ISSN 2519-2310 (Online)

КОМП'ЮТЕРНІ НАУКИ ТА КІБЕРБЕЗПЕКА, 2024, № 1 (25)

COMPUTER SCIENCE AND CYBERSECURITY, 2024, Iss. 1 (25)

DOI: https://doi.org/10.26565/2519-2310-2024-1-01
УДК 004.056.5

УЗАГАЛЬНЕННЯ НАПРЯМІВ ФІЛЬТРАЦІЇ DNS ТРАФІКУ ЯК СКЛАДОВОЇ БЕЗПЕКИ СУЧАСНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Данило Чепель[1], студент магістратури спеціальності «Комп'ютерні системи та мережі», кафедра захисту інформаційних систем та технологій, e-mail: dan4epel@gmail.com, ORCID: https://orcid.org/0009-0009-7449-8095

Сергій Малахов[1], доктор філософії, старший науковий співробітник, кафедра комп'ютерних наук, e-mail: malakhov@karazin.ua, ORCID: https://orcid.org/0000-0001-8826-1616

[1]*Харківський національний університет імені В.Н. Каразіна, майдан Свободи, 4, Харків, 61022, Україна*

Рукопис надійшов 21 квітня 2024 р. Отримано після рецензування 21 травня 2024 р. Прийнято 23 червня 2024 р.

Анотація: В роботі проведено аналіз джерел, стосовно методів і технологій DNS (Domain Name System) фільтрації трафіку. Визначені п'ять основних напрямків, які активно використовуються для підвищення безпеки на рівні DNS. Усі розглянуті технології пропонують підвищення якості DNS фільтрації. Підкреслено, що одночасне комбінування різних підходів може підвищити загальний рівень безпеки. Узагальнення результатів досліджень з проблематики безпеки DNS трафіку, вказує на існування певних проблем у якості використовуваних каналів розвідки загроз. Саме тому впровадження AI та LM технологій, повинно посилити «глибину» екстракції корисної інформації про актуальні загрози. Звернено увагу на те, що розгляд питань ІБ, слід вести виключно у розрізі недопущення диспаритету можливостей штучного інтелекту (AI) на користь протиборчої сторони (тобто зловмисників). Практично це означає, що майбутні системи фільтрації DNS, повинні широко впроваджувати останні напрацювання на рівні стеку VR, AI, LM та DL технологій. Це особливо важливо в межах протидії алгоритмам генерації доменів (DGA - Domain Generation Algorithm) та поширення ботнетів. Наголошено на специфіку питань забезпечення консенсусу безпеки та продуктивності діючих інформаційно-комунікаційних систем (ІКС) при впровадженні в них інструментів шифрування DNS. В якості основної проблеми, пов'язаної з шифруванням DNS трафіку, підкреслена можливість його використання з боку зловмисників, як інструменту приховування їх деструктивної діяльності (фішинг, спам та інші).

Ключові слова: *DNS, DGA, RPZ, інформаційна безпека, загрози безпеки, фільтрація трафіку, ботнет*

Як цитувати: Чепель Д., Малахов С.. Узагальнення напрямів фільтрації DNS трафіку як складової безпеки сучасних інформаційних систем. *Комп'ютерні науки та кібербезпека.* 2024; № 1(25): С. 6–21. https://doi.org/10.26565/2519-2310-2024-1-01

In cites: Chepel D., Malakhov S. (2024). Summary of DNS traffic filtering trends as a component of modern information systems security. *Computer Science and Cybersecurity.* 1(25): 6–21. https://doi.org/10.26565/2519-2310-2024-1-01 (in Ukrainian)

1. Вступ

Технологія зіставлення доменних імен - *Domain Name System* (*DNS*) із їх числовими IP-адресами, є найважливішим механізмом сучасного Інтернет, виступаючи в якості умовного «посередника», який перетворює «зручні» для користувачів доменні імена в їх IP-адреси [1]. Система із розгалужених *DNS* серверів не тільки спрощує процес навігації в Інтернеті але й забезпечує ефективне і точне з'єднання, як між користувачами, так і «місцями призначення» їх пошукових запитів (інформаційними ресурсами) в Інтернеті. Нажаль, сучасні мережеві зловмисники знаходять способи використання *DNS* служб для реалізації різних варіантів атак, причому як окремо, так і в якості складового елементу при реалізації багатоходових - інтегрованих атак [2-3]. Тому, на поточний момент фільтрація *DNS* трафіку є невід'ємною складовою заходів з інформаційної безпеки (ІБ) для переважної більшості сучасних інформаційно-комунікаційних систем (ІКС) Інструменти управління й фільтрації *DNS* забезпечують контроль доступу до веб-ресурсів, захист від шкідливого програмного забезпечення (ПЗ) і надає можливість гнучкого впровадження потрібних політик безпеки на рівні мережі (*для моделі OSI*).

Метою роботи є стислий огляд відомих напрямів використання *DNS* технології, що відіграють важливу роль у забезпеченні ІБ сучасних ІКС.

Ключовими питаннями, що розглядаються, є: - канали розвідки загроз ІБ; - шифрування *DNS* трафіку; - синтез та управління зонами політик реагування на основі *DNS*; - особливості алгоритмів генерації фіктивних доменів та виявлення активності ботнетів (серверів управління ботнетами).

2. Основна частина

2.1. Основні вектори застосувань технології DNS при вирішенні питань ІБ

Служба/Система DNS. Ця служба відіграє ключову роль у функціонуванні та масштабованості мережі Інтернет, оскільки майже кожен інший протокол залежить від вирішення домену *DNS* для своєї коректної роботи. *DNS* є одним з небагатьох протоколів, що складають умовне «ядро» Інтернету. В загальному випадку, *DNS* використовується переважно для перетворення «зручних» для читання людиною доменних імен у їх цифрові IP-адреси. Для пошуку потрібного мережевого домену клієнт/користувач надсилає *DNS*-запит до відповідного рекурсивного *DNS* серверу, який, зазвичай, надається поточним інтернет провайдером та має можливості розпізнавання і кешування (тимчасового зберігання) доменних імен. У випадку, коли використовуваний сервер доменних імен не має у своєму кеші необхідних відомостей, то він звертається до кількох інших – «зовнішніх» *DNS* серверів, які зберігають розподілену базу даних доменних імен та їх відповідні IP-адреси. Таким чином, у пошуках потрібного мережевого домену, кожний умовний *DNS* запит транслюється через певні сегменти ієрархічної мережі із довірених серверів імен, доки не знайде потрібну відповідь (*зіставлення*) та не надішле її клієнту (*користувачеві*). Отримавши потрібну IP-адресу, шукач необхідного інформаційного ресурсу може використовувати її для підключення до хосту призначення [1].

DNS-фільтрація. *DNS*-фільтрація мережевого трафіку є елементом проактивної стратегії кіберзахисту, що діє на рівні системи доменних імен для контролю та управління доступом до Інтернету в мережі. Використовуючи *DNS*-фільтрацію, організації можуть впроваджувати потрібні політики безпеки, які обмежують доступ до певних веб-сайтів та/чи категорій контенту, які вважаються такими, що не відповідають корпоративним вимогам. Цей механізм фільтрації працює шляхом перехоплення *DNS*-запитів і їх наступного порівняння із попередньо визначеними реєстрами дозволених чи заблокованих доменних імен та IP-адрес. У разі наявності відповідного ресурсу в стоп листі, *DNS*-фільтр блокує таке з'єднання.

DNS-фільтрація надає організаціям і окремим мережевим користувачам кілька помітних переваг, зокрема підвищення поточного рівня кібербезпеки шляхом запобігання відвідуванню потенційно зловмисних та/чи небажаних інформаційних ресурсів (наприклад, як функція «батьківський контроль»). Така фільтрація джерел контенту допомагає забезпечити дотримання відомчих нормативних вимог, обмежуючі доступ до сайтів, які не відповідають політиці безпеки компанії/установи. Крім того, *DNS*-фільтрація сприяє підвищенню продуктивності персоналу, обмежуючи його доступ до інформаційних ресурсів, що не пов’язані з виконанням їх функціональних обов’язків, та зменшує навантаження на корпоративну мережу, шляхом адміністрування небажаного ресурсоємного трафіку [4]. Також слід підкреслити, що делегування функцій *DNS*-фільтрації на довірені зовнішні ресурси/сервіси, дозволяє в значній мірі позбутися необхідності регулярного перевірки й оновлення стану відповідних реєстрів доступу силами корпоративних фахівців та забезпечити більшу функціональну стійкість корпоративної інфраструктури в разі відповідних атак.

Канали розвідки загроз. Канали розвідки загроз є важливим компонентом для реалізації сучасних стратегій ІБ (*див. рис.1*). Їх використання, в режимі реального часу, забезпечує корпоративних фахівців з ІБ відомостями про нові загрози, вразливості і діяльність кіберзловмисників [2-3]. Вони функціонують шляхом постійного збору та узагальнення даних з різних джерел для виявлення потенційних кіберзагроз і вразливостей [5-6]. Зазвичай ці канали містять індикатори компрометації, наприклад, такі як: - «шкідливі» IP-адреси, доменні імена, хеші файлів та типові шаблони/сценарії підозрілої поведінки [3, 7].

Інтеграція каналів розвідки загроз в інструменти та корпоративні системи ІБ дозволяє організаціям автоматично блокувати відомі зловмисні чи скомпрометовані джерела та ранжувати пріоритетність сповіщень системи безпеки на основі відомостей стосовно актуальності інформації та серйозності наслідків. Це дає змогу приймати обґрунтовані рішення, покращувати час реагування на інциденти та покращити загальну систему ІБ. Використовуючи канали розвідки поточних загроз, сучасні організації можуть покращити показник поінформованості про стан актуальних загроз та завчасно вживати профілактичних заходів для усунення відповідних вразливостей власних ІКС ще до того, як ними спробують скористатися зловмисники.

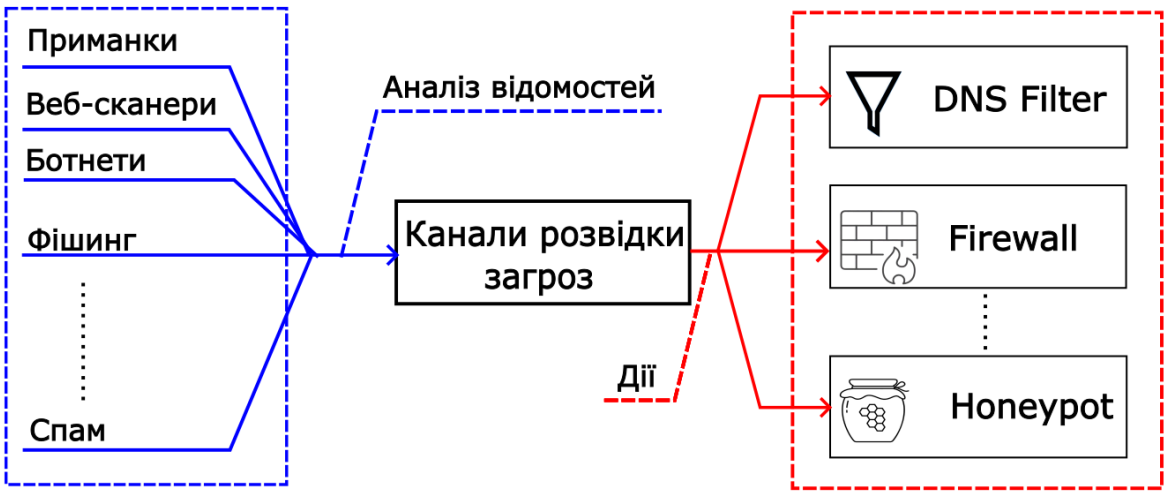

Рис. 1 - Сутність використання каналів розвідки загроз ІБ
Fig. 1 - The essence of using threat intelligence feeds

Постійно співвідносячи дані внутрішнього моніторингу безпеки із зовнішніми каналами розвідки загроз, сучасні організації можуть виявляти приховані загрози та превентивно їм протидіяти [7-9]. Такий проактивний підхід до кібербезпеки допомагає випереджати кіберзлочинців, мінімізувати вплив інцидентів безпеки та ефективно захищати конфіденційні дані й критично важливі активи [10].

Сервери управління ботнетом. Сервер управління ботнет системи являє собою централізований (*ведучій*) сервер, що використовується зловмисником для дистанційного управління скомпрометованими мережами та/чи пристроями, відомих, як боти або бот-мережі. Командно-контрольні сервери ботнетів (*див. рис.2*) відіграють ключову роль в організації зловмисних дій, таких як проведення розподілених атак на відмову в обслуговуванні (*DDoS-атак, в т.ч. DNS amplification attack*), *DNS* та *NTP Spoofing*, розсилання спаму, здійснення шахрайства, поширення зловмисного ПЗ тощо [3, 11-12].

Аналізуючи поточні властивості мережевого трафіку і таким чином ідентифікуючи роботу відповідних серверів, засоби безпеки можуть протидіяти впливу ботнетів, своєчасно парируючи їх зловмисну дію. Переваги виявлення такого трафіку передбачають зменшення ризику атак з боку ботнетів, захист мережевих пристроїв від їх компрометації з використанням експлойтів та підтримку безпечного корпоративного середовища [5-7, 13].

Шифрування DNS трафіку. Шифрування *DNS* трафіку, зокрема *DNS-over-TLS* (*DoT*), *DNS-over-HTTPS* (*DoH*) та *DNS-over-QUIC* (*DoQ*), відіграє важливу роль у підвищенні безпеки та ефективності контролю *DNS* запитів [14]. Цей процес перетворює інформацію *DNS* трафіку у зашифрований формат, що гарантує можливість декодування інформації лише довіреними сторонами, такими як *DNS*-клієнт і сервери *DNS* провайдера.

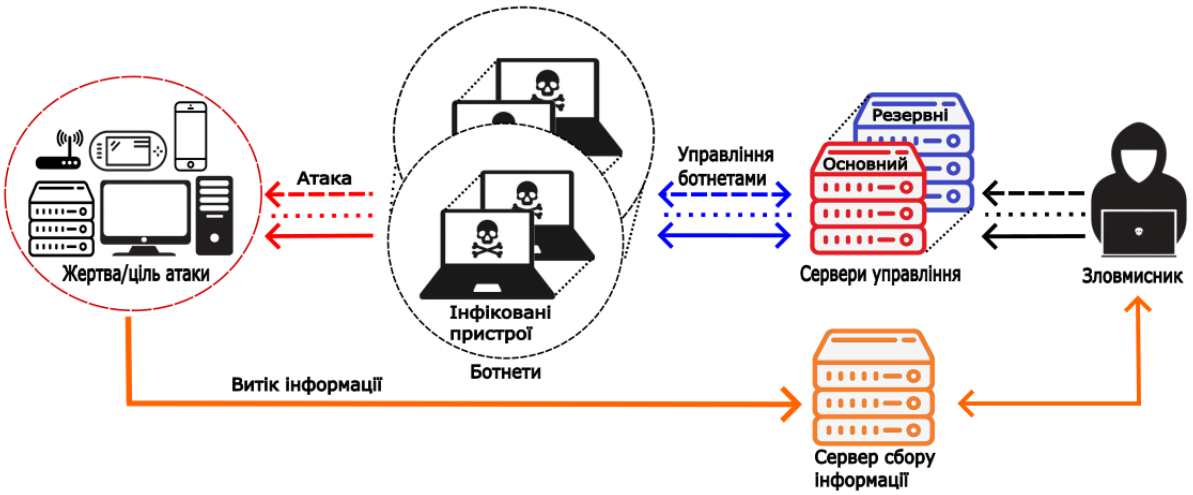

Рис. 2 - Архітектура ботнета (авторська розробка)
Fig. 2 - Architecture of a botnet (author's development)

Шифрування зменшує ризик атак на *DNS* трафік і маніпуляції з даними цих запитів, знижуючи ймовірність неавторизованих змін у *DNS* записах. Крім того, існуючі протоколи шифрування *DNS* підвищують рівень цілісності й конфіденційності відповідного трафіку, протидіючи несанкціонованому моніторингу та відстеженню відомостей *DNS*-запитів. Процес шифрування *DNS* трафіку, в цілому, сприяє підвищенню конфіденційності та анонімності онлайн дій користувачів, однак на цьому шляху є і певні складнощі. Наприклад, складність відстеження вмісту зашифрованого *DoH* трафіку, з боку адміну безпеки, свідчить про те, що

аналіз мережевих *DoH* з'єднань з метою виявлення потенційного шкідливого трафіку (*наприклад з боку зовнішніх командно-контрольних серверів умовних бот-систем [13]*), є актуальним напрямом для його подальшого аналізу [14].

Зони політики реагування. *Response Policy Zone* (*RPZ*) – це механізм, який використовується при фільтрації *DNS* для визначення діючих локальних політик у стандартизованому форматі та завантаження/оновлення політик із інших, «зовнішніх» джерел. Використовуючи *RPZ*, сучасні організації можуть оперативно контролювати, які запити можуть обробляти їхні сервери *DNS*, а які ні. Це дозволяє оперативно блокувати шкідливі домени й ресурси або виконувати інші дії на основі попередньо встановлених політик безпеки. Політики безпеки формалізуються у вигляді файлів складених для відповідних зон *DNS* (*див. рис.3*), котрі формуються за визначеними корпоративними критеріями та/чи діючими нормами мережевої поведінки [15] для основних груп користувачів інформаційних послуг компанії/установи. Цей процес в рівній мірі відноситься, як для власного персоналу, так і користувачів основних послуг компанії.

Впровадження концепції *RPZ* полегшує, масштабування, використання й оновлення актуальних зон безпеки. Парадигма *RPZ* передбачає їх спільне застосування між декількома *DNS*-серверами (через передачу зон), що дозволяє оперативно транслювати дані політики за допомогою звичайних протоколів *DNS* [14]. Політики *RPZ* складаються з відповідних поведінкових (логічних) тригерів та дій. Тригери визначають, коли потрібно застосувати ту чи іншу політику (*тобто декларують певні мережеві умови/обставини*), а дії, відповідно, вказують, які саме процедури слід виконати в даному разі.

Впровадження *RPZ* забезпечує уніфікацію, масштабованість і гнучкість управління політиками *DNS*. Це підвищує безпеку і цілісність налаштувань фільтрації *DNS* трафіку, а також дозволяє організаціям визначати й застосовувати власні політики для адміністрування сервісу *DNS* [16].

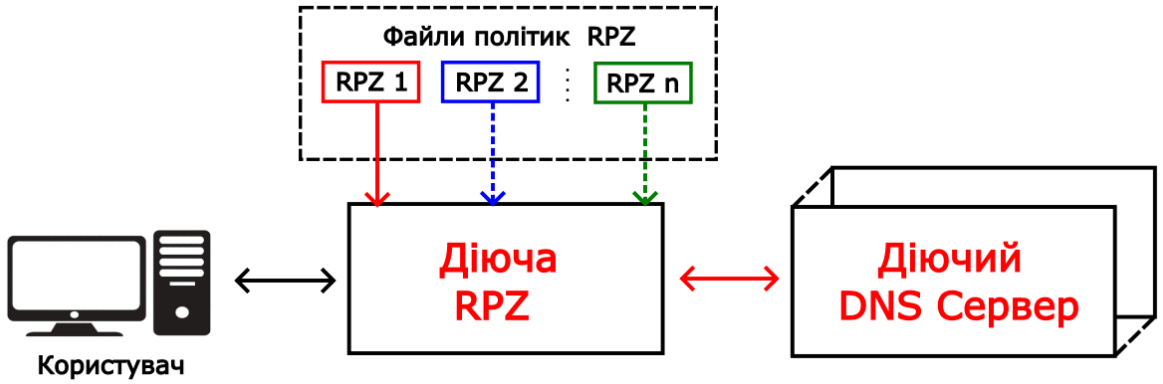

Рис. 3 - Сутність використання RPZ (авторська розробка)
Fig. 3 - The essence of using RPZ (author's development)

Алгоритми генерації доменів. *Domain Generation Algorithm* (*DGA*) – це алгоритми, які використовуються кіберзловмисниками для генерування великої кількості доменних імен, що слугують умовними точками «зустрічі» в мережі між скомпрометованими пристроями та серверами управління зловмисника. В цьому випадку (*див. рис.4*), скомпрометовані/атаковані комп'ютери й інше мережеве устаткування намагаються встановити зв'язок (*DNS spoofing*) з цими згенерованими доменними іменами, щоб отримати від них «оновлення» чи інші команди з

боку атакуючої сторони. Ці алгоритми створені для періодичного генерування значної кількості доменних імен, що помітно ускладнює боротьбу з ботнетами. Таким чином *DGA* використовуються для приховування фактичного розташування командно-контрольних серверів ботнетів серед великої кількості потенційно легітимних адрес, що значно ускладнює пошук та блокування (згодом і видалення) цих доменів. В широкому сенсі *DGA*, за своєю парадигмою, є своєрідним аналогом атак типу *DNS amplification* [12].

Виявлення злочинних доменних імен, що синтезовані *DGA*, є складної задачею через їх великі обсяги відповідної генерації та випадковий характер цих процесів. Однак, залучення технологій штучного інтелекту і машинного навчання (*AI/LM*), та впровадження методів глибокого навчання, потенційно демонструють високі показники в ідентифікації злочинних *DGA* [17].

2.2. Бліц-огляд робіт, щодо практичних реалізацій механізмів DNS-фільтрації

Спираючись на аналіз ряду відомих робіт, проведемо узагальнення основних відомостей, стосовно особливостей взаємозв'язку технології *DNS* та питань безпеки сучасних ІКС. Результати такого огляду систематизовано у відповідності до запропонованої в п.п. 2.1 послідовності розгляду для найбільш поширених напрямів застосувань інструментів та методів *DNS*-фільтрації.

Канали розвідки загроз. В роботі [18] розглянуто проблематику «пасивних» *DNS*-потоків для отримання актуальної інформації про потенційні загрози безпеки. Автор роботи фокусує увагу на ідентифікації підозрілих і зловмисних доменів, виявленню зловживань *DNS* та їх аномалій, підкреслюючи важливість перехресної перевірки даних з іншими джерелами інформації про кіберзагрози. Акцентовано необхідність ретельного аналізу *DNS*-трафіку для виявлення різноманітних кіберзлочинних дій, таких як ботнети, спам і фішинг. Крім того, дослідження автора зосереджене на розробці та впровадженні масштабованої методики «пасивного» аналізу *DNS*, яка забезпечує своєчасне виявлення актуальних загроз ІБ.

Рис. 4 - Інфографіка порядку дій зловмисника при використанні DGA (авторська розробка)
Fig. 4 - Infographic of the attacker's actions during the use of DGA (author's development)

Проблематика визначення «якості» каналів розвідки загроз безпеки є вкрай актуальним та доволі складним завданням, оскільки їх важко порівнювати між собою. Так наприклад, у роботі [19] її автором розглядається методологія вимірювання надійності та якості безкоштовних каналів розвідки про кіберзагрози з відкритим кодом. У цьому дослідженні дані аналізуються за допомогою різних метрик, наприклад: – обсягом даних, швидкістю змін, географічним розподілом та збігами між різними каналами.

Підкреслено, що різні канали зосереджені на різних питаннях, що ускладнює прямі порівняння. Автором стверджується, що остаточного методу визначення найкращого каналу поки не існує та можна лише зробити певні висновки, стосовно їх якості. Дослідження підкреслює складність оцінки безкоштовних каналів розвідки загроз та потребу в більш надійних та достовірних інструментах [19].

Робота [20] також розглядає проблематику оцінки якості каналів розвідки і пропонує всебічний аналіз каналів розвідки загроз. Автори цієї роботи звертають увагу на необхідність та важливість емпіричних оцінок у цій галузі. Дослідження представляє набір показників для оцінки каналів розвідки загроз, включаючи такі як: – обсяг, диференціальний внесок, унікальний внесок, затримку, точність, охоплення та ін.. Дослідивши 47 каналів із різними IP-адресами та 8 каналів із хешами файлів зловмисного ПЗ, автори роботи виявили значні обмеження в охопленні та точності наявних даних розвідки загроз. Це вказує на високий ступінь унікальності та помилкових узагальнень (прогнозів) для різних каналів. В цілому, ця робота надає обґрунтовану методологію для оцінки каналів розвідки загроз та підкреслює важливість постійного розвитку методів їх оцінки [20].

Виявлення активності ботнетів. Дослідницька група авторів роботи [21] пропонує огляд джерел, який включає в себе вичерпний аналіз методів виявлення ботнетів на основі аналізу *DNS* трафіку. Робота звертає увагу на проблему ботнетів та пов'язаних з ними загроз ІБ. Автори класифікують та порівнюють кілька підходів, що використовують різні властивості *DNS* трафіку, такі як: – зміна домену, лексичні характеристики доменних імен і шаблони в запитах та *DNS* відповідях. В роботі аналізуються сильні й слабкі сторони для відповідних підходів. Зазначено, що методи виявлення на основі *DNS* мають переваги перед методами на основі хосту, оскільки вони можуть надати більш широке уявлення про мережеву активність і уникнути деяких обмежень, пов'язаних з розгортанням систем моніторингу в мережі. У роботі також обговорюються обмеження існуючих підходів, такі як відсутність стандартних метрик і показників продуктивності та підкреслено потреба в нових методологіях виявлення для протидії поширенню загроз ботнетів [21].

В роботі [22] розглядаються різні методології аналізу поведінки ботів та ботнетів, включаючи статистичний аналіз і вимірювання трафіку та наголошується на важливість комплексного підходу до виявлення ботнетів. На думку авторів для ряду попередніх робіт була притаманна деяка невизначеність, насамперед в частині, що підкреслює складність пошуку всіх типів ботнетів через складність моделі їх поведінки. Саме тому дана робота пропонує новий механізм виявлення ботнетів, заснований на моніторингу трафіку *DNS* для виявлення групової активності розподілених ботів, усуваючи обмеження попередніх підходів і забезпечуючи більш надійний метод для виявлення різних варіацій ботнетів [22].

Робота [23] містить огляд існуючих методів виявлення ботнетів та пов’язаних з ними обмежень. Авторами роботи висвітлюються проблеми виявлення нових різновидів ботнетів та звертається увага на необхідності впровадження методів, що не базуються на перевірці корисного навантаження пакетів, оскільки вони могли би працювати із зашифрованими мережевими протоколами [14]. У роботі обговорюється обмеження існуючих методів виявлення при роботі з новими атаками ботнетів. Також підкреслено переваги аналізу поведінки трафіку порівняно з аналізом корисного навантаження пакетів, зокрема можливість працювати із

зашифрованим трафіком та менший вплив на продуктивність мережі. У дослідженні запропонована модель виявлення, окреслено параметри її експериментальної оцінки та надано результати для запропонованого детектора, котрі свідчать про його здатність виявляти ботнет-атаки з високою точністю [23].

Шифрування DNS. Робота [24] надає ґрунтовний огляд поточного спектру можливостей шифрування *DNS* [14], зосереджуючись на стандартних методах: – *DoT*, *DoH* та *DoQ*. Автори аналізують статус прийняття цих методів, їх продуктивність, переваги та проблеми безпеки. Основним фокусом статті є зловживання шифруванням *DNS* для командно-контрольних комунікацій (*див. рис.2*) і каналів викрадення/витоку даних, що створює певні труднощі у виявленні та боротьбі з відповідною діяльністю. Також обговорюються методи аналізу зашифрованого *DNS*-трафіку для профілювання дій користувачів з метою виявлення зловмисної та/чи нештатної мережевої активності. Авторами роботи сформульовано напрями майбутніх досліджень, стосовно підвищення продуктивності та безпеки шифрування *DNS* [24].

Автори роботи [25] провели детальний аналіз розгортання і використання протоколів *DNS* шифрування, зосереджуючись на *DoT* та *DoH*. Дослідження охоплює порівняльну оцінку різних протоколів *DNS* шифрування та проблеми безпеки, що пов’язані з цими протоколами, зокрема оцінку доступності та продуктивності, а також порівняння обсягів трафіку між традиційними й зашифрованими *DNS* запитами. Автори дослідження підкреслюють, що хоча якість послуг постачальників *DNS* загалом є задовільна, однак, деякі служби мають неправильні конфігурації, що потребує уваги. Висновки висвітлюють поточний стан галузі телекомунікацій до широкомасштабного впровадження зашифрованих *DNS* протоколів [25].

Стаття [26] присвячена дослідженню шифрування *DNS* запитів для захисту конфіденційності користувачів від атак, що передбачають аналіз трафіку. У роботі вивчаються питання ефективності аналізу *DNS* трафіку для виявлення моделей веб-активності користувачів через зашифрований *DNS*, з особливим акцентом на протокол *DoH* [14]. Пропонуючи новий набір функцій, розроблений спеціально для аналізу зашифрованого *DNS*-трафіку, автори демонструють «успішні» атаки з високою точністю, підкреслюючи існуючі обмеження поточних засобів захисту. Автори досліджень оцінюють рівень захисту, який забезпечують *DoH* і *DoT*, акцентуючи, що *DoT* демонструє кращій рівень безпеки. Підкреслено, що потенціал фільтрації трафіку на основі *DNS*, навіть у сценаріях із зашифрованим *DNS*, надає цінну інформацію про вразливості і засоби захисту в рамках зашифрованого *DNS* [26].

Зони політики реагування (*RPZ*). Робота [27] надає широкий аналіз проблематики зон політики реагування *DNS*. Автор детально розглядає історію, розвиток та особливості реалізації *RPZ* в ПЗ сервера імен *BIND*, а також приклади їх (політик) розгортання в реальному середовищі. Згідно з дослідженням, впровадження зон політики реагування ефективно блокує спроби *DNS* запитів з небезпечними доменами, захищаючи клієнтські системи без втрати їхньої продуктивності. Автором роботи представлено набір інструментів для аналізу журнальних даних *RPZ*, який сприяє завчасної ідентифікації потенційно скомпрометованих систем та небажаної мережевої поведінки користувачів. У роботі спрогнозовано подальші напрямки розвитку *RPZ*, включаючи залучення комерційних постачальників відповідних послуг та вдосконалення механізмів захисту від фішингових атак [3, 27-28].

Дослідження роботи [29] присвячено питанням виявлення і блокування аномальних вихідних *DNS*-запитів, що пов’язані із функціонуванням ботнетів. Автори пропонують систему на основі політик, яка використовує зони політики реагування *DNS* для вдосконалення свого попереднього підходу, котрий базувався на базі даних *MySQL*, основним недоліком якого була мережева затримка. Система що розглядається використовує програмно-визначену мережу для контролю мережевого трафіку та аналізу *DNS*-запитів на відповідність політикам, збереженим у відповідних *RPZ*, ефективно зменшуючи затримку і поліпшуючи виявлення, та блокування

шкідливого *DNS*-трафіку. Робота містить попередню оцінку продуктивності і функціональності системи, яка підтверджує її ефективність у локальному мережевому середовищі на основі програмно-визначеної мережі. Автори планують продовжити оцінку цієї системи в умовах роботи реальної мережі та вивчення методів збереження конфіденційності *DNS* трафіку [29].

Виявлення алгоритмів генерації доменів. Робота [30] пропонує всебічний огляд проблематики у напряму виявлення алгоритмів генерації доменів. Автори вказують на важливість тестів, стандартизованих метрик і методів виділення ознак для підвищення надійності та відтворюваності експериментів у дослідженнях *DGA*. Досліджуючи різні *DGA* та їх альтернативи проведено розгляд стратегій, котрі використовуються зловмисниками, та потребу в більш складних методах виявлення. Запропонована авторами методологія застосовує ймовірнісні підходи для ефективного виявлення *DGA* на основі списку слів. Робота пропонує аналіз поточного стану виявлення *DGA* та окреслює можливі майбутні напрями досліджень для протидії інструментам створення шкідливих доменів.

Авторський колектив роботи [31] представляє власний підхід до ідентифікації алгоритмів генерації доменів, шляхом використання методів глибокого навчання (*DL - Deep Learning*). Дослідження зосереджено на вирішенні труднощів виявлення *DGA*, які генерують домени шляхом псевдовипадкового об’єднання словникових термінів. Використовуючи контекстно-залежне вбудовування слів та «простий» повнозв’язний класифікатор, автори роботи демонструють ефективність свого підходу до класифікації доменів. Використання попередньо підготовлених слів, мінімальні обсяги вихідних даних та коротка тривалість термінів навчання, відрізняють цей підхід від існуючих методів. Дослідники підкреслюють оригінальність своєї методики, яка не потребує розробки функцій вручну та вивчення списків слів *DGA* [31], що підтверджує її потенціал для умов реального застосування.

У роботі [32] досліджуються особливості виявлення зловмисних доменних імен генерованих *DGA*, за допомогою реалізації різних архітектур *DL*. Дослідження охоплює використання згорткової нейронної мережі (*CNN*), рекурентної нейронної мережі (*RNN*), довготривалої короткочасної пам’яті (*LSTM*) та інших моделей. Автори досліджують ефективність різних підходів *DL* для точного визначення шкідливих доменів, порівнюючи показники продуктивності різних архітектур моделей глибокого навчання. Запропонований фреймворк [32] демонструє високу ефективність у виявленні доменних імен, що синтезовані *DGA* та може бути використаний для блокування ботів від зовнішніх зв’язків і порушення каналів управління з командно-контрольними серверами ботнетів (*див. рис.2*).

2.3. Узагальнення поточних застосувань та концептуальних напрацювань в рамках проблематики фільтрації DNS

Як вже було зазначено вище, канали розвідки загроз (*рис.1*) є важливими джерелами критично важливих даних про поточні кіберзагрози, які допомагають завчасно виявляти і оперативно реагувати на нові загрози ІБ. Однак при цьому, актуальною проблемою залишається оцінка якості цих каналів. Дослідження за цим напрямом пропонують нові метрики та методики для оцінювання каналів розвідки, в т.ч. на основі аналізу даних *DNS*-трафіку. Крім того, наголошується на високому ступені унікальності та надмірності помилкових спрацювань у різних каналах розвідки. Узагальнюючи стан напрацювань та поглядів дослідників на подальші можливості більш релевантної екстракції даних з каналів розвідки загроз, можна зробити висновок, про необхідність покращення ефективності механізмів оцінки наявних каналів розвідки та концентрації зусиль на зменшенні частки помилкових спрацювань (*прогнозів*).

Виявлення ознак мережевої активності командних серверів ботнетів (*рис.2*) може надати важливу інформацію для систем безпеки з фільтрацією *DNS*-трафіку. Впровадження такого

механізму протидії дозволяє відокремити інфіковані засоби у мережі від відповідних командних центрів або завчасно захистити мережу від атак ботнетів, наприклад за рахунок нав'язування мережевої «гри» з використанням мережевих пасток [6-7]. Поточний стан досліджень тримає у фокусі питання виявлення каналів управління ботнетів, що в свою чергу, зумовлює постійне вдосконалення методик аналізу їх поведінки шляхом комплексного моніторингу *DNS*-трафіку, включаючи «роботу» з зашифрованим трафіком [14]. Отримані напрацювання декларують досить високу точність виявлення для відомих різновидів ботнетів, однак дослідники звертають увагу на обмеження існуючих підходів [30-32].

Стосовно напряму шифрування *DNS*, слід чітко розділяти дві взаємопов'язані іпостасі подальшого розвитку подій. Так, з одного боку шифрування *DNS*, може сприяти підвищенню якості фільтрації *DNS*, теоретично забезпечуючи при цьому більш безпечний канал для *DNS*-запитів, запобігаючи підробці та/чи втручанню в трафік зловмисників. Однак, з іншого боку, із впровадженням шифрування *DNS* виникає проблема ускладнення процесу виявлення зловмисного трафіку [14], зокрема трафіку командно-контрольних центрів ботнетів (*див. рис.2*). Більш того, у аналізованих роботах є приклади «успішних» атак на шифрування *DNS* (наприклад у [26]), що ставить під сумнів ефективність шифрування, як інструменту із забезпечення конфіденційності мережевої активності користувачів. Автори робіт пропонують власні методи аналізу шифрованого трафіку для профілювання активності користувачів з метою виявлення зловмисних дій та вказують на перевагу *DNS-через-TLS* у ефективності захисту. В якості основної проблеми, у межах напряму шифрування *DNS*, слід зазначити можливість використання зловмисниками технологій шифрування цього трафіку з метою ускладнення виявлення їх деструктивної діяльності (*фішинг, спам, DDos, DNSA тощо*).

Практика використання зон політик реагування (*RPZ*) незмінно продовжує привертати увагу дослідників [27, 29] до цього напряму та є ефективним інструментом управління безпекою сучасних ІКС на рівні служби *DNS*, що забезпечує завчасне виявлення й блокування небезпечних доменів.

Виявлення ознак роботи алгоритмів генерації доменів (*DGA*), що виступають головним інструментом для створення сукупності умовних «точок зустрічі» кіберзловмисників з їх власними командно-контрольними серверами ботнетів (*див. рис.2*), залишається вкрай важливим завданням. Стрімке й одночасне поширення Інтернету речей (*IoT*), технологій віртуалізації (*VR*), штучного інтелекту і машинного навчання (*AI/LM*), лише додатково підкреслюють вектор на невідкладність розробок, що адекватні рівню та темпу появи нових загроз ІБ. Вочевидь, що проблематика оперативної ідентифікації, блокування генерації і поширення злочинних доменів [30-32] ще до того, як вони зможуть завдати шкоди, є безумовно пріоритетним напрямом для подальших досліджень фахівців з ІБ.

Останні дослідження [22-24, 30-32] в галузі протидії впливу *DGA* розглядають тести, метрики та нові методи виявлення відповідних алгоритмів, котрі базуються на ймовірнісному аналізі і техніках *LM/DL*. Узагальнюючи цей досвід можна стверджувати, що пріоритетним напрямом з протидії *DGA*, є інтеграція нових - більш вдосконалених методик у єдину інтегровану систему фільтрації *DNS*, що втілює парадигму проактивного захисту та базується на останніх напрацюваннях в галузі штучного інтелекту і машинного навчання. Впровадження цих технологій розширює можливості поведінкового аналізу мережевої активності [6-7] та вдосконалює евристичні алгоритми, що здатні завчасно й оперативно виявляти і класифікувати підозрілі домені, тим самим усуваючи основні передумови для поширення активності ботнетів. Тож найбільш ймовірним напрямом досліджень в галузі проблематики фільтрації *DNS*, можна вважати синтез нових структур та логіки роботи інтегрованих підсистем *DNS* безпеки (*див. рис.5*), що впроваджують останні напрацювання на рівні стеку *VR-AI-LM-DL* технологій. Вочевидь, що саме таке поєднання, може дати паритетну відповідь на загрозу масштабного

впровадження *AI* в алгоритми зловмисної генерації доменів. Іншими словами, де-факто потрібно вести розмову про необхідність ефективної протидії впливу *AI* як основного елемента протиборчої сторони '[33].

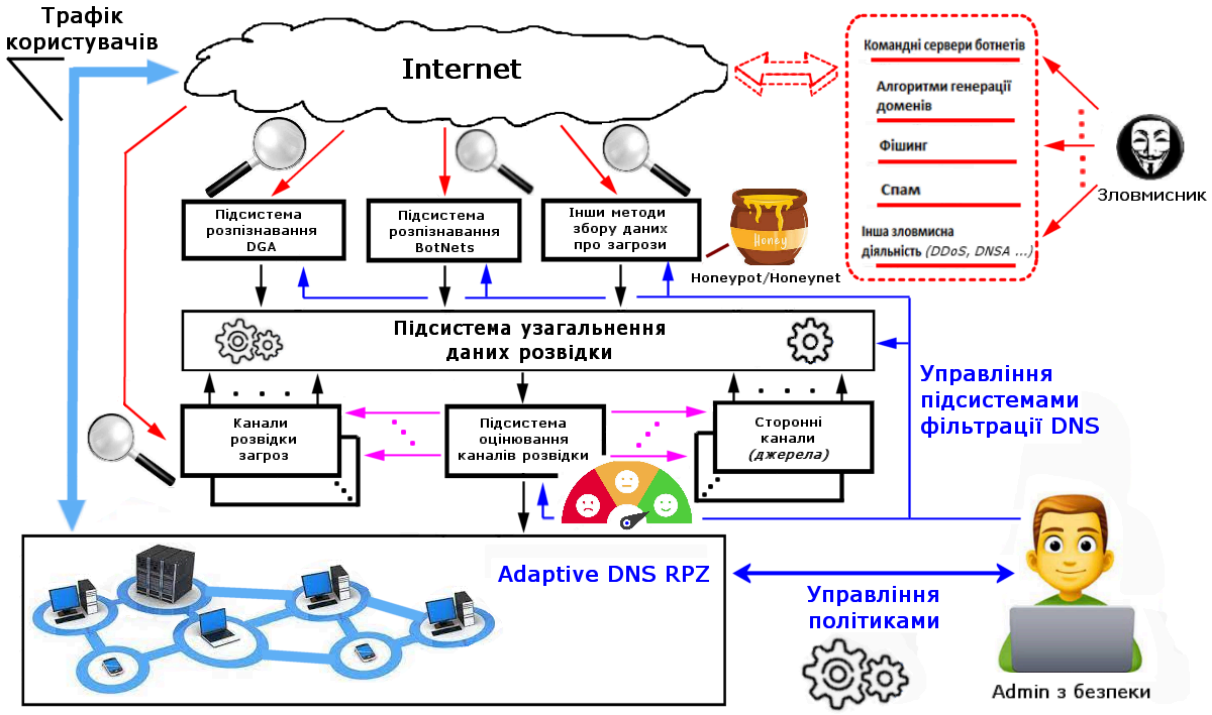

Рис. 5 - Структурний концепт інтегрованої системи DNS безпеки [33]
Fig.5 - Structural concept of an integrated DNS security system [33]

Для ефективної протидії новим загрозам таки системи мають впроваджувати механізми комплексної обробки та агрегування даних у канали розвідки загроз. Ці механізми повинні забезпечувати постійний моніторинг і оновлення інформації, надаючи актуальні дані для аналізу загроз та прийняття коригуючи рішень (*наприклад, стосовно зміни поточної RPZ на рис.5*). Дані із системи агрегування інформації (*узагальнення даних розвідки*) повинні оперативно використовуватися для покращення якості оцінки наявної сукупності основних та сторонніх каналів розвідки загроз. Відповідним чином, мають бути модифіковані адаптивні зони політик реагування, які використовують дані з каналів розвідки загроз для автоматичного застосування заходів захисту та/чи коригування налаштувань параметрів функціонування окремих підсистем інтегрованої системи *DNS* безпеки.

Узагальнюючи результати різних дослідницьких груп [21-27, 29-32], слід відзначити важливість робіт у напрямах оптимізації порядку взаємодії різних компонентів системи розпізнавання і збору даних та вдосконалення механізмів оновлення й активації політик реагування (*RPZ*). Зокрема це передбачає розробку інтерфейсів обміну даними, уніфікацію форматів даних та забезпечення безпеки передачі інформації (*особливо в разі реалізації розподіленої та/чи хмарної системи безпеки*).

3. Висновки

1. Новий, прийдешній постквантовий технологічний уклад, виводить довічний процес протистояння засобів атаки і захисту на принципово новий рівень, де можливості людини, як

адміністратора систем безпеки, повинні бути корінним образом переосмислені й модифіковані [33]. Причина такого стану справ очевидна: – масштаби, темп і сутність технологічного розвитку сучасного інформаційного суспільства, котрі перетнули межу фізіологічних можливостей сучасної людини. У цьому сенсі, сфера ІБ є одним із флагманських движків, де базовими аргументами назрілих змін є:

- масштабність наслідків;
- багатопотоковість даних;
- взаємопов'язаність процесів;
- складність формалізації завдань;
- висока швидкість перебігу подій і явищ;
- зростання обсягів оброблюваної інформації;
- розподіленість інфраструктур та основних акторів;
- необхідність протидіяти впливу AI як протиборчій стороні тощо.

2. Додатковими факторами, котрі виступають потужним прискорювачем процесів створення сучасних ІКС є стрімке поширення технологій *IoT* та *mesh*-мереж (*що вже вийшли за рівень Scatternet*). Конвергенція цих напрямів з можливостями *AI* та *LM*, створює нові горизонти задач особливо в частині протидії алгоритмам генерації доменів та ботнетів на стороні кіберзлочинців.

3. Розгляд питань з забезпечення ІБ слід вести виключно у розрізі недопущення диспаритету можливостей *AI* на користь протиборчої сторони. На практиці це означає, що майбутні системи захисту повинні широко впроваджувати останні новації на рівні стеку *VR*, *AI*, *LM* та *DL* технологій.

4. Особливої уваги потребують питання забезпечення балансу безпеки та продуктивності (швидкодії) перспективних ІКС при впроваджені в них інструментів шифрування *DNS*. Розробка нових методів шифрування, які одночасно забезпечують високий рівень захисту, мінімізують затримки у передачі даних і при цьому не ускладнюють процес виявлення зловмисного трафіку, є важливим напрямом для подальших досліджень.

5. Аналіз результатів досліджень з проблематики аналізу і фільтрації *DNS* трафіку, вказує на існування певних проблем у якості використовуваних каналів розвідки загроз безпеки, де впровадження технологій *AI* та *LM* повинно прискорити й одночасно посилити «глибину» екстракції потрібної, корисної інформації про актуальні загрози [33].

Конфлікт інтересів

Автори повідомляють про відсутність конфлікту інтересів.

Список літератури:

1. What is DNS? Вилучено з URL: https://www.cloudflare.com/learning/dns/what-is-dns/
2. Погоріла, К., Лєсная, Ю., Богданова, Є., & Малахов, С. (2022). Соціальний інжиніринг, як фактор реалізації інсайдерських загроз. *Scientific Collection «InterConf», (111): with the Proceedings of the 1st International Scientific and Practical Conference «Scientific Community: Interdisciplinary Research» (June 6-8, 2022)*. Boston, USA; pp. 494-501. Вилучено з https://archive.interconf.center/index.php/conference-proceeding/article/view/645/666
3. Лєсная, Ю., Малахов, С. Узагальнення основних передумов реалізації фішингових атак. *Proceedings of the XVII International Scientific and Practical Conference*. Ankara, Turkey. 2023. Pp.453-457. Available at: https://doi.org/10.46299/ISG.2023.1.17
4. What is DNS filtering? Вилучено з URL: https://www.cloudflare.com/learning/access-management/what-is-dns-filtering/

5. Яремчук, К., Воскобойников, Д., & Мелкозьорова, О. (2022). Сучасні загрози та способи забезпечення безпеки веб-застосунків. *Комп'ютерні науки та кібербезпека,* (2), 28-34. https://doi.org/10.26565/2519-2310-2022-2-03
6. Богданова, Є., Чорна, Т., & Малахов, С. (2022). Огляд поточного стану загроз, що обумовлені впливом експлойтів. *Комп'ютерні науки та кібербезпека,* (2), 35-40. https://doi.org/10.26565/2519-2310-2022-2-04
7. Кохановська, Т., Нарежний, О., & Дьяченко, О. (2020). Дослідження можливостей технології Honeypot. *Комп'ютерні науки та кібербезпека,* 1(1), 33-42. https://doi.org/10.26565/2519-2310-2020-1-03
8. Михайленко Д., Нємцев М. Особливості технології мережевих пасток як інструменту активного захисту та аналізу дій атакуючої сторони. *Proceedings of the XXI International Scientific and Practical Conference.* Melbourne, Australia. 2023. Pp. 483-487. Available at: https://doi.org/10.46299/ISG.2023.1.21
9. Січкар, М., & Малахов, С. (2024). Узагальнення особливостей відомих засобів міжмережевого екранування. *Proceedings of the XXI International Scientific and Practical Conference.* Sofia, Bulgaria. 2024. Pp. 370-376. Available at: https://doi.org/10.46299/ISG.2024.1.21
10. What is a Threat Intelligence Feed? Вилучено з URL: https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/threat-intelligence-feeds/
11. Guofei Gu, Junjie Zhang & Wenke Lee. BotSniffer: Detecting Botnet Command and Control Channels in Network Traffic. URL: https://people.engr.tamu.edu/guofei/paper/Gu_NDSS08_botSniffer.pdf
12. How Does a DNS Amplification Attack Work? (2024). Check Point. Вилучено з https://www.checkpoint.com/cyber-hub/network-security/what-is-dns-security/what-is-a-dns-amplification-attack/
13. Albulayhi, K., Smadi, A., Sheldon, F., & Abercrombie, R. (2021). IoT Intrusion Detection Taxonomy, Reference Architecture, and Analyses. Sensors, (6432), 21. https://doi.org/10.3390/s21196432
14. Коробейнікова, Т., & Федчук, Т. (2024). Огляд протоколів DNS, DOH та DOT. *Collection of Scientific Papers «ΛΟΓΟΣ»*, (March 1, 2024; Paris, France), 253–256. https://doi.org/10.36074/logos-01.03.2024.056
15. Гайкова, В., & Малахов, С. (2021). Аналіз факторів і умов реалізації кібербулінгу з урахуванням можливостей сучасних інформаційних систем. *Комп'ютерні науки та кібербезпека,* (1), 50-59. https://doi.org/10.26565/2519-2310-2021-1-04
16. Hugo M. Connery. DNS Response Policy Zones History, Overview, Usage and Research. URL: https://www.dnsrpz.info/RPZ-History-Usage-Research.pdf
17. What Are Domain Generation Algorithms? Вилучено з URL: https://www.akamai.com/glossary/what-are-dgas
18. Anhar Haneef. On the Scalable Generation of Cyber Threat Intelligence from Passive DNS Streams URL: http://surl.li/phbham
19. Keijo Korte. Measuring the quality of Open Source Cyber Threat Intelligence Feeds. URL: http://surl.li/yhiqoe
20. Vector Guo Li, Matthew Dunn, Paul Pearce, Damon McCoy, Geoffrey M. Voelker, Stefan Savage, Kirill Levchenko. Reading the Tea Leaves: A Comparative Analysis of Threat Intelligence, URL: https://www.usenix.org/system/files/sec19-li-vector_guo.pdf
21. Constantinos Patsakis, Fran Casino. Exploiting Statistical and Structural Features for the Detection of Domain Generation Algorithms. URL: https://arxiv.org/pdf/1912.05849
22. Joewie J. Koh, Barton Rhodes. Inline Detection of Domain Generation Algorithms with Context-Sensitive Word Embeddings. URL: https://arxiv.org/pdf/1811.08705
23. Amara Dinesh Kumar, Harish Thodupunoori, R. Vinayakumar, K. P. Soman, Prabaharan Poornachandran, Mamoun Alazab, and Sitalakshmi Venkatraman. Enhanced Domain Generating Algorithm Detection Based on Deep Neural Networks. URL http://surl.li/sgufmu
24. Minzhao Lyu, Hassan Habibi Gharakheili, Vijay Sivaraman. A Survey on DNS Encryption: Current Development, Malware Misuse, and Inference Techniques. URL: https://arxiv.org/pdf/2201.00900
25. Chaoyi Lu, Baojun Liu, Zhou Li, Shuang Hao, Haixin Duan, Mingming Zhang, Chunying Leng, Ying Liu, Zaifeng Zhang & Jianping Wu. An End-to-End, Large-Scale Measurement of DNS-over-Encryption: How Far Have We Come? URL: http://surl.li/ebouep

26. Sandra Siby, Marc Juarez, Claudia Diaz, Narseo Vallina-Rodriguez, Carmela Troncoso. Encrypted DNS - Privacy? A Traffic Analysis Perspective. URL: https://arxiv.org/abs/1906.09682
27. Hugo M. Connery. DNS Response Policy Zones History, Overview, Usage and Research. URL: https://www.dnsrpz.info/RPZ-History-Usage-Research.pdf
28. Скибун, О. (2023). Фішинг та фішери в сучасному світі. *Grail of Science*, (23), 259–264. https://doi.org/10.36074/grail-of-science.23.12.2022.38
29. Hikaru Ichise, Yong Jin & Katsuyoshi Iida. Policy-based Detection and Blocking System for Abnormal Direct Outbound DNS Queries using RPZ. URL: https://eprints.lib.hokudai.ac.jp/dspace/handle/2115/86951
30. Kamal Alieyan, Ammar Almomani, Ahmad Manasrah, Mohammed M. Kadhum. A survey of botnet detection based on DNS. URL: http://surl.li/vqinqn
31. Hyunsang Choi, Hanwoo Lee, Heejo Lee, Hyogon Kim. Botnet Detection by Monitoring Group Activities in DNS Traffic. URL: http://surl.li/nbbypc
32. David Zhao, Issa Traore, Bassam Sayed, Wei Lu, Sherif Saad, Ali Ghorbani, Dan Garant. Botnet detection based on traffic behavior analysis and flow intervals. URL: http://surl.li/ydwehw
33. Чепель, Д., Малахов, С. & Колованова, Є. (2024). Огляд можливостей фільтрації DNS, як інструмента безпеки сучасних інформаційних систем. *Grail of Science*, (42), 395–398. https://doi.org/10.36074/grail-of-science.02.08.2024

SUMMARY OF DNS TRAFFIC FILTERING TRENDS AS A COMPONENT OF MODERN INFORMATION SYSTEMS SECURITY

Danylo Chepel[1], CSD Student (master), Department of Security of Information Systems and Technologies; e-mail: dan4epel@gmail.com; ORCID: https://orcid.org/0009-0009-7449-8095
Serhii Malakhov[1], Ph.D., Senior Researcher, Computer Science Department;
e-mail: malakhov@karazin.ua; ORCID: https://orcid.org/0000-0001-8826-1616
[1] *V. N. Karazin Kharkiv National University, Ukraine*

Manuscript was received April 21, 2024; Received after review May 21, 2024; Accepted June 23, 2024

Abstract. The study analyzes sources related to methods and technologies for DNS (Domain Name System) traffic filtering. Five main directions are identified that are actively used to enhance security at the DNS level. All examined technologies offer improvements in the quality of DNS filtering. It is emphasized that combining different approaches simultaneously can enhance overall security. The summary of research results on DNS traffic security issues indicates certain problems in the quality of the threat intelligence channels used. Therefore, the implementation of AI and LM technologies should enhance the "depth" of extracting useful information about current threats. It is emphasized that the consideration of information security issues should be conducted exclusively in the context of preventing the disparity of artificial intelligence (AI) capabilities in favor of the adversary (i.e., cybercriminals). Practically, this means that future DNS filtering systems should widely implement the latest advancements in VR, AI, LM, and DL technologies. This is particularly important in countering Domain Generation Algorithm (DGA) mechanisms and the spread of botnets. The specific issues of ensuring a consensus on the security and performance of current information and communication systems when implementing DNS encryption tools are highlighted. The primary problem associated with DNS traffic encryption is the potential for its misuse by attackers to conceal their destructive activities (phishing, spam, etc.).

Keywords: *DNS, DGA, RPZ, information security, security threats, traffic filtering, botnet*

Conflicts of Interest: the authors declare no conflict of interest.

References

1. What is DNS? URL: https://www.cloudflare.com/learning/dns/what-is-dns/
2. Pohorila, K., Lesnaya, Yu., Bogdanova, E., & Malakhov, S. (2022). Social engineering as a factor in the implementation of insider threats. *Scientific Collection «InterConf», (111): with the Proceedings of the 1st International Scientific and Practical Conference «Scientific Community: Interdisciplinary Research» (June 6-8, 2022)*. Boston, USA; pp. 494-501. https://archive.interconf.center/in-dex.php/conference-proceeding/article/view/645/666 [In Ukrainian]
3. Lesnaya, Yu., Malakhov, S. Generalization of the main prerequisites for the implementation of phishing attacks. *Proceedings of the XVII International Scientific and Practical Conference.* Ankara, Turkey. 2023. Pp.453-457. Available at: https://doi.org/10.46299/ISG.2023.1.17 [In Ukrainian]
4. What is DNS filtering? URL: https://www.cloudflare.com/learning/access-management/what-is-dns-filtering/
5. Yaremchuk, K., Voskoboynikov, D., & Melkozyorova, O. (2022). Modern threats and ways to secure web applications. *Computer Science and Cybersecurity*, (2), 28-34. https://doi.org/10.26565/2519-2310-2022-2-03 [In Ukrainian]
6. Bohdanova, E., Chorna, T., & Malakhov, S. (2022). Overview of the current state of threats caused by the influence of exploits. *Computer Science and Cyber Security,* (2), 35-40. https://doi.org/10.26565/2519-2310-2022-2-04 [In Ukrainian]
7. Kokhanovska, T., Narezhny, O., & Dyachenko, O. (2020). Exploring the capabilities of Honeypot technology. *Computer Science and Cybersecurity,* 1(1), 33-42. https://doi.org/10.26565/2519-2310-2020-1-03 [In Ukrainian]
8. Mykhaylenko D., Nemtsev M. Peculiarities of the technology of network traps as a tool of active protection and analysis of the actions of the attacking party. *Proceedings of the XXI International Scientific and Practical Conference.* Melbourne, Australia. 2023. Pp. 483-487. Available at: https://doi.org/ 10.46299/ISG.2023.1.21 [In Ukrainian]
9. Sichkar, M., & Malakhov, S. (2024). Generalization of the features of known means of network shielding. *Proceedings of the XXI International Scientific and Practical Conference.* Sofia, Bulgaria. 2024. Pp. 370-376. Available at: https://doi.org/10.46299/ISG.2024.1.21 [In Ukrainian]
10. What is a Threat Intelligence Feed? URL: https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/threat-intelligence-feeds/
11. Guofei Gu, Junjie Zhang & Wenke Lee. BotSniffer: Detecting Botnet Command and Control Channels in Network Traffic. URL: https://people.engr.tamu.edu/guofei/paper/Gu_NDSS08_botSniffer.pdf
12. How Does a DNS Amplification Attack Work? (2024). Check Point. URL: https://www.checkpoint.com/cyber-hub/network-security/what-is-dns-security/what-is-a-dns-amplification-attack/
13. Albulayhi, K., Smadi, A., Sheldon, F., & Abercrombie, R. (2021). IoT Intrusion Detection Taxonomy, Reference Architecture, and Analyses. Sensors, (6432), 21. https://doi.org/10.3390/s21196432
14. Korobeynikova, T., & Fedchuk, T. (2024). Overview of protocols DNS, DOH, DOT. *Collection of Scientific Papers «ΛΟΓΟΣ»*, (March 1, 2024; Paris, France), 253–256. https://doi.org/10.36074/logos-01.03.2024.056 [In Ukrainian]
15. Haykova, V., & Malakhov, S. (2021). Analysis of factors and conditions for the implementation of cyberbullying, taking into account the capabilities of modern information systems. *Computer Science and Cybersecurity,* (1), 50-59. https://doi.org/10.26565/2519-2310-2021-1-04 [In Ukrainian]
16. Hugo M. Connery. DNS Response Policy Zones History, Overview, Usage and Research. URL: https://www.dnsrpz.info/RPZ-History-Usage-Research.pdf
17. What Are Domain Generation Algorithms? URL: https://www.akamai.com/glossary/ what-are-dgas
18. Anhar Haneef. On the Scalable Generation of Cyber Threat Intelligence from Passive DNS Streams URL: http://surl.li/phbham
19. Keijo Korte. Measuring the quality of Open Source Cyber Threat Intelligence Feeds. URL: http://surl.li/yhiqoe
20. Vector Guo Li, Matthew Dunn, Paul Pearce, Damon McCoy, Geoffrey M. Voelker, Stefan Savage, Kirill Levchenko. Reading the Tea Leaves: A Comparative Analysis of Threat Intelligence, URL: https://www.usenix.org/system/files/sec19-li-vector_guo.pdf

21. Constantinos Patsakis, Fran Casino. Exploiting Statistical and Structural Features for the Detection of Domain Generation Algorithms. URL: https://arxiv.org/pdf/1912.05849
22. Joewie J. Koh, Barton Rhodes. Inline Detection of Domain Generation Algorithms with Context-Sensitive Word Embeddings. URL: https://arxiv.org/pdf/1811.08705
23. Amara Dinesh Kumar, Harish Thodupunoori, R. Vinayakumar, K. P. Soman, Prabaharan Poornachandran, Mamoun Alazab, and Sitalakshmi Venkatraman. Enhanced Domain Generating Algorithm Detection Based on Deep Neural Networks. URL http://surl.li/sgufmu
24. Minzhao Lyu, Hassan Habibi Gharakheili, Vijay Sivaraman. A Survey on DNS Encryption: Current Development, Malware Misuse, and Inference Techniques. URL: https://arxiv.org/pdf/2201.00900
25. Chaoyi Lu, Baojun Liu, Zhou Li, Shuang Hao, Haixin Duan, Mingming Zhang, Chunying Leng, Ying Liu, Zaifeng Zhang & Jianping Wu. An End-to-End, Large-Scale Measurement of DNS-over-Encryption: How Far Have We Come? URL: http://surl.li/ebouep
26. Sandra Siby, Marc Juarez, Claudia Diaz, Narseo Vallina-Rodriguez, Carmela Troncoso. Encrypted DNS - Privacy? A Traffic Analysis Perspective. URL: https://arxiv.org/abs/1906.09682
27. Hugo M. Connery. DNS Response Policy Zones History, Overview, Usage and Research. URL: https://www.dnsrpz.info/RPZ-History-Usage-Research.pdf
28. Skibun, O. (2023). Phishing and phishers in the modern world. *Grail of Science*, (23), 259–264. https://doi.org/10.36074/grail-of-science.23.12.2022.38 [In Ukrainian]
29. Hikaru Ichise, Yong Jin & Katsuyoshi Iida. Policy-based Detection and Blocking System for Abnormal Direct Outbound DNS Queries using RPZ. URL: https://eprints.lib.hokudai.ac.jp/dspace/handle/2115/86951
30. Kamal Alieyan, Ammar Almomani, Ahmad Manasrah, Mohammed M. Kadhum. A survey of botnet detection based on DNS. URL: http://surl.li/vqinqn
31. Hyunsang Choi, Hanwoo Lee, Heejo Lee, Hyogon Kim. Botnet Detection by Monitoring Group Activities in DNS Traffic. URL: http://surl.li/nbbypc
32. David Zhao, Issa Traore, Bassam Sayed, Wei Lu, Sherif Saad, Ali Ghorbani, Dan Garant. Botnet detection based on traffic behavior analysis and flow intervals. URL: http://surl.li/ydwehw
33. Chepel, D., Malakhov, S. & Kolovanova, E. (2024). Overview of DNS filtering capabilities as a security tool for modern information systems. *Grail of Science*, (42), 395–398. https://doi.org/10.36074/grail-of-science.02.08.2024 [In Ukrainian]