УДК 004.738.5:338.46

Грабар О. І., Шкуратенюк Т. А., Ляшук В. В.
Житомирський державний технологічний університет

Протидія кіберзлочинності на прикладі вірусів

Анотація. Актуальність проблеми кіберзлочинності та хакерських атак в сучасному інформаційному світі підтверджується дослідженнями бурхливого розвитку комп'ютерних вірусів за останні 50 років. Метою даної статті є розкриття сутності явища кіберзлочинності. В статті розглянуто два найбільш сучасних віруси «Snake» та «Stuxnet», наведено результати їх роботи та можливості протидії їм. Механізми контролю, запобігання та розслідування посягань у кіберпросторі дуже обмежені як соціально, так і технологічно. Перспективи подальших досліджень цього явища в Україні та на міжнародному рівні потребують новітніх методів боротьби та блокування роботи хакерських атак в умовах інформаційних війн.

Ключові слова: кіберзлочинність, інформаційна безпека, віруси.

Сучасні інформаційні технології використовується практично у будь-яких галузях діяльності людей і є одним з головних рушіїв у сучасному розвитку суспільства. Але разом з тим виникає проблем, які важко розв'язати. Однією з таких проблем є кіберзлочинність. Поширення комп'ютерної злочинності привело до необхідності вивчення цього явища, вироблення рекомендацій стосовно її нейтралізації.

Мета написання даної роботи – розкрити сутність кіберзлочинності, дослідити проблеми нейтралізації цього явища.

Поняття «кіберзлочинність» вперше з'явилось в американській, а потім і в іншій іноземній літературі на початку 1960-х рр. і визначалося як порушення чужих прав та інтересів стосовно автоматизованих систем опрацювання даних. Кіберзлочинність (англ. Cybercrime) – це поняття, яке охоплює комп'ютерну злочинність (де комп'ютер – предмет злочину, а інформаційна безпека – об'єкт злочину) та інші правопорушення, де комп'ютер є знаряддям або способом злочину проти власності, авторських прав, громадської безпеки, моралі тощо [1].

З кожним роком все більше зростає кількість людей, які використують ресурси мережі Інтернет, і, як показує статистика, кількість злочинів, що вчиняються у кіберпросторі також зростає.

На жаль деякі держави вже розробляють доктрину ведення інформаційних воєн з використанням електронних засобів, для чого створюються спеціальні комп'ютерні програми і розробляється відповідне обладнання. Також за допомогою інформаційних технологій конфліктуючі сторони можуть розповсюджувати віруси, зламувати паролі і розповсюджувати дезінформацію через мережу Інтернет.

Як відомо, українські комп'ютерні мережі, в тому числі урядові, вражає вірус під кодовою назвою «Змія». Це помітила британська аерокосмічна та військова група Bae System. Вірус «Змія» має також іншу назву – «Uroborus» (міфічна рептилія, що ковтає власний хвіст і символізує вічне повернення). За січень 2014 року зафіксовано 22 випадки атак. Як зазначають експерти, за своєю складністю та потужністю цей вірус може зрівнятися хіба що з програмою Stuxnet, що була виявлена 2010 року. Тоді вона була спрямована на виведення із ладу ядерної програми в Ірані.

За допомогою «Uroborus» хакери могли паралізувати передавання даних, вилучити документацію і отримували в Україні повний доступ до атакованої системи, поставивши під загрозу обороноздатність держави. Експерти переконані, що настільки складна операція потребує великих затрат і не може бути здійснена групою хакерів, атаки відбувалися із часового поясу GMT+4, у базовому коді виявили фрагменти тексту кирилицею.

Механізми контролю, запобігання та розслідування посягань у кіберпросторі дуже обмежені як соціально, так і технологічно. Як показує приклад атак на ядерне виробництво Ірану, навіть відключення особливо важливих для держави об'єктів від глобальних інформаційних мереж не захищає їх від можливих атак: вірус Stuxnet, поширювався через портативні накопичувальні пристрої, що під'єднуються до комп'ютера через порт USB [2].

Розглянемо детальніше вірус «Snake» або, як його ще називають, «Uroborus».

Змія або Uroborus — комп'ютерний хробак. Дослідники британської фірми BAE Systems Applied Intelligence зафіксували в 2013—2014 роках спалах виявлених випадків зараження інформаційних систем приватних підприємств та державних установ України комп'ютерним хробаком (з руткітом), який вони назвали «Змія». Дослідники з німецької фірми GData назвали цього хробака «Uroborus». На думку дослідників обох фірм, цей хробак можливо пов'язаний та був створений на основі хробака Agent.BTZ, який в 2008 році вразив інформаційні системи Центрального Командування ЗС США.

Фахівці із CERT-UA(Computer Emergency Response Team of Ukraine – команда реагування на комп'ютерні надзвичайні події в Україні) – спеціалізований структурний підрозділ Державного центру кіберзахисту та протидії кіберзагрозам (ДЦКЗ) Державної служби спеціального зв'язку та захисту даних в Україні (Держспецзв'язку)) виявили кілька особливостей вірусу «Uroborus»:

- складність програмного коду (що обумовлює можливість його розроблення із залученням значної кількості людських, технічних і фінансових ресурсів (зокрема, це можуть бути науково-дослідні установи, IT-корпорації, державні установи, спецслужби тощо);

- наявність літер кирилиці у програмному коді;
- схожість за низкою характеристик (імена файлів, ключі шифру, основні характеритсики тощо) із троянською програмою Agent.BTZ, яку було знайдено в інформаційних системах ЗС США в 2008 році, що призвело до повної відмови ЗС США від використання USB-носіїв (через які програма поширювалася в автоматизованих системах військового призначення);
- географія поширення вірусу.

«Uroborus» може поширюватись різними способами, зокрема, через так звані атаки Watering-Hole. Його складно виявляти, він функціонує автономно, та самостійно поширюється в інфікованих мережах. Враженими можуть бути навіть комп'ютери без прямого під'єднання до Інтернет.

В інтернет-просторі України вперше було застосовано троянські програми, ключовою серед яких став вірус Uroburos. З одного боку, призначення цього вірусу було формування бот-мережі із заражених комп'ютерів та отримання повноцінного доступу до їх ресурсів, а з іншого – викрадення даних з цих комп'ютерів. Об'єкти атаки також, вочевидь, були обрані не випадково – веб-ресурси органів державної влади (в тому числі силових структур), засобів масового інформування, фінансових установ, великих промислових підприємств. Протягом січня 2014 року було зафіксовано 22 випадки інфікування інформаційних систем, хоч разом з тим протягом 2013 року «Uroborus» був виявлений не більше 8 разів. В Україні зловмисники із застосуванням «Uroborus» отримували повний доступ до вражених систем. За даними CERT-UA основними відомими станом на березень 2014 року об'єктами ураження «Uroborus» є:

- веб-ресурси органів державної влади (в тому числі силових структур);
- веб-ресурси засобів масового інформування;
- веб-ресурси фінансових установ;
- веб-ресурси великих промислових підприємств.

Фахівці CERT-UA не виключають, що головним призначенням Uroborus було порушення фукціонування об'єктів інформаційної інфраструктури України для викрадення конфіденційних даних. Ретельна підготовка, прихованість дій, спрямованість кібератак (США -2008 рік, Україна – 2014 рік), а також залучення значних ресурсів – все це опосередковано свідчить про причетність іноземних спецслужб. В цьому контексті CERT-UA та деякі українські фахівці з інформаційної безпеки вбачають основним мотивом ініціатора кібератак необхідність встановлення прихованого контролю за визначеними об'єктами для подальшого спостереження за інформаційним обміном з власної території [3].

«Uroborus» був застосований не лише проти України, а й проти інших країн. Зокрема, дане ПЗ згадане в річному звіті німецької контррозвідки за 2015 рік. Німецька контррозвідка зазначила, що, як і раніше, в 2015 році використовували «змію» (він же – «Turla») проти установ у всьому світі. В Німеччині жертвами кібератак з його застосуванням стали посольства, заклади вищої освіти, дослідницькі інститути, приватні підприємства.

Інший вірус Win32 / Stuxnet – комп'ютерний черв'як, вражає комп'ютери, що функціонують під управлінням операційної системи Microsoft Windows. 17 червня 2010 року його виявив антивірусний експерт Сергій Уласень з білоруської компанії «ВірусБлокАда». Вірус був виявлений не тільки на комп'ютерах рядових користувачів, але і в промислових системах, управління автоматизованими виробничими процесами.

Це перший відомий комп'ютерний хробак, через вторгнення якого перехоплюються і модифікуються інформаційні потоки між програмованими логічними контролерами марки Simatic S7 і робочими станціями SCADA-системи Simatic WinCC фірми Siemens. Таким чином, черв'як може бути використаний як засіб несанкціонованого збирання даних (шпигунства) і диверсій в АСУ ТП промислових підприємств, електростанцій, аеропортів і т.п.

Унікальність програми полягала в тому, що вперше в історії кібератак через вторгнення вірусу фізично руйнувалася інфраструктура інформаційної системи.

Давно відомо, що Stuxnet – одна з найскладніших і найретельніших продуманих кібератак з тих, які відомі. Вибір перших цілей дозволяє зрозуміти, наскільки ретельно була проведена підготовка до неї», – пояснює Олександр Гостєв, головний антивірусний експерт «Лабораторії Касперського». На Рис.1 наведена схема принципу роботи антивірусу «Касперського».

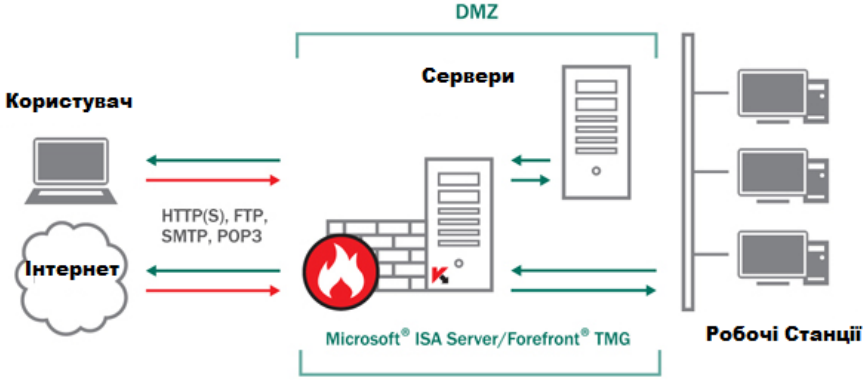

Рис.1. Принцип роботи антивірусу «Касперського».

Розслідуючи дану атаку, фахівці припустили, що «черв'як» потрапив до «жертв» через USB-накопичувачі, під'єднувані до комп'ютера, але аналіз слідів однієї із перших атак показав, що перший примірник Stuxnet був скомпільований за лічені години до зараження. За такий короткий проміжок часу вкрай малоймовірно встигнути зібрати шкідливу програму, записати її на USB-носій і забезпечити доставку до комп'ютера жертви. Швидше за все, зловмисниками було використано інший спосіб зараження [4].

Даний вірус небезпечний через чотири шляхи вразливості системи Microsoft Windows (вразливість «нульового дня» (zero-day) і три раніше невідомі вразливості), що дозволяє чого поширювати за допомогою USB-flash накопичувачів. Залишатися непоміченим антивірусними програмами йому допомагала наявність справжніх цифрових підписів (два дійсних сертифікати, випущених компаніями Realtek і JMicron).

Обсяг вихідного тексту вірусу становить приблизно 500 КБ коду на мові асемблера, C і C ++.

Отже розглянувши два відомі віруси, можна уявити, наскільки серйозними можуть бути наслідки кібератак.

Щодо класифікації кіберзлочинів, то найбільш поширена в даний час ґрунтується на Конвенції Ради Європи про кіберзлочинність, що була відкрита для підписання у листопаді 2001 р. В цьому документі кіберзлочини поділяються на п'ять груп:

- злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему);
- злочини, пов'язані з використанням комп'ютера як засобу скоєння злочинів, а саме – для маніпуляцій з даними (комп'ютерне шахрайство та комп'ютерні підроблення);
- злочини, пов'язані з контентом (змістом збережуваних матеріалів);
- злочини, пов'язані з порушенням авторського права і суміжних прав;
- акти расизму та ксенофобії, вчинені за допомогою комп'ютерних мереж [5].

Щоб уявити собі масштаби і обороти цього кримінального бізнесу, досить навести деякі приклади. Віртуальні шахраї, заволодівши через Мережу номерами більш ніж мільйона банківських карт - громадян США, одночасно зробили розкрадання в 130 банкоматах в 49 містах Америки. Вся операція тривала не більше 30 хвилин, а розмір прибутку злочинців склав близько 9 мільйонів доларів, які потім були переведені на рахунки в різні держави. У 2010 р. ФБР висунуло звинувачення проти 37 жителів Росії, України та інших східноєвропейських країн, підозрюваних у використанні комп`ютерного вірусу для злому американських банківських рахунків [6].

В даний час не існує ні релевантної статистики, через які відображається реальна картина стану кіберзлочинності, ні надійних методів збирання таких даних. І справа не тільки у відсутності однаковості національного кримінального законодавства країн у сфері боротьби з кіберзлочинністю і різної практики його застосування, відмінностях у формуванні кримінальної статистики та особливостях правоохоронної системи. Так, до цих пір неясно, до якої міри вірогідна статистика про економічні втрати в результаті кіберзлочинності.

Найбільша частина кіберзлочинності залишається за рамками статистики − можна з упевненістю стверджувати, що в офіційну статистику потрапляє лише десять, у кращому випадку двадцять відсотків скоєних діянь[6].

Інформаційна безпека вже розглядається державами як одне з пріоритетних завдань у сфері національної безпеки та міжнародної політики. Концепція інформаційної безпеки включає як захист користувачів мереж, так і захист держави в цілому. Однак оскільки жодна держава не може захистити себе, здійснюючи заходи лише на національному рівні, для комплексної протидії кіберзлочинності необхідні:

– гармонізація кримінального законодавства про кіберзлочини на міжнародному рівні;

– розробка на міжнародному рівні та імплементація в національне законодавство процесуальних стандартів, використання яких дозволить ефективно розслідувати злочини в глобальних інформаційних мережах, отримувати, досліджувати і надавати електронні докази з урахуванням транскордонності цієї проблеми;

– налагоджене співробітництво правоохоронних органів під час розслідування кіберзлочинів на оперативному рівні;

– механізм вирішення юрисдикційних питань у кіберпросторі [5].

На сучасному етапі важливу роль у боротьбі з кіберзлочинністю відіграють спеціалізовані міжнародні угоди (наприклад, Конвенція Ради Європи про кіберзлочинність, рішення Ради Європейського Союзу, спільний проект Європейського союзу і Міжнародного Союзу Електрозв'язку для держав Тихоокеанського регіону (проект ICB4PAC), проект ООН з розробки законодавства в сфері кіберзлочинності для країн Африки (проект ESCWA), однак вони не є за своєю суттю універсальними міжнародними інструментами, незважаючи на те, що деякі з них вийшли за своїм впливом далеко за рамки регіону, в якому вони були прийняті.

Протидіяти кіберзлочинності на сучасному етапі дуже важко, оскільки технології постійно удосконалюються, а разом з ними удосконалюється кіберзлочинність.

Висновки. Кіберзлочинність є порівняно новим видом суспільно небезпечних діянь, проте на відміну від традиційних крадіжок і шахрайства, вона постійно удосконалюється і розвивається разом з інформаційними технологіями. На сьогодні доводиться констатувати, що законодавство України є

недосконалим у сфері боротьби з кіберзлочинністю. Міжнародне співробітництво є ключовим моментом у ліквідації правового вакууму, існуючого між розвитком інформаційних технологій та реагуванням на них законодавства. Процес вироблення заходів на міжнародному рівні, як показує досвід, сам по собі є комплексною проблемою. Однак це єдиний шлях забезпечити безпеку інформаційних ресурсів користувачів і держави від злочинних посягань, а також ефективно розкривати і переслідувати кіберзлочини [5].

Список використаних джерел

1. Савчук Н. В. Кіберзлочинність: зміст та методи боротьби / Н. В. Савчук // Теоретичні та прикладні питання економіки: зб. наук. праць. – К.: Видавничо–поліграфічний центр «Київський університет», 2009. – Вип. 19. – С. 338–342.
2. Номоконов В. А. Киберпреступность: прогнозы и проблемы борьбы / В. А. Номоконов, Т. Л. Тропина // Библиотека криминалиста. – №5 – 2013. – С. 148–160.
3. Клаверов В. Б. Современная киберпреступность : характеристика и подробный анализ / В. Б. Клаверов // Издательство LAP Lambert Academic Publishing. – 2012.- С. 92.
4. Спеціалізований структурний підрозділ Державного центру кіберзахисту та протидії кіберзагрозам (ДЦКЗ) [Електронний ресурс] // – Режим доступу: http://cert.gov.ua/?p=344.
5. Лаборатория Касперского [Електронний ресурс] // – Режим доступу: http://www.kaspersky.ru/about/news/virus/2014/stuxnet-v-detaliakh.
6. Незалежна асоціація банків україни [Електронний ресурс] // – Режим доступу: http://anticyber.com.ua/article_detail.php?id=140.
7. Зеркало недели. Украина [Електронный ресурс] // – Режим доступу: http://zn.ua/TECHNOLOGIES/smi-rossiya-zapustila-virus-zmeya-nachav-kibervoynu-protiv-ukrainy-140801_.html.
8. Odnako.su. [Електронный ресурс] // – Режим доступу: http://odnako.su/news/world/-33754-zapustiv-virus-zmeya-rossiya-nachala-kibervoynu-protiv-ukrainy---smi/.
9. Хабрахабр [Електронный ресурс] // – Режим доступу: https://habrahabr.ru/post/159053/

Противодействие киберпреступности на примере вирусов

Грабар О.И., Шкуратенюк Т.А., Ляшук В.В.

Аннотация. Актуальность проблемы киберпреступности и хакерских атак в современном информационном мире подтверждается исследованиями бурного развития компьютерных вирусов за последние 50 лет. Целью данной статьи является раскрытие сущности явления киберпреступности. В статье рассмотрено два наиболее современных вируса "Snake" и "Stuxnet", приведены результаты их работы и возможности противодействия им. Механизмы контроля, предотвращения и расследования посягательств в киберпространстве очень ограничены как социально, так и технологически. Перспективы дальнейших исследований этого явления в Украине и на международном уровне нуждаются в новейших методах борьбы и блокирования работы хакерских атак в условиях информационных войн.

Ключевые слова: киберпреступность, информационная безопасность, вирусы.

Counteraction to cybercrime is on example of viruses

Grabar O.I., Shkuratenuk T.A., Liashuk V.V.

Resume. Actuality of problem of cybercrime and hacker attacks in the modern informative world is confirmed by researches of rapid development of computer viruses for last 50 years. The aim of this article is opening of essence of the phenomenon of cybercrime. In the article it is considered two most modern viruses of "Snake" and "Stuxnet", their job and possibility of counteraction performances over are brought to them. The mechanisms of control, prevention and investigation of encroachments in a cyberspace are very limited both socially, and technologically. Prospects of further researches of this phenomenon in Ukraine and at an international level need the newest methods of fight and blocking of work of hacker attacks in the conditions of informative wars.

Keywords: cybercrime, informative safety, viruses.