УДК 004.4

В.Д. Погребенник, П.Т. Хромчак
Національний університет “Львівська політехніка”,
кафедра захисту інформації

АКТИВНІ МЕТОДИ ВИЯВЛЕННЯ БОТНЕТ-МЕРЕЖ

Підсумовано та описано групи активних методів виявлення ботнет-мереж. Наведено основні недоліки та переваги роботи кожного з них.

Groups of active techniques of botnet detection mechanisms are described and summarized. The main advantages and disadvantages of each of them are discussed.

Вступ

Група активних методів виявлення ботнет-мереж використовує підходи, які взаємодіють з досліджуваним ресурсом. Ця група є найдієвішою в контексті протидії ботнетам та їх виявлення. На відміну від пасивних методів, взаємодія з суб’єктом дослідження накладає певні обмеження на вимірювання, що може проявлятися спотворенням точності вихідних даних. Так, наприклад, програма-аналізатор залишає сліди в аналізованому трафіку, що часто впливає на чистоту вибірки вхідних даних та їх аналіз. Окрім цього, головним недоліком активних методів виявлення є можливість їх детектування з боку власника ботнету, що в деяких випадках може призвести до таких контрзаходів, як зміна локації C&C, архітектури ботнету чи дій у відповідь, таких як DdoS тощо. Загалом група активних методів виявлення зомбі-мереж фокусується на протоколах, що використовують ботнети, та на їхній архітектурі.

Наведено різноманітні підходи до вимірювань показників активності ботнету та його виявлення. Методи, що застосовують для аналізу мережевих даних, містять техніки, які безпосередньо чи опосередковано взаємодіють з ботнетом, центром управління ботнетами та навіть провайдерами зв’язку, що надають послуги хостингу тощо.

Метою роботи є підбиття підсумку щодо використання та групування активних методів виявлення ботнет- мереж, а також висвітлення основних недоліків та переваг роботи кожного з них під час роботи в інформаційній мережі контрольованої зони.

Ізоляція

У загальних рисах термін “ізоляція” (sinkholing) описує технічний контрзахід для призупинення діяльності хоста чи його від’єднання від решти ботнету. Ізоляцію застосовують проти різних суб’єктів типово C&C, так званих місць збирання викраденого контенту тощо.

Найпоширеніший різновид ізоляції полягає у зміні доменного імені центру управління ботнетом на “підконтрольний” – такий, що створено у науково-дослідних цілях, як зображено на рис. 1.

Схожого ефекту можна досягти зміною статичного маршруту до центру управління ботнетом, що дасть змогу перескерувати мережевий трафік до вищезгаданого центру. Обидва підходи з урахуванням незначних покращень дають змогу детально проаналізувати масштаби ботнет-мережі та принципи, що покладено в основу її керування. Описані методи можна застосувати і до окремого вузла ботнету з метою вивчення його поведінки в стресових ситуаціях та для аналізу механізму завадостійкості до відімкнення центрів управління.

Також за допомогою функції дзеркалювання портів в активному комутаційному мережевому обладнанні можливо здійснити прозоре (невидиме) перескерування трафіку до другорядного джерела для дослідження, проте такий механізм є менш прийнятним, оскільки дозволяє ботнету функціонувати повноцінно протягом всього терміну. Це може бути корисно, коли необхідно провести ряд операцій, пов'язаних із з'ясуванням фундаментальних принципів роботи роботи ботнету аж до моменту централізованого та організованого відімкнення C&C серверів.

Базові принципи цього методу полягають у тому, що саме доменне ім'я, а не IP-адреса слугує засобом з'єднання з центром управління безпосередньо. Беручи до уваги цей факт, можна стверджувати, що використання методу ізоляції передбачає низький рівень прийняття неправильних рішенн.

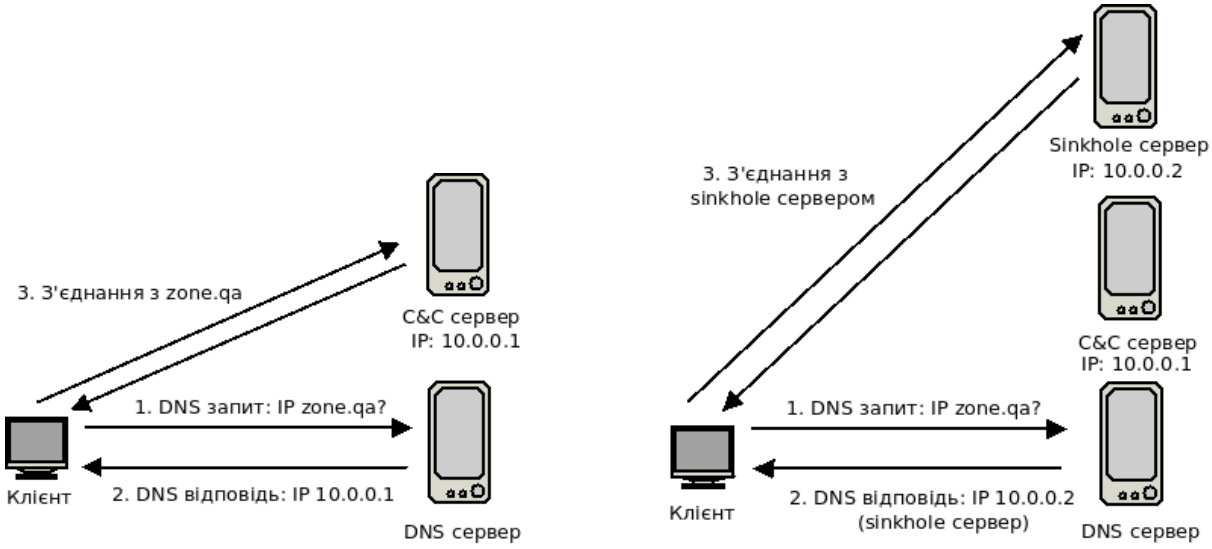

Рис. 1. Принцип роботи технології ізоляції

Недоліком цього методу є те, що точність вимірів та оцінка масштабів ботнету залежать від інформації, яка доступна для хоста управління. Якщо кожний бот, котрий контактує з C&C, надає вичерпну інформацію, яку можна використати для його унікальної ідентифікації, то досяжна точність є високою. З іншого боку, якщо обсяг інформації, котрий можна отримати, аналізуючи з'єднання між центром та ботом, є обмеженим, то результати виміру матимуть високу дисперсію. Так, наприклад, якщо канал комунікації між клієнтом та C&C є шифрований, то лише IP-адреси сторін можна використати для подальшого аналізу.

Вимірювання через унікальну IP-адресу містить різні аспекти, які можуть помітно вплинути на результати. З одного боку, якщо декілька інфікованих хостів є під'єднані до спільного маршрутизатора, який використовує NAT (Network Address Translation) трансляцію, то декілька ботнет-клієнтів будуть пораховані як один. Така поведінка притаманна мобільним пристроям, котрі використовують шлюзи, на яких здійснюється трансляція NAT. З іншого боку, якщо IP-адреси видаються динамічно та з великого адресного простору, то один клієнт може бути порахований як декілька.

Інфільтрація

Технології інфільтрації ботнетів можна поділити на дві групи: програмно залежні та апаратно залежні. Перша покриває дослідження, що зосереджуються на аналізі коду ботнету та мережевих даних, що йдуть у напрямку до клієнта для перехоплення контролю та проведення вимірювань. Друга група використовується у випадку, коли є можливість фізичного доступу до обладнання, на якому знаходиться центр управління ботнетом з метою прослуховування та перехоплення даних.

Програмно залежна інфільтрація замість емуляції чи модифікації коду бота на підконтрольному хості з наміром під'єднання боту до мережі та виміру його показників йде на крок попереду та має на меті отримання повного контролю над ботом. Це, як правило, вимагає як точку відліку застосовувати технології зворотного аналізу коду ПЗ комунікаційного механізму, який використовує бот. Такий аналіз дозволяє іноді навіть точно встановити потенційних жертв через аналіз уразливостей чи експлойтів, які використовує бот. Цю процедуру можна порівняти із аудитом безпеки чи тестуванням на проникність ботнету та його інфраструктури. Інформацію, отриману в процесі аналізу, можна застосувати для займання ключових позицій в його роботі та навіть повного перехоплення керування. Апаратно залежна інфільтрація може бути використана у випадку коли точно встановлено IP адреса центру управління ботнетом та можлива взаємодія із компанією, що надає послуги хостингу чи дата центром безпосередньо. Отримавши дані з порта, що віддзеркалює мережевий трафік підозрілого сервера, дані комунікацій можуть бути записані для подальшого аналізу. Це дозволяє детально розглянути мережеві дані, що дають таку важливу інформацію про роботу ботнету, як: кількість інфікованих хостів, їх місцерозташування та інші різноманітні атрибути з'єднань. Цей метод має спільні із методом ізоляції обмеження, а саме: при використанні ботнетом шифрованих з'єднань значно зменшується кількість доступних параметрів комунікацій та точність вимірювання. Також використання власниками ботнету так званого стійкого (від англ. abuse – зловживання) хостингу в країнах, де закон недостатньо адекватно регулює питання інформаційної безпеки чи механізм відкликання права оренди серверів та надання інформаційних каналів невідпрацьований, дозволяє їм безперешкодно управляти ботнетом чи хоча б отримати час для зміни провайдера, IP-адрес тощо.

Виявлення та вимірювання, основані на протоколі IRC

Сьогодні протокол IRC (Internet Relay Chat) досі слугує для управління ботнетом та його інфраструктурою. Згідно із щорічним звітом компанії Symantec, 31 % усіх відомих ботнетів використовують IRC як комунікаційний протокол [3]. IRC – це простий та надійний протокол, що використовується в чатах, а також характеризується високою функціональністю у сфері ботнетів. IRC орієнтовані центри управління використовують один або декілька IRC каналів на публічних чи приватних серверах для обміну службовими повідомленнями. Переважно новий бот спершу під'єднується до такого каналу та стає в режим очікування нових повідомлень та подальших інструкцій. Для того, щоб виміряти боти, спершу потрібно отримати інформацію, яка стосується параметрів з'єднання з каналом. Це, як правило, IP-адреса сторін та номер порту IRC-сервера, а також ім'я каналу. Зазвичай таку інформацію отримують аналізом коду бота чи моніторингу мережевих даних між C&C та клієнтом. Іноді, залежно від складності механізму взаємодії, можна отримати навіть реквізити автентифікації в каналі.

На другому етапі можливо під'єднатись до каналу та отримати додаткову інформацію про внутрішню архітектуру та масштаби ботнету загалом. Якщо канал управління знаходиться на публічному сервері, іноді можливо отримати імена клієнтів у каналі. Як правило, для управління ботнетом використовують приватні повідомлення замість публічних. Також часто для обміну повідомленнями використовуються механізми шифрування з'єднань, що ускладнює обробку даних чи повідомлень, які передаються за допомогою семантичного аналізу.

Аналіз записів у кеші DNS

Ця технологія заснована на такій властивості DNS сервера, як кешування запису про ресурс. Коли в локального DNS сервера запитується інформація про ресурс, яка йому невідома, сервер використає серію рекурсивних запитів, що врешті-решт дозволять отримати необхідну інформацію від авторитетного сервера відповідної зони. Коли відповідь отримано, її пересилають клієнту, що здійснив запит, а також записують у локальний кеш з метою економії ресурсів та підвищення швидкодії. Таку особливість роботи кешуючого DNS можна використати для вимірювальних цілей.

Головна ідея цього методу полягає у непрямій перевірці інформації про те, чи домен, що достовірно належить ботнету, був запитаний через конкретний DNS та кешованої інформації про ресурс, як показано на рис. 2, та встановлення факту присутності інфікованих клієнтів всередині мережі.

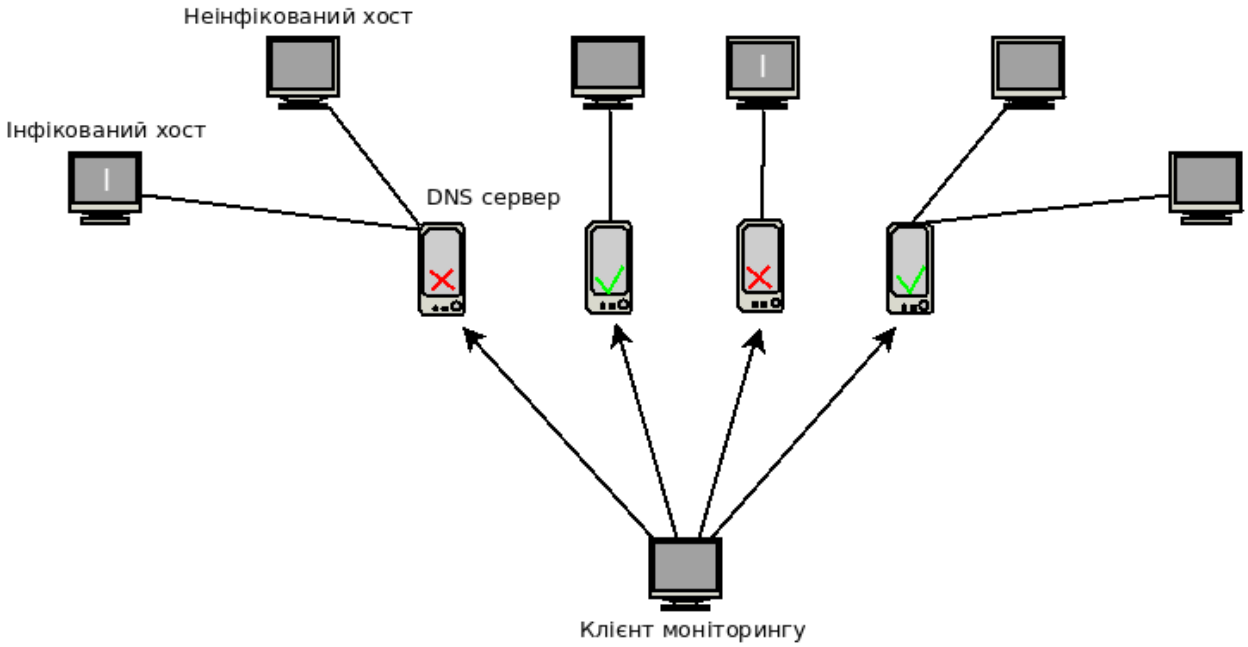

Рис. 2. Принцип роботи методу аналізу кеш-записів DNS сервера

Переважно для аналізу записів використовують дві підтехніки, вибір якої залежить від конфігурації DNS сервера. Перша передбачає, що запит надсилається до DNS сервера із спеціальним т.зв прапорцем “нерекурсивності”, що забороняє серверу використовувати серію рекурсивних запитів до авторитетного сервера зони. Поведінка сервера імен залежатиме від того, чи міститься запис про ресурси в його локальному кеші. Якщо запис знайдено, то у відповідь клієнт отримає запитувану інформацію. Якщо необхідного запису не буде знайдено в кеші, то у відповідь клієнт не отримає запитуваних даних чи отримає адресу авторитетних серверів, які можуть допомогти отримати необхідну інформацію, як зображено на рис. 3. Проте цей метод не завжди спрацьовує, оскільки більшість серверів імен просто відкидають такі клієнтські запити з метою захисту від DoS атак.

Друга техніка працює з будь-якими серверами імен, проте змінює кеш DNS сервера. У цьому випадку запит містить прапорець рекурсивності – запит буде відіслано до інших серверів. Це дає змогу визначити, чи відповідь вже була присутня в кеші до цього, чи ні. Результату досягають аналізуючи поле TTL (Time To Live) пакета відповіді. Якщо його значення дорівнює величині, яка встановлюється локальним сервером, це означає, що в кеші вже містився запис про ресурси. Якщо значення менше, це означає, що запит пересилався до інших серверів імен, оскільки це свідчить про те, що TTL значення сервера для цього домена вже було зменшене (розпочате) до контрольного запиту. Ця техніка можлива через те, що сервер не оновлює значення TTL для кешованого домена. Недоліком такого методу є те, що запит від аналітика залишить запис у кеші, що заблокує можливість використання цієї техніки знову – аж поки сервер не видалить запис з кешу. Цей підхід добре масштабується, що дає змогу розпаралелити процес аналізу. Обмеження виникають стосовно кількості доменних імен, які аналізуються. Багато серверів обмежують кількість запитів, які буде опрацьовано від одного клієнта. Це означає, що аналіз доменних імен може бути неповним. Залежно від загальної кількості доменів це може призвести до небажаних затримок в опрацюванні запитів.

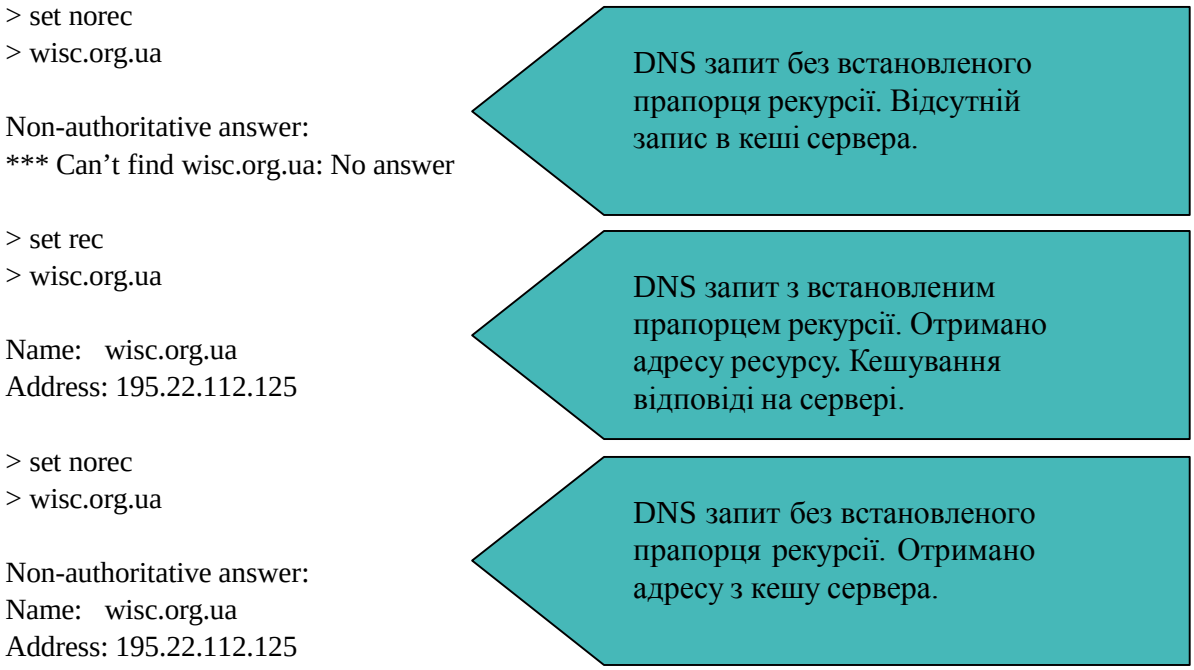

Рис. 3. Використання прапорця "нерекурсивності" для аналізу записів у кеші DNS

Розглядаючи точність цього підходу, справедливо зауважити, що він не придатний для викриття справжніх розмірів ботнету. Натомість він корисний для аналізу сегментів мережі Інтернет. Він дає змогу дедуктивно проаналізувати інформацію про те, наскільки поширене конкретне шкідливе ПЗ у межах аналізованого сегмента мережі.

Відслідковування швидкозмінних мереж

Деякі ботнет-мережі використовують т. зв. швидкозмінні (fast-flux) мережі задля підвищення відмовостійкості та надійності мережі загалом. Fast-flux мережі використовують швидкозмінні записи про ресурси на DNS, що вказують на велике число хостів, котрі працюють як додатковий проксі-прошарок для приховування наявної системи доставки контенту всередині ботнету. Часто проксі-хости – це користувацькі комп'ютери, що були скомпрометовані ботнет-клієнтами чи сторонніми експлойтами. Використовуючи асоціацію одного домену з великою кількістю IP-адрес, мережа стає стійкішою до контрзаходів. Проте лише дуже особливі властивості DNS записів обслуговують такий тип мереж, що дозволяє розрізняти їх з-поміж інших. Записи про домени, що під'єднані до fast-flux мереж, мають мале значення часу життя запису про ресурси, переважно, декілька хвилин. Це виявляється TTL значенням, що міститься в пакеті відповіді, який був згенерований первинним DNS сервером наприкінці ланцюга рекурсивних перетворень і який знаходиться під контролем власника ботнету [1]. Переважно шкідливий сервер імен управляється ботмастером або встановлюється як додатковий сервіс на скомпрометованому вузлі. Через певний час результатом нового запиту буде інший набір асоційованих IP-адрес з маловідомою схожістю до попередньої топології.

Додаткова, навіть характерніша особливість прослідковується у різноманітті IP-адрес, що повертаються для швидкозмінної мережі: такі IP-адреси належатимуть до кількох незалежних мереж та провайдерів. Типові сервіси з малим значенням TTL, наприклад, високопрофільні веб-сайти на кшталт google.com чи facebook.com зазвичай повертають адреси, котрі належать до близьких за значенням адресних просторів чи спільних для автономної системи об'єктів маршрутизації. Моніторингом доменів, чиї DNS-відповіді характеризуються низьким TTL, не лише ідентифікують швидкозмінні мережі, але виокремлюють групи хостів, що належать до неї, як показано на рис. 4.

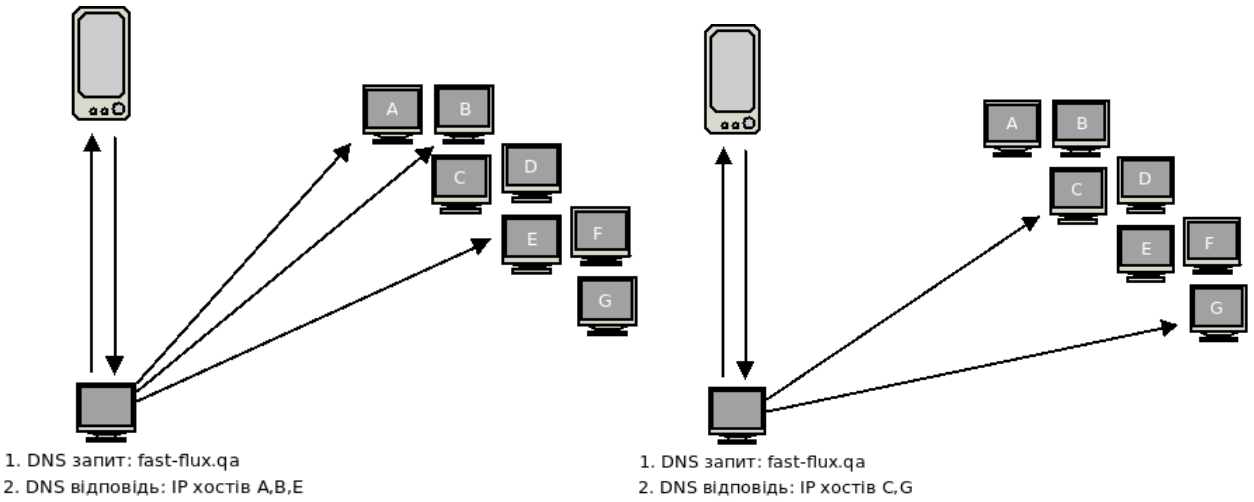

Рис. 4. Принцип роботи швидкозмінних мереж

Так, Т. Хольц та Дж. Назаріо продемонстрували результати моніторингу ботнетів на основі аналізу швидкозмінних мереж [2]. Для збирання вхідних даних вони використали мережу ATLAS (Arbor Networks' Active Threat Level Analysis System), що являє собою глобально розподілену мережу з приманок, сенсорів DoS та ін. джерел збирання даних. Система використовує різні джерела інформації для формування списку потенційних ботнет-належних доменів, які є швидкозмінними, беручи до уваги дані з таких джерел, як: листи зі спамом, списки ненадійних доменних імен тощо. Всі потенційні ботнет-кандидати оцінюються евристикою, що бере до уваги такі параметри, як TTL, номер AS (Autonomous System), IP-адреса, метрика та ін. Публікація результатів аналізу містила дані, зібрані та проаналізовані протягом чотирьох місяців. Протягом цього періоду було виявлено 928 різноманітних швидкозмінних мереж із загальною кількістю хостів близько 15 мільйонів з використанням запропонованого методу. Т. Хольц та Дж. Назаріо виявили, що близько третини доменів були активними менше одного тижня з піками активності, що тривали менше одного дня. Також вони зауважили, що середній час використання таких доменів становив близько 18 днів. Іншим відкриттям стало те, що майже у 80 % випадків домени були активовані за один місяць до початку активного використання.

Підрахунок мереж типу "точка–точка"

P2P-мережа – варіант "архітектури системи, в основу якої покладено мережу рівноправних вузлів. Ботнети, що використовують такий тип мережі, називаються ботнет-мережами з децентралізованою архітектурою. В децентралізованому ботнеті окремі боти формують області (групи), що знають лише про обмежене коло сусідів, що належать до цієї групи. Це забезпечує потужну платформу для роботи ботнету та запобігає його відімкненню за рахунок ізоляції як основних, так і запасних центрів управління. Окремий хост ботнету ідентифікується за допомогою унікального ключа, що поєднується з такою додатковою інформацією, як IP-адреса, номер порту тощо. Головна ідея використання мережі "точка–точка" полягає у створенні надбудованої мережі, котра використовує власний адресний простір та протоколи маршрутизації для обміну повідомленнями між ботами, що дає змогу досягти високої завадостійкості до відключень центрів управління [4].

Незважаючи на це, можливо проаналізувати списки сусідів боту та рекурсивно підрахувати й визначити інші інфіковані хости, що належать до нього. Для цього потрібен фізичний доступ до інфікованих комп'ютерів для подальшого аналізу коду боту. В ідеалі результатом такого підрахунку має стати вичерпний список ботів P2P-мережі. На рис. 5 наведено механізм детектування та підрахунку ботів, що належать до сегмента зомбі-мережі за результатами аналізу списків сусідів хостів D та E.

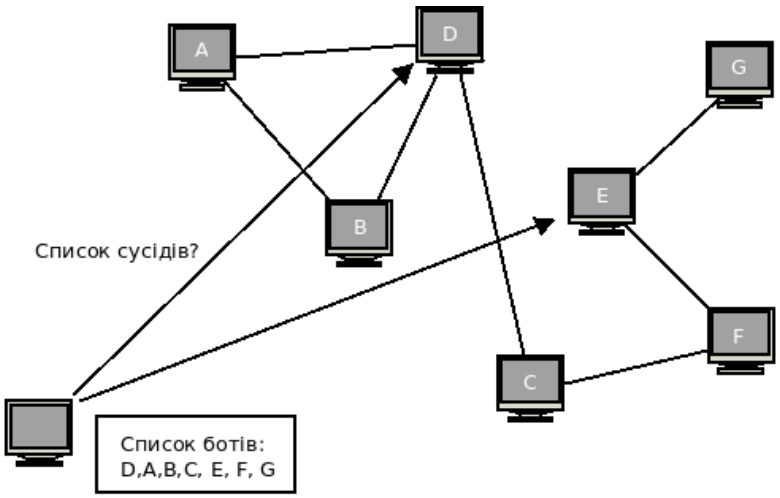

Рис. 5. Виявлення ботнетів P2P-ботнет мережі

Так, Т. Хольц продемонстрував методи систематичної інфільтрації та виміру параметрів децентралізованого ботнету за допомогою підрахунку хостів ботнету. Слід зауважити, що достовірність результатів аналізу залежала від реконструкції протоколів комунікації із залученням методів криптоаналізу та використання уразливостей у методах шифрування [5].

Висновок

Підсумовано та описано активні методи виявлення ботнет-мереж, що ґрунтуються на різноманітних технологічних рішеннях та передбачають втручання в роботу інформаційної мережі. Також наведено приклади конкретних технік та описано загальні особливості їхньої роботи, а також основні переваги та недоліки цих методів.

1. DNS Cache Snooping. Grangeia, L. Research Paper, 2004. 2. As the Net Churns: Fast-Flux Botnet Observations. Holz, T., Nazario, J. In: Proceedings of the 3rd International Conference on Malicious and Unwanted Software (MALWARE'08), 2008. 3. Symantec Global Internet Security Threat Report: Trends for 2009 (Volume XV). Symantec Corp., 2010. 4 Погребенник В.Д., Хромчак П.Т. Розроблення моделі системи виявлення центрів управління ботнет-мережами // Вісник Нац. ун-ту "Львівська політехніка". "Автоматика, вимірювання та керування". – 2009. – № 639. 5. Measurements and mitigation of peer-to-peer-based botnets: a case study on storm worm. Holz, T., Steiner, M., Dahl, F., Biersack, E., Freiling, F. In: Proceedings of the 1st Usenix Workshop on Large-Scale Exploits and Emergent Threats (LEET'08), 2008.