2. Хохряков Г.Ф. Криминология: Учебник / Отв. ред. В.Н. Кудрявцев. – М.: Юристъ, 1999. – С. 264-265.

3. Див.: Кулагина И.Ю., Колюцкий В.Н. Возрастная психология: Полный жизненный цикл развития человека. Учебное пособие для студентов высших учебных заведений. – М.: ТЦ "Сфера", 2001. – С. 280-327.

4. Див.: Експрес-інформація про стан злочинності на території України за 2004 – 2008 рр. Частина 5. МВС України. Управління оперативної інформації. – Київ, 2008.

5. Див.: Ремшмидт Х. Подростковый и юношеский возраст. Проблемы становления личности. – М.: "Мир", 1994.

6. Долгова А.И., Ермаков В.Д., Беляева Н.В. Проблемы типологии несовершеннолетних преступников //Вопросы борьбы с преступностью. Вып. 24. – М., 1976. – С. 18-24.

7. Детальніше див.: Антонян Ю.М., Бородин С.В. Преступность и психологические аномалии. - М., 1987; Антонян Ю.М. Психологическое отчуждение ребенка и проблема "случайного" и " закономерного" преступного поведения. – Ереван, "Айстан", 1987; Пирожков В.Ф. Законы преступного мира молодежи (криминальная субкультура). - Тверь, издательство "Приз", 1994.

8. Див.: Криминология: Учебник для вузов / Под общ. ред. проф. А.И. Долговой. – 2-е изд., перераб. и доп. – М.: Издательство НОРМА, 2001. – С. 31-39.

9. Социально-психологическая характеристика личности несовершеннолетнего преступника : сборник научных трудов о программе исследования личности несовершеннолетнего преступника и социальной ситуации ее развития / под ред. Г. М. Миньковского. – М. : Ротапринт Всесоюз. ин-та по изучению причин и разработке мер предупрежд. преступн., 1975. – С. 115.

Стаття надійшла до редколегії 27.05.2010 р.

УДК 343.346.8

І.О. Вороное

ФЕНОМЕН BOTNET – ЛАТЕНТНА МОБІЛІЗАЦІЯ СЕГМЕНТІВ МЕРЕЖІ ІНТЕРНЕТ ДЛЯ ВЧИНЕННЯ ЗЛОЧИНІВ У СФЕРІ ВИСОКИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Мета статті полягає у дослідженні феномену ботнет, аналізу відповідної термінології, систематизації основних напрямків використання сегментів мережі та визначенні концептуальних заходів протидії цьому явищу. Внесено пропозиції щодо організації нових досліджень.

Ключові слова: *ботнет, злочини у сфері високих інформаційних технологій, латентна мобілізація, сегменти Інтернет, цифрова інформація, методика розслідування.*

Цель статьи заключается в исследовании феномена ботнет, анализе соответствующей терминологии, систематизации основных направлений использования сегментов сети, и определении концептуальных мероприятий противодействия этому явлению. Внесены предложения относительно организации новых исследований.

Ключевые слова: *ботнет, преступления в сфере высоких информационных технологий, сегменты Интернет, цифровая информация, методика расследования.*

Annotation: The purpose of the article is to study the phenomenon of Botnet, analyze the relevant terminology, systematization of the main directions of use of network segments and definition of conceptual measures to counteract this phenomenon. The proposals for organization of new researches have been made.

Keywords: *botnet, high-tech information crimes, latent mobilization, Internet segments, digital information, criminal investigation.*

У сучасному світі найпродуктивнішими з точки зору генерації новітніх протиправних ідей, без сумніву, є високі інформаційні технології – наукоємні універсальні та багатофункціональні технології, що мають широку сферу застосування і здатні викликати ланцюгову реакцію не тільки корисних дій. Властивості та можливості високих інформаційних технологій постійно привертають увагу кримінального суспільства, яке використовує та пристосовує їх для власних функціональних потреб та вчинення злочинів.

Проблемам розкриття та розслідування злочинів у сфері високих інформаційних технологій присвячені наукові розробки вчених України і інших держав СНД: П.Д. Біленчука, А.С. Білоусова, Л.В. Борисової, В.М. Бутузова, Н.Л. Волкової, В.Б. Вєхова, Ю.В. Гавриліна, В.О. Голубєва, А.І. Журби, В.Є. Козлова, В.В. Крилова, В.О. Мєщерякова, Ю.Ю. Орлова, Д.В. Пашнєва, В.Д. Поливанюка, О.А. Самойленко, О.І. Усова, І.Ф. Харабе-рюша, В.П. Шеломєнцева та інших.

Разом з тим, незважаючи на активізацію зусиль, спрямованих на протидію означеним злочинам, комплексного дослідження феномену Botnet – латентної мобілізації сегментів мережі Інтернет для вчинення злочинів у сфері високих інформаційних технологій представниками відомчої науки ще не здійснено, що свідчить про актуальність обраної теми дослідження, її наукову і практичну значущість.

Науково-теоретичне підґрунтя дослідження склали праці фахівців дальнього зарубіжжя: Тростен Хольтца (Thorsten Holtz), Кена Дунгама (Ken Dunham), Джима Мєльніка, (Jim Melnick), Карума Дамбека (Karun Dambiec), Лі Венка (Lee Wenke) та інших.

Розвиток високих інформаційних технологій та глобальний процес інформатизації створює для злочинності доволі сприятливі умови. Орієнтація кримінальної спільноти на використання високих інформаційних

технологій зумовлюється перспективністю їх використання у кримінальній діяльності. По-перше, це рентабельно, оскільки вже сформована відповідна необхідна інформаційна інфраструктура, не має потреб здійснювати значні витрати на її створення, підтримку та подальший розвиток. По-друге, кримінальні структури є частиною суспільства і завдяки цьому унеможливлюється реалізація вибірковості у розповсюдженні програмних та апаратних засобів. По-третє, внаслідок розвитку суспільства, його залежність від високих інформаційних технологій набуває прямо пропорційну лінійну форму. І, насамкінець, швидка ротація високих інформаційних технологій призводить до скорочення строків інноваційного циклу певного засобу, насамперед програмного, створюючи при цьому їх постійну динамічну конкуренцію, внаслідок якої постійно зростає кількість можливих способів вчинення злочинів в одиницю часу.

Таким чином, вчасне визначення фактичних тенденцій, необхідність постійного відстеження можливостей та розпізнавання інноваційних форм злочинної діяльності має принципове значення. У цьому аспекті привертає увагу масштабне багатоцільове використання інформаційно-технічних ресурсів мережі Інтернет, яке можна визначити як латентну мобілізацію комп'ютерів для вчинення низки злочинів.

Мета статті полягає у дослідженні феномену ботнет, проведенні аналізу відповідної термінології, систематизації основних напрямків використання сегментів мережі та визначенні концептуальних заходів протидії цьому явищу.

Відповідно до мети визначимо основні завдання дослідження ботнет:

- проаналізувати відповідну термінологію та з'ясувати ступінь вивченості досліджуваної проблеми у вітчизняній і зарубіжній теорії та практиці;
- відстежити історію виникнення та розвитку;
- визначити структуру та надати належну класифікацію означених мереж;
- надати характеристику та розглянути основні напрямки використання, у тому числі визначити перспективні;
- запропонувати заходи протидії використанню у злочинних цілях.

Аналіз зарубіжних джерел, свідчить, що для позначення "захопленої" мережі комп'ютерів використовується термін Botnet, який є скороченим збірним поняттям від англійських слів robot и network.[1] Термін "ботнет" можна вважати загальним поняттям і використовувати у сполученні зі словом "мережа", за аналогію як "мережа Інтернет". У загальному визначенні ботмережа – це субмережа, що виникає внаслідок загальної або часткової мобілізації ресурсів, яка проводиться відкрито або приховано для зосередження сил та засобів з певною метою.

[1] Lee Wenke, Wang Cliff, Dagon David. Botnet Detection, 2008. – 168 p.

Краще розуміння Botnets допомагатиме координувати і розвивати різні технології, щоб протистояти цій серйозній загрозі безпеки.

Виникнення та розвиток феномену ботнет тісно пов'язано з "комп'ютерною" злочинністю, а саме з етапами її розвитку. Відомо, що спочатку такі злочини вчинялися з безпосереднім використанням певного комп'ютера, який автономно зберігав та обробляв інформацію. Виникнення мережевих технологій дозволило підключатися до інших комп'ютерів і вчиняти злочин вже дистанційно. Згодом, за допомогою все тих же мереж, злочинці почали з метою збільшення своїх можливостей об'єднуватися для здійснення так званих "атак" на певні комп'ютери. Започатковується та відпрацьовується новий принцип високотехнологічної злочинної діяльності, згідно з якою можливості одного програмно-апаратного комплексу помножуються на їхню кількість. Спочатку певна кількість необхідних технічних засобів досягалася за рахунок комп'ютерів, які належали членам злочинного угрупування. Виникнення та вдосконалення телекомунікаційних програмних засобів надали можливість одному користувачу встановлювати контроль над великою кількістю комп'ютерів і керувати ними.

В основу створення ботнетів було покладено принцип мережного адміністрування. Як адміністратор керує певною корпоративною мережею, так і злочинець заради досягнення мети використовує віддалений доступ для керування комп'ютерами, підключеними до неї.

Історія сучасних ботнетів тісно пов'язана з появою і розвитком "троянських" програм, які активно використовувалися для прихованого збору таких даних як номери кредитних карток, стан грошевого рахунку, коди ліцензійного програмного забезпечення, кодів доступу до різних послуг, тощо.[1] Бажання розширити можливості програм для збору даних шляхом доповнення їх функцією віддаленого управління призвело до появи приблизно у 1999 році нових рішень – NetBus і BackOrifice2000. Зазначені програмні пакети містили у собі набір функцій для опосередкованого керування комп'ютером і дозволяли запускати певні програми, отримувати знімки з екрану монітора, відкривати і закривати привід для зчитування компакт-дисків. Вже через рік, у 2000 році вищевказані програмні засоби могли керувати вже декількома комп'ютерами одночасно, але пасивно очікували безпосереднього з'єднання з боку керуючого. Наступне вдосконалення призвело до того, що програма сама відкривала порт зв'язку і встановлювала з'єднання. При постійному включенні такий комп'ютер знаходився на перманентному двосторонньому зв'язку, тобто в реальному масштабі часу отримував команди й звітував про їх виконання.

[1] Ken Dunham, Jim Melnick. Malicious Bots: An Inside Look into the Cyber-Criminal Underground of the Internet, 2008. – 168 p.

В той же час з'явилися перші публікації з цієї тематики, переважно у хакерських Інтернет-виданнях, які ще більше привернули увагу та зацікавили широку аудиторію. На жаль, в неї не виявилося вітчизняних юристів, правоохоронців, або вони не придали належного значення новому технологічному рішенню у сфері високих інформаційних технологій. Як наслідок у черговий раз не був зроблений аналіз його можливого використання та негативних наслідків.

Взаємодія між складовими комп'ютерами мережі ботнет відбувається за допомогою мережевих протоколів, типи яких є підставою для їх класифікації. За типом протоколів, що використовуються, мережі ботнет поділяються на такі групи як IRC, IM та Web – орієнтовані.

IRC-орієнтовані мережі відносяться до найперших видів ботнетов, де керування ботами здійснювалося на основі IRC (Internet Relay Chat) – сервісу Інтернет, який надає користувачам можливість спілкування шляхом надсилання текстових повідомлень багатьом кореспондентам з усього світу одночасно (в режимі реального часу). Кожен комп'ютер з'єднувався із зазначеним у програми-бота IRC-сервером, заходив на певний канал і чекав наступних команд.

IM-орієнтовані являються не дуже популярним видом ботнетів. Відрізняються від своїх IRC-орієнтованих аналогів тільки тим, що для передачі даних використають певні канали IM-служб (Instant Messaging – системи миттєвої передачі повідомлень), наприклад AOL, MSN, ICQ та ін. Невисока популярність таких ботнетів обумовлена складностями, що виникають при створенні окремого аккаунта, тобто облікового запису у комп'ютерній системі як сукупності засобів та прав користувача IM-служби для кожного бота. Справа в тому, що боти повинні виходити в мережу й постійно бути присутнім в режимі он-лайн. Оскільки більшість IM-служб не дозволяють входити в систему з різних комп'ютерів, використовуючи той самий аккаунт, у кожного бота повинен бути свій номер IM-служби. При цьому власники IM-служб усіляко перешкоджають будь-якій автоматичній реєстрації акаунтів. У результаті адміністратори IM-орієнтованих ботнетів значно обмежені в числі наявних зареєстрованих акаунтів, а значить й у числі ботів, одночасно присутніх у мережі. Звичайно, боти можуть використати той самий акаунт, виходити в онлайн один раз у певний проміжок часу, відсилати дані на номер хазяїна й протягом короткого проміжку часу очікувати відповіді. Але це породжувало проблему швидкого реагування на відповідні команди.

Web-орієнтовані – це відносно новий тип ботнетів, що швидко розвиваються завдяки відносної легкості розробки, великої кількості web-серверів в Інтернеті й простоти керування. Для керування web-орієнтованих ботнетів використовується CGI (від англ. Common Gateway Interface – загальний інтерфейс шлюзу, який використовується для зв'язку зовнішньої програми з web-сервером).

Обравши найліпший тип протоколу обміну, створювачі ботнетів швидко переключилися на дослідження можливих варіантів їх архітектури. Виявилось, що ботмережа з єдиним центром керування вельми уразлива. Єдиний центр керування був класичним технологічним рішенням для управління, але одночасно виступав критичним вузлом, оскільки його виявлення і відключення неминуче призводило до припинення існування ботмережі. Це надало поштовх до створення ботнетів з іншою архітектурою. Стали проводитися відповідні експерименти, внаслідок яких було знайдено чергове необхідне технологічне рішення. У 2007 році виникли та почали розвиватися ботмережі, у яких функції центру міг виконувати будь-який комп'ютер системи. Архітектура, покладена в основу при їх створенні, отримала назву P2P (від англ. "peer-to-peer" – від рівноправного до рівноправного, тобто один користувач мережі, який надає ресурси іншому учаснику одноранговой мережі, користується його ресурсами).

За типом архітектури ботмережі поділяються на мережі з єдиним центром керування або децентралізовані. У мережі ботнет з єдиним центром керування усі комп'ютери з'єднуються з важливим фрагментом, який позначається як C&C (Command&Control Centre – командно-управлінський центр). Він виступає ключовою ланкою у функціонуванні такої мережі, оскільки знаходиться у режимі постійного очікування підключення комп'ютерів, яких реєструє у своїй базі даних. За допомогою центру здійснюється й наступне спостереження за роботою підключених комп'ютерів та розсилка необхідних команд. Для керування централізованою мережею особою, яка її створила, достатньо мати безпосередній або віддалений доступ. Останній має низку переваг. Мережі з єдиним центром керування являються найпоширенішим типом, виходячи з того, що їх легше створювати та керувати ними. Проте, й нейтралізація побудованих за таким принципом мереж можлива шляхом виявлення їх центру.

У мережі ботнет з децентралізованим керуванням P2P комп'ютери з'єднуються з певним комп'ютером, що вже є її складовим елементом. Кожен комп'ютер такої мережі має список своїх "сусідів" для того, щоб при отриманні команди передавати її іншому. Таким чином, керування цією мережею можливе при наявності доступу, знов таки, безпосередньому або віддаленому до хоча б одного з цієї системи комп'ютерів.

Для швидкого зростання кількості "захоплених" комп'ютерів, як правило, здійснюється підпорядкування не тільки, а може і не стільки комп'ютерів окремих користувачів в мережі, скільки серверів локальних мереж. Підпорядковані комп'ютери можуть стати засобами приєднання цілих корпоративних мереж. За такою схемою відбувається швидка будова злочинної технічної "піраміди". Після встановлення контролю над

окремим комп'ютером або цілою локальною чи корпоративною мережею останні підключаються до командного центра для отримання подальших інструкцій.

Для створення ботмереж використовується багато методів, зокрема соціальної інженерії, що дозволяють за короткий проміжок часу швидко збільшувати кількість залучених комп'ютерів. Впровадження кодів спеціальних програм здійснюється за допомогою web-сайтів, у тому числі спеціально створених, електронної пошти, пристроїв уводу-виводу.

Технічна спадкоємність також відіграло не останню роль, оскільки завдяки їй ботнети з єдиним центром керування швидко перебудовувалися або приєднувалися до необхідних фрагментів мережі. Для постійного активного залучення ресурсів комп'ютера як найменшої структурної одиниці ботмережі, провокаційно розповсюджуються привабливі посилання, наприклад на останню версію ліцензійного програмного забезпечення або нові розважальні програми, популярні фільми, ігри. Для здійснення підключення використовується масова або сфокусована розсилка поштових листів, відкриття яких запускає необхідну програму для встановлення контролю над ресурсами комп'ютера. Не останню роль відіграють у широкому залученні нових комп'ютерів як складових ботмереж сайти з порнографією, які, на жаль, мають численну кількість відвідувачів. По суті, для встановлення контролю над ресурсами комп'ютера необхідно, щоб користувач погодився з посиланням або відкрив отримане поштове повідомлення.

Для забезпечення самого процесу будови бот-мережі поряд з власними дослідженнями можливих технологій створення активно використовується перевірений та усталений метод – купівля заздалегідь зарезервованих уразливих місць програмного забезпечення масового використання. Вартість невідомої уразливості в операційній системі або популярному браузері може скласти десятки тисяч доларів.

Практично у любому елементі програмного забезпечення, особливо великого об'єму, криються свої секрети, знайти які не просто, оскільки програмний код замасковано під реально існуючий алгоритм або його частину. Так, наприклад, кількість виявлених побічних фрагментів коду дорівнюється: в програмних оболонках Windows XP – 2, Linux – 3, Fine Reader – 2, Adobe – 12, Ahead Nero Burning – 3, Microsoft Office – 17, WinRaR – 2, іграх Half-Life – 20, Max Payne – 13, WarCraft3 – 8, Quake III Arena – 7 відповідно[1].

Квінтесенція досліджень зі створення та вдосконалення опосередкованих засобів встановлення контролю над великою кількість комп'ютерів,

[1] Гурьянов К.В., Шатило Я.С. Безопасны ли лицензионные программные продукты? // Научно-практический журнал Информационная безопасность регионов, 2008. – № 1(2). – С. 4-9.

підключених до мережі Інтернет, призвела до появи масштабних ботмереж з потужними можливостями, відомих як StormWorm, Mayday, Rustock, Maazben, Kido, Cutwail, ZeuS, Kneber.

Узагальнення уривчастих відомостей дозволяє відтворити значну частину "кримінальної" картини. Відправною точкою технологічного циклу будови кримінального адміністрування виступає знайдена уразливість програмного забезпечення. Вона може існувати внаслідок недосконалості, помилки або завдяки спеціальному резервуванню. Таким чином, уразливості поділяються на природні та штучно створені. Виявлення невідомої уразливості або її купівля відкривають можливість написання спеціальної програми, її продажу у "чистому" виді, тобто без змін. Створена спеціальна програма може використовуватися безпосередньо для будови і керування бот-мережею або бути проданою. В дусі кращих традицій розповсюдження програмного забезпечення купівля таких програм супроводжується таким сервісом, як оновлення та подальше вдосконалення продукту.

Коло суб'єктів, які можуть прийняти опосередковану або безпосередню участь у такій багатоваріантній схемі, можливо поділити на такі категорії: створювачі ліцензійних програмних продуктів, дослідники, створювачі нелегального програмного забезпечення, розповсюджувачі, орендодавці та орендатори, тобто кінцеві користувачі. Якщо мова йде про суто кримінальне використання, то усіх таких осіб, які належать до однієї або декількох категорій одночасно, поєднує єдина мета – бізнес на основі уразливості програмного забезпечення. Ботнети використовуються для збору інформації, а це, по суті, безвідходна діяльність – збирається все, що може бути продано.

Для вивчення феномену ботмережі із середини німецькі дослідники здійснили проект під назвою "Приваблива мережа" (Honeynet). Сутність проекту полягала у створені локальної мережі з Інтернет з'єднанням та імітації активної обробки даних, щоб привернути увагу. Дуже швидко ця мережа стала частиною ботнету, внаслідок чого була отримана копія програми, що використовувалася.[1] Програмне забезпечення для функціонування ботмережі являє собою ELF-файл (Executable and Linkable Format – формат адаптованих файлів для мережевого використання, що виконуються та компонуються), що має розмір приблизно 1,2 мегабайта. Вартість такого програмного забезпечення для побудови керованих субмереж коливається від 5 до 1000 доларів США. Популярністю користуються системи, якими легше користатися. Програмні засоби, на яких функціонують ботмережі, можуть спеціально створюватися відповідно

[1] Niels Provos, Thorsten Holtz. Virtual Honeypots: From Botnet Tracking to Intrusion Detection illustrated edition, 2007. – 480 p.

до програмного забезпечення, яке типово встановлюється користувачем на комп'ютерах: системні програмні оболонки, текстові і графічні редактори, Інтернет браузери, а також ігри. Сучасний комп'ютер не може функціонувати без системних програмних оболонок, тому технологія створення ботмереж орієнтується саме на операційні системи Windows та Linux. Проте, видається, що навряд чи таке рішення може конкурувати з комплексним підходом, основаному на сполученні усіх можливих варіантів і способів здійснення підключення та встановлення контролю.

Цікавим і одночасно важливим є питання щодо кількості комп'ютерів у відомих сьогодні ботмережах для визначення їх потужності. Але класифікація ботмереж за розміром носить проблемний характер. Важко визначити систему відповідних показників для класифікації на певні групи. Річ у тому, що кількість комп'ютерів у ботмережі – величина динамічна. Постійну зміну кількісного складу ботнетів зумовлюють технічні, організаційні чинники, а також стратегія і тактика їх використання. До технічних обставин відноситься електричне живлення. Вимкнення комп'ютера призводить до його "виведення" з ботмережі до наступного увімкнення. Таким чином, кількість комп'ютерів постійно змінюється.

Бот-мережі використовуються для здійснення широко спектру завдань:

- відправка даних, які зберігаються або обробляються;
- приєднання інших комп'ютерів або цілих мереж;
- розсилання інформаційних пакетів (спам, реклама, порнографія);
- організація блокування комп'ютерів та мереж;
- компрометація адреси окремого комп'ютера або національного сегмента певної держави.

Треба відмітити, що прибутковим буде будь-який напрямок використання, який би зловмисник не обрав, причому ботнет дозволяє здійснювати всі перераховані види діяльності одночасно.[1] Собівартість створення мережі ботнет з 10 000 комп'ютерів складає приблизно декілька тисяч доларів. Використовуючи її тільки для розсилки спаму, можна заробити вже десятки тисяч в місяць.[2] У світовому масштабі обертаються мільярдні суми, які виникають внаслідок функціонування бот-мереж. Еволюція розвитку злочинів у сфері високих інформаційних технологій аналогічна традиційному шляху вдосконалення злочинного світу: від окремих злочинів до організованих злочинних угрупувань.

Специфіка мережі ботнет ще й у тому, що вона може використовуватися для самозахисту. Управлінський програмний код сучасних ботме-

[1] Как это работает: ботнеты // ComputerBild, 2009. – № 17. – С. 57 (56-59).

[2] Идибман В. Информационная безопасность сегодня: без паники и всерьез // Компьютерное обозрение, 2009. – № 41 (707). – С. 20-27.

реж має швидкий цикл оновлення – приблизно один раз на годину. Така динамічна конспірація не просто вражає, але й заставляє замислитися щодо визначення швидкості технології протидії. Технічно мережа ботнет складається з певних кількісних груп комп'ютерів, щоб у разі можливого виявлення обмежитися втратою лише частини окремого сегменту, а не всієї мережі. При виявленні деструктивних заходів впливу ресурси мережі ботнет можуть використовуватися для самозахисту. У такому випадку фіксується Інтернет-адреса, збирається необхідна службова інформація щодо потужностей супротивника і в залежності від його "вагової" категорії виділяється частина або усі ресурси мережі ботнет для інформаційного блокування. Також бот-програма може блокувати доступ користувача до ресурсів Інтернет, оскільки він може бути використаний для пошуку заходу протидії шляхом ознайомлення з консультаційними форумами, завантаженню відповідного програмного забезпечення для блокування функціонування бот-програми.

Перспективним напрямком для створення мереж ботнет є смартфони та комунікатори. Такі пристрої завдяки програмним можливостям, специфіки внутрішньої архітектури виступають незахищеними та перспективними з точки зору кримінального впливу на об'єкти. Наявність у таких пристроїв власного каналу Інтернет зв'язку, відсутність спеціальних програмних засобів захисту, підключення до стаціонарних комп'ютерів та ноутбуків для обміну даними значно розширює тактичні можливості злочинців щодо встановлення контролю і приєднання до ботмереж нової телекомунікації. В основу отримання доступу до цих засобів зв'язку покладено принцип функціонування таких каналів передачі даних як SMS (Short Message Service – послуга передачі і прийому коротких текстових повідомлень у телекомунікаційних мережах) або Bluetooth (технологія бездротового зв'язку між різними пристроями). Також використовуються технічні можливості UMTS (від англ. Universal Mobile Telecommunications System – технологія мобільного зв'язку третього покоління 3G, надає можливість високошвидкісної передачі даних з використанням радіодоступу широкосмугової кодової модуляції) або WiMAX (від англ. Worldwide Interoperability for Microwave Access – стандарт безпровідного зв'язку, що забезпечує широкосмуговий зв'язок на значні відстані зі швидкістю, порівняною з кабельними з'єднаннями). Дослідники компанії TrendMicro виявили програму Sysmbos_YXES для створення ботмереж з мобільних телефонів[1]. Знайдені у телефонній книзі контакти будуть використовуватися для приєднання інших пристроїв.

Ботмережі також являють собою вид інформаційної зброї для впливу на певну ціль або об'єкт, що має активне з'єднання з ресурсами Інтер-

[1] Бот-сети начали создавать из сотовых телефонов // http://itua.info/news/security/21791.html

нет. Такі дії можуть вчинятися з будь-якого географічного сегменту Інтернет із застосуванням імітації використання певної національної зони. Ботнети являють собою вид інформаційної зброї, але це теми іншого дослідження. Так, наприклад, американська компанія NetWitness відмічає, що ботмережа Kneber складається з систем, що знаходяться на території Єгипту, Мексиці, Саудівської Аравії, Туреччини та США, а на початку свого існування керувалася з Німеччини.[1]

Для виявлення ботнетів доцільно використовувати комплексне рішення на базі технологій фільтрації пакетів та подальшого аналізу з використанням методів аналізу групової активності DNS-серверів (одержання інформації про домени), та SMTP-трафіку (змісту мережевого протоколу) на поштових шлюзах та виявлення ботнет-трафіку серед потоку IRC. Тобто виявляти "зайве" навантаження мережевих каналів зв'язку. Такий підхід знаходить підтримки у працях вітчизняних та зарубіжних дослідників.[2,3]

Для дослідження зразка програми ботмережі російський дослідник І.Ю. Юрін пропонує вирішити такі задачі:[4]

- чи можливо за допомогою даного програмного продукту здійснювати несанкціоноване знищення, блокування, модифікацію або копіювання інформації, порушувати роботу комп'ютерів або їх мереж?
- чи є дані у досліджуваній програмі, які можуть персоналізувати її автора?
- чи є програма керованою, тобто має функцію отримувати команди та передавати інформацію за запитом?
- чи має програма функцію автоматичного відновлення модулів?
- зі скількох файлів складається головна програма, чи є допоміжні?

Організація протидії с ботмережами потребує наступних дій:

- дослідження мережевих журналів окремого комп'ютера та локальних мереж, що підключені до Інтернет;
- виділення мережевих адрес комп'ютерів-одногрупників;
- вибір серед них мережевих адресів комп'ютерів-одногрупників, що розташовані на території країни;
- визначення фізичного розташування комп'ютера та провайдера, що надає послуги зв'язку.

---

[1] http://www.netwitness.com/

[2] Погребенник В.Д., Хромчак П.Т. Розроблення моделі системи виявлення центрів управління ботнет-мережами // Вісник національного університету "Львівська політехніка", 2009. – № 639. – С. 117-123.

[3] Karun Dambiec. Detecting Potential Peer-to-Peer Botnets Using The Payload Of Network Packets, 2010. – 76 p.

[4] Особенности экспертного исследования IRC-ботов, используемых для построения зомби-сетей // Компьютерно-техническая экспертиза, 2007. – № 1(1). – С. 11 (10-15).

Проведене дослідження комплексу проблем, пов'язаних із існуванням та розвитком феномену ботнет, дозволяє зробити наступні висновки.

Темпи розвитку означених протиправних діянь, ступень їх розповсюдження, різноманітність проявів, системність, масштабність і, нарешті, динамічність дають підставу стверджувати, що у майбутньому неодмінно будуть з'являтися нові напрямки для відповідних, і, головне, своєчасних досліджень.

Виникнення феномену ботнет, який, безумовно, є наслідком високих інформаційних технологій, можливо розглядати як своєрідний орієнтир або показник. Гуманітарні науки з точки зору динаміки розвитку значно відстають від технічних. Про це, зокрема, свідчить часовий розрив між технічними новаціями і появою відповідних досліджень на шпальтах юридичних видань. В аспекті виникнення феномену ботнет цей термін складає приблизно 10 років. Суттєве відставання теорії та практики боротьби з високотехнологічною злочинністю криється у тому, що вітчизняна наука здебільшого займає позицію очікування. Для виявлення інноваційних тенденцій та форм злочинної діяльності у сфері високих інформаційних технологій необхідно слідкувати за публікаціями зарубіжних дослідників, взаємодіяти з відповідними правоохоронними органами зарубіжних країн та проводити власні дослідження. Між тим, аналіз багатьох наукових праць щодо розкриття та розслідування злочинів у сфері високих інформаційних технологій свідчить про відсутність посилань на спеціальну технічну літературу та джерела дальнього зарубіжжя.

Російський дослідник В.О. Мещеряков відмічає, що для запобігання кримінальному використанню мереж ботнет необхідне проведення широкого спектру кримінологічних, кримінально-правових і, в першу чергу, криміналістичних і кримінально-процесуальних досліджень, орієнтованих на виявлення механізму слідоутворення[1]. Погоджуючись в цілому з наведеною позицією, відзначимо, що відповідні дослідження потрібно проводити для удосконалення й оперативно-розшукової діяльності. Специфіка та можливості сформованих мереж ботнет повинні враховуватися при запобіганні та розкритті усього спектру злочинів у сфері високих інформаційних технологій: у сфері використання комп'ютерів, незаконних дій з платіжними картками та іншими засобами доступу до банківських рахунків, шахрайства, шахрайств, розповсюдження порнографії в мережі Інтернет та іншими каналами зв'язку, тощо. Сучасна стратегія протидії злочинності у сфері високих інформаційних технологій пови-

[1] Мещеряков В.А. Криминалистический анализ противоправного использования ботнетов // Воронежские криминалистические чтения : сб. науч. трудов. – Вып. 11 / Под ред. О. Я. Баева. – Воронеж : Изд-во Воронеж. гос. ун-та, 2009. – С. 266 (252-266).

нна спиратися не тільки на вирішення поточних завдань, а в першу чергу на визначення перспективних напрямків її розвитку.

Стаття надійшла до редколегії 11.05.2010 р.

УДК 351.746.2:342.97(477)

І.В. Краснобрижий

ПРАВОВА РЕГЛАМЕНТАЦІЯ ВЗАЄМОДІЇ ПІДРОЗДІЛІВ ДСБЕЗ МВС УКРАЇНИ З ІНШИМИ ОПЕРАТИВНИМИ ПІДРОЗДІЛАМИ ОВС ПОТРЕБУЄ ВДОСКОНАЛЕННЯ: ПОСТАНОВКА ПРОБЛЕМИ

У статті здійснюється аналіз літературних та нормативних юридичних джерел, що висвітлюють або ж регламентують аспекти взаємодії підрозділів ДСБЕЗ МВС України з іншими оперативними підрозділами ОВС.

Ключові слова: *економічна злочинність, взаємодія, суб'єкт взаємодії, компетенція, функція, законність.*

В статье проводится анализ литературных и нормативных юридических источников, которые отражают либо регламентируют аспекты взаимодействия подразделений ГСБЭП с другими оперативными подразделениями ОВД.

Ключевые слова: *экономическая преступность, взаимодействие, субъекти взаимодействия, компетенция, функция, законность.*

In the article on the base of the juridical sources the problematic questions of interaction of the detachments of the Organs of internal affairs as to the actions against economic crime.

Key words: *economic crime, interaction, the subject of interaction, competence, function, legality.*

Взаємодія підрозділів ДСБЕЗ з іншими оперативними підрозділами ОВС у процесі боротьби з економічною злочинністю, будучи одною з видів соціальної діяльності, підкоряється законам суспільного розвитку й зазнає змін прогресивного характеру. Одне з найважливіших місць у цьому процесі займає правове регулювання, від ефективності якого прямо залежить оперативність і якість розв'язуваних завдань. Саме ця обставина й обумовлює необхідність його глибокого вивчення.

Так, на думку фахівців у галузі права (С.С. Алексєєв та ін.) під правовим регулюванням варто розуміти здійснюваний за допомогою права й всієї сукупності правових засобів юридичний вплив на суспільні відносини. Дане поняття охоплює багатогранну діяльність держави, спрямовану на формування юридичних засобів організації громадського життя,