексний погляд на діяльність збройних сил Російської Федерації в інформаційному просторі» 2011 року.

Перший визначає національні інтереси Росії в інформаційній сфері, говорить про ризики та можливості, які супроводжують технологічний розвиток. Другий - це збір пропозицій для контролю діяльності в інформаційній сфері (у тому числі таких питань, що стосуються надання населенню доступу до Інтернет-ресурсів). В офіційному документі, підготовленому міністерством оборони Російської Федерації, наявні схожі положення до тих, що містяться в стратегії Сполучених Штатів Америки. Вона зосереджена на трьох основних пунктах:

- моніторинг кіберпростору, пошук загроз;
- запобігання поширенню загроз;
- усунення загроз.

На перший погляд увагу привертає відсутність будь-якої згадки про активні дії, що виконуються у кіберпросторі. Тим не менш, на практиці для такої діяльності делегуються відповідальні хакери, так звані «кіберкозаки». Російські хакери мають дуже довгу історію діяльності у кіберпросторі. Перший прояв кібершпигунства належав саме їм, коли у 1989 році, було викрадено секретні дані з американського Держдепартаменту, які згодом опинилися у руках КДБ. Особливістю російського інтернет-спільноти є наявність великої кількості незалежних груп хакерів, які іноді співпрацюють з урядом. Діяльність більшості з них обмежується найпростішими атаками, але є водночас підрозділи, котрі

стали легендою у середовищі хакерів, як наприклад, хакер «Hell», який підозрювався в крадіжці інформації, чи хакер на прізвисько «Север», котрого називали королем спаму. Вважається, що більшість їхньої діяльності підтримується і координується російською владою [2]. Ще однією відмінною особливістю є безліч форумів в Інтернеті, де початківці хакери можуть знайти інформацію і програми, необхідні для здійснення нападів в кіберпросторі. Ці платформи також використовуються вже для більш скоординованих та масштабніших атак.

З початку 90-х років і поширенням Інтернету, на євразійському просторі домінує централістичний підхід країни до питання участі влади у процесі розширення і поглиблення контролю над мережевими ресурсами. Федеральна служба безпеки для моніторингу електронної пошти та інших повідомлень використовує програму «СОРМ». За словами представників міністерства це допомагає в боротьбі з тероризмом і дозволяє виявляти іноземних розвідників У нещодавно опублікованому звіті американської компанії «CrowdStrike» про безпеку в Інтернеті вказано на групу так званих російських «енергетичних ведмедів», як активного фрагмента шпигунства, діяльність яких спрямована на незаконне придбання інформації про діяльність західних енергетичних компаній [2].

Як відомо, Росія виступає за контроль переданих та отриманих даних по мережі Інтернет, а також цензури, вказуючи на загрозу національній безпеці країни. Така позиція щодо свободи інформації в кіберпросторі стала причиною не підписувати Будапештської конвенції про боротьбу з кіберзлочинністю, зважаючи на можливість доступу до даних, розташованих на території Росії державами-учасницями Конвенції без її згоди, а також потенційної інтервенцією іноземних розвідок. Незважаючи на вказані фактори, саме Росія вважається одним з найактивніших порушників кіберпростору.

Купівля-продаж конфіденційної особистої інформації з кожним роком стає все більш і більш прибутковим бізнесом. Проблемою є той факт,що люди, як

правило, використовують однакові паролі для різних сайтів, що спрощує процес крадіжки даних з веб-сайтів, де може зберігатися цінна інформація, як наприклад, номери банківських рахунків або рахунків в брокерських будинках.

Проаналізувавши тенденції розвитку кіберзлочинності на світовому рівні [1], а також розглянувши міжнародні прояви активності кібернетичної тріади, можемо дійти висновку про зростаючу роль російської сторони у вищезазначеному процесі, адже її діяльність в кіберпросторі дуже схожа на постійно здійснювану Китаєм, і скерована проти своїх опонентів, як зовнішніх, так і внутрішніх. Однак відмінністю, як зазначалося раніше [1], є те, що Пекін ставить акцент у своїх діях на активному промисловому шпигунстві, і менш зосереджений на аспекті кібервійни.

Література:

1. Якубівська Ю.Є. Світові тенденції розвитку кіберзлочинності / Ю.Є. Якубівська // Зовнішня торгівля: право та економіка. Науковий журнал. - № 5-6 / 2014. -К.: УДУФМТ,2014.

2. Rosyjski cyberatak na Ukrainę : [Źródło elektroniczne] /red. P. Łuczuk // Strefa Wolnego Slowa, 2014. – Dostęp : http://niezalezna.pl/58139-rosyjski-cyberatak-na-ukraine-jak-deklaracja-wojny

3. Rosyjscy hakerzy zaatakowali NATO. Szpiegowali także firmę energetyczną z Polski : [Źródło elektroniczne]. – Dostęp : http://niezalezna.pl/60405-rosyjscy-hakerzy-zaatakowali-nato-szpiegowali-takze-firme-energetyczna-z-polski

4. Tajemniczy cyberatak w Belgii : [Źródło elektroniczne] /red. P. Łuczuk // Strefa Wolnego Słowa, 2014. – Dostęp : http://niezalezna.pl/55043-tajemniczy-cyberatak-w-belgii-sluzby-putina-chcialy-wykrasc-dokumenty-ws-ukrainy

5. Kozlowski A. Cyberwojownicy Kremlia: [Źródło elektroniczne] / Andrzej Kozlowski // Andrzej Kozłowski // Stowarzyszenia Europejskie Centrum Analiz, 2014. – Dostęp : http://geopolityka.org/analizy/2836-andrzej-kozlowski-cyberwojownicy-kremla