

СИТЕМА DAAR ТА МОНІТОРИНГ ЗЛОВЖИВАНЬ У ГАЛУЗІ ДОМЕННИХ ІМЕН

Влітку 2018 року Інтернет-корпорація з присвоєння імен і номерів (ICANN) анонсувала публікацію матеріалу, що містить опис методології DAAR, тобто платформи звітності про випадки зловживання доменами, підкріплений двома досить критичними і повноцінними аналізами експертів у даній галузі. Такий документ є важливим і заслуговує уваги, адже слугуватиме в майбутньому для прийняття адекватних та своєчасних рішень в галузі розробки політики та правил щодо доменної індустрії.

Перш за все слід розуміти, що DAAR (Domain Abuse Activity Reporting, ДААР) - це система, яку ICANN застосовує з ціллю моніторингу зловживань і незаконних дій щодо доменів та їх реєстрації на верхньому рівні (мова про так звані TLD, тобто доменні імена верхнього рівня). Дана система на постійній основі займається збором даних відносно реєстрації та виникнення загроз безпеці із багатьох каналів отримання такої інформації. Саме на основі неї експерти корпорації визначають і повідомляють про використання доменів в таких нелегальних справах як розповсюдження шкідливих програм, фішинг, розсилка спаму тощо [1].

Місія корпорації ICANN, створеної у 1998 р. як некомерційна громадська корпорація, полягає у забезпеченні "стабільного, безпечного та єдиного глобального інтернету". Саме даний орган займається координацією унікальних ідентифікаторів відомих нам як доменні імена [2].

Основна ж мета ДААР - це своєчасне інформування ICANN-спільноти про активність, яка може нести загрозу безпеці в рамках мережевих операцій.

Для підвищення довіри до ДААР ICANN залучила двох незалежних аналітиків, Маркуса Ранума та Джона Бамбенека до вироблення всебічного аналітичного матеріалу (статті), який присвячено методології. Також експерти висловили свої думки про дані по загрозам, і засвідчили надійність мереж отримання даних, які ICANN вирішила використовувати в цьому проекті.

Marcus J. Ranum у своєму аналізі резюмував наступне:

1. Система ДААР достовірно вираховує загрози безпеці і може застосовуватися з упевненістю. Аналітик вказує на те, що Система являє собою "історичний набір джерел даних" тобто складається із метаданих DNS (Domain Name System) та даних класифікації сторонніх виробників.

Тобто точність вказаного набору буде настільки ж високою, як і у вказаних джерел даних. Але і самих таких джерел є достатньо, навіть без ДААР, а таому Система буде радше застосовуватися як якісний історичний довідник для спільноти, дослідників і реєстраторів.

2. Відповідь на питання про наявність загрози безпеці інтернет-користувачам при використанні ними спам-доменів є стверджувальною. Адже такі доменні імена не тільки справляють марне надмірне навантаження на інфраструктуру DNS. Вони сприяють і розбудові інфраструктури спаму, яка є популярним засобом атаки. Недолік ДААР полягає у тому, що вона не пояснює наступне: ці великі потоки несуттєвих атак на основі спаму покликані відволікти увагу від більш суттєвих атак [3, с. 8-10].

Свій експертний висновок надав і John Vambenek:

1. Необхідно створити оновлений документ (наприклад, на базі вже існуючої Білої книги або у якості окремого документу), який буде вміщувати конкретну і повну інформацію сприводу того, що включено до ДААР. Адже на сьогодні вказана Біла книга є застарілою і не відповідає сучасним реаліям.

2. Важливо виявляти та занотовувати (в інтерфейсі) недоступність протягом тривалого проміжку часу доменних імен.

3. Слід послідовно проводити переоцінювання існування джерел даних із відкритим вихідним кодом, адже вони можуть допомогти підвищити прозорість реальних зловживань, які стосуються доменних імен.

4. Слід також видалити додаток Mozilla Firefox AdBlock, про що, доречі, згадувалося у Білій книзі.

5. Важливо також видалити рекламні веб-адреси хоча б з каналів даних, в ідеалі - повністю видалити їх.

6. Слід приділяти увагу можливості надання «ваги» доменним іменам, що існують протягом досить тривалого проміжку часу. Адже вони зазвичай варті довіри.

7. Головне – це постійно контролювати кількість доменів, щодо яких важко встановити реєстратора через проблеми з доступом до Whois [4, с. 5-9, 36]. (Це система, яка покликана допомогти перевірити доменне ім'я на зайнятість, діагностувати проблеми при реєстрації, але головне її призначення полягає у наданні інформації про реальну фізичну особу, місце ведення діяльності організації, а також контактної інформації інтернет-продавця або компанії, або будь-який інший організації з присутністю в інтернеті [5]).

Отже, Domain Abuse Activity Reporting — є важливим засобом надання ICANN-спільноті надійних даних, що дозволить робити аналіз загроз безпеці існування DNS. ДААР є дійсно важливою і корисною системою, що допоможе і дослідникам мережі інтернет та зловживань доменами, і

розробникам відповідних політик у їх роботі. Можна сказати, що сьогодні ДААР дійсно працює, тим не менш слід урахувати аналіз, проведений експертами, задля корегування системи та її покращення.

Література

1. Domain Abuse Activity Reporting System // Internet Corporation for Assigned Names and Numbers. URL: <https://www.icann.org/icann-acronyms-and-terms/en/G0068> (дата звернення: 23.01.2019).

2. What is ICANN Policy? // Internet Corporation for Assigned Names and Numbers. URL: https://www.icann.org/policy#what_is_policy (дата звернення: 20.01.2019).

3. Ranum M. Review of The Domain Abuse Activity Reporting system (DAAR) and methodology / Marcus J. Ranum. – Los Angeles: ICANN, 2018. – 18 с.

4. Bambenek J. DAAR Validation Report / John Bambenek. – Los Angeles: ICANN, 2018. – 18 с.

5. About WHOIS // Internet Corporation for Assigned Names and Numbers. URL: <https://whois.icann.org/en/about-whois> (дата звернення: 25.01.2019).

УДК 349.2:316.647.82-053 (043.2)

Хоцяновська Н. Ф., старший викладач,
Національний авіаційний університет, м. Київ, Україна,
Хом'яченко С. І., к.ю.н., доцент,
Національний університет біоресурсів
і природокористування України, м. Київ, Україна

ПРОБЛЕМИ УДОСКОНАЛЕННЯ ЗАКОНОДАВСТВА ІЗ ЗАХИСТУ ВІД ДИСКРИМІНАЦІЇ ЗА ВІКОМ У СФЕРІ ПРАЦІ

Україна перебуває у стані демографічної кризи: населення України старішає. Причинами цього явища є недостатній рівень народжуваності, трудова міграція працездатної молоді, участь молоді у захисті України під час АТО, тощо.

Законодавство України декларує захист від будь-якої дискримінації в сфері праці та зайнятості населення. В тому числі стосовно: статі, раси, національності, політичних поглядів, соціального стану і віку особи. В той же час практика свідчить про недостатній захист від дискримінації. Певні положення, які містять дискримінаційні ознаки можна знайти у більшості оголошень про вакансії. Серед найбільш розповсюджених є обмеження за віком при висуненні вимог до кандидатів на посаду. Така дискримінація не обмежується необґрунтованою відмовою у прийнятті на роботу, а включає в себе такі випадки, як: відмова у підвищенні по службі, необґрунтовано низький рівень заробітної плати, вищий порівняно з іншими працівниками рівень навантаження, незаконне звільнення та ін.