ВІДГУК

офіційного опонента на дисертацію Бобровнікової Кіри Юліївни
«Інформаційна технологія виявлення бот-мереж
у корпоративних мережах на основі аналізу DNS-трафіка»
подану на здобуття наукового ступеня кандидата технічних наук
за спеціальністю 05.13.06 – інформаційні технології

Актуальність теми.

Бот-мережі є одним з найбільш небезпечних видів шкідливого програмного забезпечення. Переважна більшість бот-мереж для керування інфікованими комп'ютерними системами використовує DNS. Саме цей факт часто використовують як один із перспективних напрямків по виявленню бот-мереж. Однак, оскільки відомі підходи виявлення бот-мереж на основі аналізу DNS-трафіка не враховують важливих факторів функціонування бот-мереж, це призводить до великої кількості хибних спрацювань. Серед недоліків відомих методів виявлення бот-мереж є можливість ухилення від виявлення шляхом динамічної зміни шкідливого коду, системи керування та портів або використання стандартних портів.

Під час виявлення невідомих ботів в корпоративній мережі виникає протиріччя між двома важливими показниками: інформаційною безпекою мережі та оперативністю роботи інформаційних систем. З метою підвищення оперативності роботи інформаційної системи корпоративної мережі, а також рівня достовірності виявлення бот-мереж, виникає потреба у зниженні рівня хибних спрацювань.

Тому, усунення недоліків відомих підходів через розроблення нових методів виявлення бот-мереж в корпоративних мережах, заснованих на аналізі DNS-трафіка, які враховують нову базову ознаку синхронності DNS-запитів та залучають методи інтелектуального аналізу даних, що дозволяє підвищити рівень достовірності виявлення невідомих ботів та оперативність роботи інформаційної системи корпоративної мережі, є актуальною задачею.

Обґрунтованість наукових положень.

Для розв'язання поставлених задач використовуються основні положення системного аналізу, методів аналізу даних, теорії мір близькості та теорії комп'ютерних мереж.

Наукові положення, висновки та рекомендації дисертаційної роботи забезпечуються:

- обґрунтованим викладенням матеріалу теоретичних розробок та коректністю використаних математичних методів;

- апробацією результатів дисертаційних досліджень на наукових конференціях та публікаціями у фахових журналах теоретичного матеріалу;

- результатами проведених експериментів та ефективним практичним впровадженням.

Наукова новизна одержаних результатів полягає в наступному:

- набула подальшого розвитку модель процесу виявлення бот-мереж в корпоративних мережах на основі аналізу DNS-трафіка. Розроблена модель відрізняється від відомих моделей тим, що задіює розроблені модель DNS-трафіка та модель бот-мереж з врахуванням системи доменних імен.

- вперше розроблено метод ідентифікації бот-мереж у корпоративних мережах на основі їх групової активності в DNS-трафіку, який, на відміну від відомих, уможливлює уточнений поділ періоду моніторингу на інтервали, в межах яких здійснюється пошук груп інфікованих комп'ютерних систем, що ґрунтується на основі аналізу значень TTL, які містяться в DNS-повідомленнях, використовує нову ознаку синхронності DNS-запитів.

- вперше розроблено метод виявлення бот-мереж, які застосовують технології ухилення від виявлення на основі DNS, у корпоративних мережах, який ґрунтується на залученні кластерного аналізу множини ознак, одержаних з корисного навантаження DNS-повідомлень.

- набула подальшого розвитку інформаційна технологія виявлення бот-мереж в корпоративних мережах на основі аналізу DNS-трафіка, яка дозволяє ідентифікувати боти, що здійснюють групову активність в DNS-трафіку, а

також виявляти боти бот-мереж, які застосовують технології ухилення від виявлення на основі DNS.

Практичне значення одержаних результатів.

Розроблено програмне забезпечення інформаційної технології виявлення бот-мереж в корпоративних мережах на основі аналізу DNS-трафіка. Результати експериментальних досліджень з використанням розробленого програмного забезпечення підтверджують вірність наукових положень запропонованої інформаційної технології, оскільки впровадження інформаційної технології підвищує достовірність діагностування на 8-22% у порівнянні з відомими програмними засобами виявлення бот-мереж.

Теоретичні та практичні результати роботи впроваджено: державне підприємство «Новатор», відділ автоматизованих систем управління; товариство з обмеженою відповідальністю «ITT - telecommunication company»; у навчальному процесі Хмельницького національного університету.

Зміст дисертації висвітлено у чотирьох розділах.

У першому розділі проаналізовано відомі технології виявлення бот-мереж; досліджено принципи функціонування бот-мереж з врахуванням системи доменних імен (DNS) та методи, на яких базуються ІТ виявлення бот-мереж на основі DNS.

У другому розділі розроблено модель бот-мереж з врахуванням системи доменних імен, а також використання бот-мережами технологій ухилення від виявлення на основі DNS, що надає можливість підвищити достовірність виявлення бот-мереж в корпоративній мережі; розроблено модель DNS-трафіка та модель процесу виявлення бот-мереж в корпоративних мережах на основі аналізу вхідного DNS-трафіка, яка ґрунтується на розроблених моделі бот-мереж та моделі DNS-трафіка; розроблено модель процесу виявлення бот-мереж в корпоративних мережах на основі аналізу вхідного DNS-трафіка є основою методів виявлення бот-мереж на основі аналізу DNS-трафіка.

У третьому розділі розроблено метод ідентифікації бот-мереж на основі їх групової активності в DNS-трафіку, що надало можливість ідентифікувати

як відомі, так і ще невідомі бот-мережі, а також здійснювати раннє виявлення – на початковій стадії поширення інфекції в мережі; розроблено метод виявлення бот-мереж, які застосовують технології ухилення від виявлення на основі DNS, що дозволяє виявляти боти відомих та нових бот-мереж, які використовують такі технології ухилення, вже на початковій стадії поширення інфекції в мережі; запропоновано методику визначення ефективності та достовірності інформаційної технології виявлення бот-мереж на основі аналізу DNS-трафіка.

У четвертому розділі розроблено алгоритми виявлення бот-мереж та програмне забезпечення, яке реалізує інформаційну технологію виявлення бот-мереж на основі аналізу DNS-трафіка; розроблено інформаційну технологію виявлення бот-мереж в корпоративних мережах на основі аналізу DNS-трафіка, яка дозволяє ідентифікувати боти, що здійснюють групову активність в DNS-трафіку, а також виявляти боти бот-мереж, які застосовують технології ухилення від виявлення на основі DNS; розроблено програмне забезпечення, яке дозволяє виявляти боти відомих та невідомих бот-мереж в корпоративній мережі.

Дисертація є завершеною науковою працею.

Повнота викладу основних результатів дисертації в наукових виданнях.

Основні результати дисертації доповідались та обговорювались на: Міжнародній конференції «Контроль і управління в складних системах» (м. Вінниця, 2014 р.); Міжнародній науково-практичній конференції молодих вчених та студентів «Інформаційне, програмне та технічне забезпечення систем управління організаційно-технологічними комплексами» (м. Луцьк, 2015 р.); Computer Networks International Conference (Брунов, Польща, 2015, 2016 рр.); International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (Варшава, Польща, 2015 р.); Cyber Forum DESSERT B2S-S2B (м. Чернівці, 2016) та інших.

За результатами проведених досліджень опубліковано 16 наукових публікацій, з них 6 статей, опублікованих у наукових фахових виданнях України (2 з яких є одноосібними), 3 – у виданнях, зареєстрованих в наукометричній базі Index Copernicus, і 2 – у періодичних закордонних виданнях, зареєстрованих у наукометричній базі Scopus, 1 з яких – у виданні, зареєстрованому в наукометричній базі Web of Science, 8 – у матеріалах конференцій, з них 1 – індексоване у наукометричних базах Scopus та Web of Science, та 1 патент на корисну модель.

Зміст автореферату та основні положення дисертації ідентичні, а їх оформлення відповідають чинним вимогам.

Зауваження до дисертації.

1. При побудові моделі бот-мережі з врахуванням DNS доцільно враховувати інженерні та організаційні засоби протидії шкідливому програмному забезпеченню. До прикладу, такі як налаштування локальних політик безпеки доступу (зокрема, формування прикладними програмами DNS-запитів), заборона звернень до зовнішніх DNS серверів та інші.

2. Враховуючи, що розробники шкідливого програмного забезпечення завжди на крок попереду технологій захисту, у рамках роботи цікавим був би прогноз щодо можливих шляхів ухилення бот-мережами від виявлення запропонованими підходами.

3. Для проведення експериментів по виявленню бот-мережі варто було б розглянути декілька патернів згенерованого програмного забезпечення з функційним навантаженням ботів.

4. У тексті дисертації подекуди (наприклад п. 5 висновків до дисертації) спостерігається надмірне вживання підрядних зворотів у реченнях, що дещо ускладнює розуміння отриманих результатів.

Висновок.

Вказані недоліки не применшують цінності дисертаційної роботи, яка викликає науковий і практичний інтерес, присвячена розробленню інформаційної технології виявлення бот-мереж у корпоративних мережах на основі

аналізу DNS-трафіка, дозволяє підвищити достовірність процесу виявлення бот-мереж в порівнянні з відомими інформаційними технологіями на 8-22% та виявляти як відомі, так і нові бот-мережі.

Дисертаційна робота Бобровнікової К. Ю. «Інформаційна технологія виявлення бот-мереж у корпоративних мережах на основі аналізу DNS-трафіка» за актуальністю тематики, рівнем виконання, новизною результатів, їх науковим і практичним значенням, обґрунтованістю висновків відповідає вимогам «Порядку присудження наукових ступенів», що висуваються до кандидатських дисертацій з технічних наук.

Зміст дисертації відповідає спеціальності 05.13.06 – інформаційні технології, а її автор, Бобровнікова Кіра Юліївна, заслуговує присудження наукового ступеня кандидата технічних наук.

Завідувач кафедри кібербезпеки
Тернопільського національного
технічного університету ім. Івана Пулюя,
к.т.н., доцент Р.О. Козак

Підпис Козака Р. О. засвідчую
Вчений секретар Крамар Г.М.