Тестове зображення з низькою деталізацією при відсутності стеганограми є «чистим» вже на 1-му рівні ДДВП без розкладу в квадродерево, тоді як для тестового зображення з високою деталізацією необхідний розклад в квадродерево для перевірки наявності прихованого повідомлення. Після роботи алгоритму для зображення з високою деталізацією отримані 4 «чисті» блоки розміром 8×8 пікселів. У випадку заповненого контейнеру обидва тестові ЦЗ є підозрілими згідно критерію СКВ, тому необхідно провести розклад обох зображень в квадродерево.

Після роботи алгоритму отриманий наступний результат: в обох зображеннях відсутні «чисті» блоки, тому зроблений висновок, що в розглянутих ЦЗ присутня стеганограма, вбудована за МКДБ. Для аналізу ефективності розробленого алгоритму розглянуто 2 групи зображень – з високою та низькою деталізацією. Кожна група складалася з 10 високоякісних зображень (наявний АБГШ з дисперсією $\sigma^2 << 10^{-2}$), що мають розмір 1280×1024 (пікс) та досліджувалися при степенях заповнення від 5% до 25%.

За результатами проведеного аналізу зроблений висновок, що розроблений алгоритм дозволяє виявляти приховані на основі МКДБ повідомлення при степені заповнення не менше 10% для зображень з високою деталізацією, та не менше 5% – для ЦЗ з низькою деталізацією.

Висновок

Представлений алгоритм має використовуватися при проектуванні КСЗІ у автоматизованих системах програмного захисту з метою попередження витоку конфіденційної інформації з внутрішньої локальної мережі ОІД до глобальної мережі Інтернет.

ЛІТЕРАТУРА

1. Домарев В.В. Безопасность информационных технологий. Системный подход [Монография]. – К.: ООО ТИД Диа Софт, 2004. – 992 с.

2. Ярочкин В.И. Информационная безопасность [Монография]. – Учебник для студентов вузов. 2-е изд. – М.: Гаудеамус, 2004. – 544 с.

3. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам [Текст]. – Учебное пособие. – М.: Горячая линия-Телеком, 2005. – 416 с.: ил.

4. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика [Текст]. – К.: «МК-Пресс», 2006. – 288 с., ил.

5. M. Kutter, F, Jordan, F, Bossen. Digital signature of color images using amplitude modulation [Text]. – Proc. of the SPIE storage and retrieval for image and video databases Vol. 3022, 1997, – p.518-526.

6. Чарльз К. Чуи. Введение в вейвлеты [Текст]: пер с англ. Я.М. Жилейкина – М.: Мир, 2001. – 412 с.

7. Гонсалес Р., Вудс Р. Цифровая обработка изображений [Текст]. – М.: Техносфера, 2005, - 1072 с.

Надійшла: 30.07.2012 р.

Рецензент: д.т.н., професор Конахович Г.Ф.

УДК 004.056.53

Пасько О.З., Пархоменко І.І., Пономаренко О.В.

БОТ-МЕРЕЖІ ЯК ЗАСІБ ВЕДЕННЯ КІБЕРВІЙН

У даній статті була розглянута проблема захисту інформаційного простору від шкідливого коду ботнет. Суть якої в складності виявлення та нейтралізації інфікованої мережі та центру її керування. Надалі були надані рекомендації щодо вибору організаційних, програмних та апаратних механізмів захисту комп'ютерних мереж від інфікування ботом.

Ключові слова: ботнет, центр управління, файрвол, антивірус, сніфер, спам-фільтр, антируткіт, аналітичний модуль.

Вступ. На тлі проблем розкрадання даних, шпигунства та витоку інформації, комп'ютерних вірусів та хакерських атак, особливу увагу варто приділити кібер війнам, які ведуть державні структури, і які стають серйозною загрозою для національної безпеки. Їхні

цілі становлять набагато вищий рівень загрози – це спроби заволодіти важливими інфраструктурними об'єктами, зокрема такими як енергетична, телекомунікаційна, фінансова системи тощо.

Постановка проблеми. Одним із методів ведення кібер війн є бот-мережі (ботнети), які все більше виділяються на фоні різноманітного інструментарію зловмисників. Ботнет - безліч підмереж, простягнутих по каналах інтернет автономними клієнтами [1], у ролі яких виступають спеціальні вірусні й шпигунські програми – боти. Вони паразитують як на звичайних персональних комп'ютерах і серверах, так і на мережному обладнанні; крім того варто додати те, що бот-код сам забезпечує свою життєдіяльність (реплікація, самозахист, механізми маскування та автозапуску), хоча в кінцевому рахунку підпорядковується своєму господарю, який займається його координуванням та активацією. Процес виявлення та нейтралізації бот-мереж є досить складним та довготривалим. По-перше, враховуючи те, що бот-код має модульну структуру - він здатний до швидкого оновлення своїх баз. По-друге розробники ботнет все частіше застосовують peer-to-peer (P2P) топологію, а тому захопити центр управління та нейтралізувати його стає досить складно.

Постановка завдання. Метою даної роботи є розробка необхідних рекомендацій для захисту інформаційного простору від бот-мереж. Постановка завдання полягає у наступному: розробка порад щодо реалізації організаційних заходів захисту від інформаційних загроз типу ботнет; огляд сучасних програмних методів захисту комп’ютерних систем від шкідливого коду; розробка порад щодо адекватного вибору програмних рішень для побудови системи захисту від бот-мереж; огляд сучасного апаратного забезпечення для захисту комп’ютерних мереж від атак зі сторони ботнет.

Основна частина. Взявши до уваги те, що створення бот-мереж конкретно не прив’язане до жодної країни, оскільки до їх складу входять комп’ютери різних національних доменів, то можна стверджувати, що захист користувачів тої чи іншої континентальної території – це не локальна проблема, а глобальна. Тобто дану задачу потрібно виводити на новий рівень – міжнаціональний.

Всю масштабність загрози, яка надходить від бот-мереж показує те, що для протидії був створений спеціальний альянс – Cyber Security Protection Alliance (ICSPA) [2]. В нього входить компанія Panda Security, а також «Лабораторія Касперського», де працюють вірусні аналітики, які досліджують типологію та особливості побудови ботнет і розробляють відповідні системи захисту. Проте яким би ефективним та дієвим не був ICSPA, він не в змозі захистити весь інформаційний простір, оскільки захист потрібно починати будувати так, як і будинок – з фундаменту. У даному випадку це комп’ютери локальних мереж та домашні користувачі. Зокрема, для зменшення ймовірності зараження окремої робочої станції потрібно слідувати декільком правилам. По-перше, необхідно виконувати певні настанови організаційних заходів, розглянемо їх детальніше.

Обережно використовувати флеш-носії та проводити їх повну перевірку при підключенні до комп’ютера. Тут мається на увазі те, що при підключенні до комп’ютера всі змінні носії потрібно перевіряти на наявність шкідливого коду за допомогою попередньо інстальованої антивірусної програми. Щодо вибору необхідного антивірусного захисту, то перш за все керуються тим для чого саме він потрібен – в нашому випадку це захист від атак зі сторони ботнет та уникнення зараження шкідливим кодом. Цьому призначенню найбільш підходить рішення Dr.Web Security Space 7.0.5.04110 [3].

Звісно вище рекомендована програма не гарантує 100% ефективності, тому її роботу рекомендовано час від часу перевіряти додатковим програмним забезпеченням. Серед даних засобів виділяються такі лікуючі утиліти [4]: Dr.Web CureIt! (детектування та лікування шкідливих об’єктів у системі); Dr.Web CureNet! (віддалена перевірка та лікування локальних мереж).

Також для перевірки якості роботи системи захисту можна використовувати спеціальні антибот-монітори, які не впливають на роботу антивірусних програм. Серед новинок виділяється програма Norton AntiBot [5].

Не надавати конфіденційної інформації (персональні дані, паролі, які застосовує користувач під час користування сервісами Інтернет) через будь-яку комп'ютерну мережу. У випадку розголошення цих даних клієнту може буде завдано шкоди, зокрема, розголошення паролю кредитної карти на порталі WebMoney чи Portmone в майбутньому призведе до несанкціонованого зняття коштів із рахунку користувача.

Не завантажувати та не встановлювати програми невідомого походження, оскільки вони можуть містити шкідливий код, а також не відкривати архіви з файлами всупереч попередженням інстальованої антивірусної програми.

Не заходити на сайти, які браузер позначає як небезпечні: вони можуть містити шкідливий контент.

Для уникнення несанкціонованого доступу до комп'ютера варто використовувати певні механізми авторизації, наприклад, пароль.

Варто додати, що потрібно *використовувати надійні паролі та зберігати їх у таємниці*, адже існують спеціальні програми – парольні зломщики, які виконують підбір ключової послідовності як шляхом повного перебору символів, так і через пошук по словнику. Отже, для запобігання створення ненадійного паролю:

- не використовувати послідовні комбінації та символи, які повторюються, наприклад, «12345678», «222222» або комбінації сусідніх літер на клавіатурі;
- варто звертати увагу на довжину паролів, які використовуються в системі, адже це є чи не основним критерієм, що визначає його ефективність; як альтернативу можна використовувати парольні фрази, які зазвичай є довшими, проте, з іншої сторони, рекомендовано, щоб кількість символів не перевищувала 14 знаків (це для збереження сумісності різних операційних систем);
- з обережністю використовувати заміну деяких символів на подібні цифри. Шахраїв та інших зловмисників, які мають достатній рівень знань для підбору та злому паролів, не вдасться ввести в оману замінами подібними до «і» на «1», або «а» на «@» у словах «M1cr0$0ft» або «П@р0ль»;
- слід використовувати букви як нижнього, так і верхнього регістру;
- не використовувати особисті дані (свої або своїх близьких) у якості паролю: цю інформацію зловмисники використають в першу чергу;
- не використовувати словникові слова (на будь-якій мові), оскільки існує спеціальне програмне забезпечення призначене для підбору паролів шляхом повного перебору слів у всіх існуючих словниках;
- використовувати декілька паролів, адже під час злому комп'ютера чи певної системи, де використовується один і той же пароль, небезпеці піддаються усі дані, захищені одною і тою ж ключовою послідовністю;
- оскільки більшість паролів користувача зберігаються на комп'ютері, то варто застосувати додаткові заходи для уникнення його злому із зовні (для початку, наприклад, закрити віддалений доступ);
- не зберігати паролі в Інтернеті - зловмисник, отримавши доступ до них, отримує доступ до всіх захищених ними даних.

Перед тим як перейти до огляду та вибору спектру представлених програмних засобів захисту варто нагадати, що ціль ботнету - встановити на комп'ютері жертви утиліту дистанційного управління, розробники якої знаходять все новіші методи проникнення шкідливого коду в систему. Саме через це потрібно обрати такі заходи, які могли б якщо не закрити всі двері для проникнення бота в комп'ютер, то хоча б детектувати його наявність для того, щоб користувач зміг вирішити цю проблему самостійно. Отже потрібен багатосторонній захист.

Як один із захисних механізмів варто обрати *персональний файрвол.* Міжмережевий екран (firewall) або мережевий екран – комплекс апаратних чи програмних засобів, що здійснює контроль і фільтрацію мережевих пакетів, які проходять через нього, на різних рівнях моделі OSI, відповідно до заданих користувачем правил з метою цілісного захисту комп'ютерної мережі від ворожого середовища [6]. Рекомендовано зупинити свій вибір на

Comodo Firewall [3], що має вбудовану функцію сніфера. Це надає можливість проаналізувати будь-яке з'єднання із зовнішнім середовищем.

Крім того програма містить захисні механізми проти примусового відключення її роботи, що є чи не основним критерієм під час вибору захисту від бот коду, який має здатність блокувати роботу захисного програмного забезпечення. Для захисту від *спам атак* (на рівні комп'ютера користувача) варто застосовувати спеціально налаштовані спам-фільтри для поштового клієнту, що інстальований в систему та використовується для роботи.

Спам-фільтр – це програмне забезпечення для автоматичного детектування спаму, яке призначене для використання кінцевими користувачами або серверами і дозволяє фільтрувати листування від спам розсилок.

Практично всі спам-фільтри використовують два основні методи фільтрації: аналіз змісту листа; аналіз відправника листа.

Варто додати, що серед спам-фільтрів є як окремі програмні розробки, які інкапсулюються в поштовий клієнт, так і вже вбудовані функціональні модулі, які потрібно лиш налаштувати належним чином. Беручи до уваги те, що бот код містить захисні механізми маскування - слід систематично перевіряти наявність замаскованих під системні процеси шкідливих кодів за допомогою антируткіт утиліт.

Руткіт (від англ. root kit, тобто «набір root'а») – це програма для приховування слідів присутності зловмисника або шкідливої програми в системі, вона замасковує її під системний процес [7, ст. 61]. Для виявлення і видалення подібних шкідливих програм існує безліч спеціалізованих програмних продуктів, які називаються, відповідно, антируткітами. Лідируючу позицію займає Rootkit Unhooker 3.7 [8].Проте варто сказати, що всі інстальовані на комп'ютері програмні продукти можуть мати свої вразливості («дірки» або люки (back door)) [3], які в подальшому можуть стати одним із шляхів проникнення бота в систему. Тому необхідно провіряти та обновлювати все те програмне забезпечення, яке використовується користувачем.

По-перше, необхідно закрити проломи в роботі самої головної програми – операційної системи (ОС). Варто нагадати, що використання ліцензійної ОС значно зменшить ризик зараження, оскільки сертифіковане програмне забезпечення гарантує виключення наявності шкідливого коду в середині програми. Плюс до цього використання ліцензійної ОС дає можливість своєчасно її оновлювати, що забезпечить зменшення помилок в її роботі. Варто додати, що існують спеціальні програмні розробки - сканери, які допомагають усунути наявні в програмному забезпеченні люки. Ці утиліти дозволяють виявити вразливості інстальованого програмного забезпечення на комп'ютері та шляхи їх нейтралізації (програма відразу видає рішення знайденої проблеми).

Сніфер. Проте може виникнути ситуація, коли бот, який проникнув в систему, не детектувався і в процесі не був видалений, тому варто розглянути специфічне програмне забезпечення, яке називається сніфером. Сніфер – це програма призначена для перехвату мережного трафіку, а оскільки при активації бот починає з'єднуватись із командним центром (через мережу) для отримання подальших інструкцій, то це є одним із найбільш дієвих методів виявлення наявності в системі шкідливого коду. Прикладом такого захисного механізму може слугувати BotSniffer, до функціональних можливостей якого входить здатність виявлення рис характерних для комп'ютерів інфікованих ботом, після чого він впроваджується до них в мережу і виходить на керуючий сервер ботнету, що дозволяє блокувати передачу команд по мережі. [9]

Щодо захисту локальних комп'ютерних мереж від атак, які спрямовані на перенавантаження пропускної здатності каналу, то тут можна зупинити свій вибір на розробках Cisco Traffic Anomaly Detector та Cisco Guard [10]. Перший модуль діє як система пасивного контролю з моніторингу мережного трафіку і спрямований на виявлення аномалій. Другий - Cisco Guard заснований на архітектурі процесу мультиверифікації і включає в себе 5 стадій з виявлення шкідливого мережного трафіку.

З іншої сторони можна оснастити маршрутизатори (чи комутатори) додатковим аналітичним модулем – McAfee Network Threat Behavior Analysis, який побудований на

основі алгоритмів систем виявлення вторгнень (intrusion detection system або IDS) та детектування аномалій (anomaly detection system або ADS) [11, ст.307]. Рішення оснащене власним чотирьох ядерними процесором та RAID-масивами. Аналітичний модуль призначений для збору трафіку та аналізу поведінки вузлів мережі та встановлених програм з метою виявлення черв'яків, бот-мереж та розвідувальних атак.

Висновки. Підводячи підсумки можна сказати, що в даній роботі було розглянуто: поради щодо реалізації організаційних заходів захисту від інформаційних загроз типу ботнет; сучасні програмні методи захисту комп'ютерних систем від шкідливого коду; рекомендації щодо реалізації програмної основи для побудови системи захисту від бот-мереж; сучасне апаратне забезпечення для захисту комп'ютерних мереж від атак зі сторони ботнет.

Беручи до уваги вище проаналізований матеріал, можна надати наступні рекомендації щодо забезпечення безпеки інформаційного простору:

1. По-перше, варто слідувати настановам організаційних заходів, зокрема – використовувати надійні паролі та зберігати їх у таємниці, для цього:довжина пароля повинна складати не менше 10 символів (до 14 знаків);

- в паролі повинні використовуватись різні регістри, цифри та спеціальні символи;
- паролі не повинні повторюватися;
- не зберігати ніяких ключових послідовностей та не надавати конфіденційної інформації через комп'ютерні мережі.

Також, не слід завантажувати та встановлювати програми невідомого походження та відкривати файлові архіви всупереч попередженням антивірусної програми, адже вони можуть містити шкідливі вкладення. Не варто ризикувати, заходячи на сайти, які браузер чи антивірусна програма позначає як небезпечні.

З іншої сторони всі змінні носії, при підключенні до комп'ютера, слід перевіряти на наявність шкідливих кодів.

2. По-друге, варто використовувати програмні захисні механізми різного призначення, зокрема:як персональний файрвол, рекомендовано обрати Comodo Firewall;

- потрібно використовувати додаткові антиспам програми або налаштувавати спам-фільтри для поштового клієнту, який використовується;
- вибір антивірусного захисту рекомендовано зупинити на рішенні Dr.Web Security Space;
- систематично перевіряти ефективність роботи створеної системи захисту шляхом використання антибот моніторів, які представленні рішенням Norton AntiBot;
- час від часу перевіряти наявність замаскованих під системні процеси шкідливих кодів за допомогою антируткіт утиліт, наприклад, Rootkit Unhooker 3.7;
- використовувати системні сканери для виявлення вразливостей програмного забезпечення комп'ютера та їх подальшої нейтралізації.

3. Щодо захисту локальних комп'ютерних мереж від зовнішніх атак зі сторони ботнет, то тут варто зупинити свій вибір на модулях Cisco Traffic Anomaly Detector та Cisco Guard. Крім того можна оснастити маршрутизатори (чи комутатори) додатковим аналітичним модулем - McAfee Network Threat Behavior Analysis, який побудований на основі алгоритмів систем виявлення вторгнень (intrusion detection system або IDS) та детектування аномалій (anomaly detection system або ADS).

ЛІТЕРАТУРА

1. За матеріалами сайту http://www.computerra.ru.
2. За матеріалами сайту http://www.spywarehelpcenter.com.
3. За матеріалами сайту http://www.anti-malware.ru/tests_history.
4. За матеріалами сайту http://www.antvirus.ru.

5. За матеріалами сайту http://www.winsecurity.ru/articles/.
6. За матеріалами сайту http://wiki.kspu.kr.ua.
7. Ken Dunham, Jim Melnick. Malicious Bots: An Inside Look into the Cyber-Criminal Underground of the Internet, 2008. – 168 p.
8. За матеріалами сайту http://infoch.info.
9. За матеріалами сайту http://www.winsecurity.ru/articles/.
10. За матеріалами сайту http://www.cisco.com.
11. Галушкін А.І. Нейронні мережі. Основи теорії. М.: Телеком, 2010. – 496 с.

Надійшла: 02.08.2012 р.

Рецензент: д.т.н., професор Юдін О.К.

УДК 004.056.5(045)

Пархоменко І.І., Пасько О.З.

ШТУЧНІ БІОЛОГІЧНІ СИСТЕМИ ЗАХИСТУ КОМП'ЮТЕРНИХ МЕРЕЖ

Ця стаття присвячена аналізу особливостей побудови штучних біологічних мереж як способу захисту комп'ютерних систем від зовнішніх атак. Прототипами цих штучних систем є захисні механізми живих істот: імунітет та нейрони.

Ключові слова: штучні нейронні мережі, штучні імунні мережі, нейромережний імунний детектор, багатошаровий персептрон, рециркуляційна нейронна мережа.

Постановка проблеми. В ході інтенсивного розвитку інформаційної сфери та ускладнення методів здійснення атак на її об'єкти, гостро постає проблема побудови надійної системи захисту. Дослідження, які проводяться в даній області, напрямлені на побудову досить специфічних мереж, прототипами яких є системи, що захищають живі організми від зовнішнього вторгнення або, якщо воно вже відбулось, спрямовані на ліквідування його наслідків. Такими системами, зокрема, являються нейронні та імунні механізми.

У даній роботі буде розглянуто:

1.Особливості функціонування штучних нейронних мереж;

2.Особливості функціонування штучних імунних мереж;

3.Можливість синтезу імунної та нейронної мережі для створення елементів (детекторів) єдиної захисної системи;

4.Особливості побудови та функціонування нейромережних імунних детекторів.

Аналіз останніх досліджень та публікацій. Проблема створення та функціонування нейронних та імунних мереж розглянута в публікаціях Галушкіна А.І. «Нейронні мережі. Основи теорії», Головко В.А. та Безобразова С.В «Штучні імунні системи для захисту інформації: виявлення і класифікація комп'ютерних вірусів», а також «Нейронні мережі: навчання, організація, застосування».

Постановка завдання. Розглянемо особливості створення та функціональні можливості штучної біологічної мережі, яка є синтезом як нейронної, так й імунної системи.

Основна частина. Спершу ознайомимось із самим поняттям штучних нейронних та імунних систем.

Штучна нейронна мережа [1, ст.93]. Штучні нейронні мережі (ШНМ) будуються по аналогії з відповідною системою живого організму. Проте перш ніж почати своє функціонування нейронні мережі спершу повинні навчатись протягом деякого періоду з метою формування вхідного вектору даних, за допомогою якого в майбутньому система буде вирішувати являється поведінка нормальною чи ні. Після навчання нейронна мережа запускається в режимі розпізнавання. Якщо у вхідному потоці не вдається розпізнати нормальну поведінку - фіксується факт атаки. Класичні нейронні мережі мають високу обчислювальну складність навчання, що ускладнює їх застосування на великих потоках даних.