ПРОБЛЕМИ КРИМІНАЛЬНОГО ПРАВА ТА КРИМІНОЛОГІЇ

УДК 004.056.5

АНАЛІЗ МЕТОДІВ ПРОТИДІЇ КІБЕРАТАКАМ

Бараненко Роман Васильович,
кандидат технічних наук, доцент,
професор кафедри професійних
та спеціальних дисциплін
(Херсонський факультет Одеського
державного університету внутрішніх
справ, м. Херсон, Україна)

Задорожна Антоніна Юріївна,
студентка (Херсонський національний
технічний університет,
м. Херсон, Україна)

Кіберзлочинність є дуже серйозною проблемою, яка поступово охоплює всі сфери життєдіяльності сучасного суспільства. Основними інструментами кіберзлочинності є ботнети, шкідливий код, розміщений на сайтах, віруси, трояни, DDoS-атаки тощо.

Розглянуто способи компрометації комп'ютерної мережі ззовні. Метою внутрішніх атак є отримання доступу до заборонених, скритих даних і ресурсів. Наведено класифікацію троянських атак. Трояни можуть бути використані кіберзлодіями й хакерами, які намагаються отримати доступ до систем користувачів. Розглянуто типи троянів. Наведено механізм поширення вірусної атаки.

Проведено аналіз технік (методів сканування) для виявлення вразливих машин: випадкове сканування, хіт-лист сканування, топологічне сканування, локальне сканування підмережі, сканування перестановкою. Запропоновано перелік необхідних заходів протидії порушникам.

З метою організації ефективної боротьби з терористичною діяльністю в кіберпросторі розглянуто три етапи захисту комп'ютерних систем та мереж. Розроблено прототип системи захисту персонального комп'ютера та наведено практичні рекомендації щодо захисту персональних комп'ютерів та комп'ютерних мереж від зовнішніх та внутрішніх вторгнень.

Ключові слова: інтернет, кібербезпека, загрози, кібератаки.

THE ANALYSIS OF THE METHODS OF THE CYBER ATTACKS COUNTERACTION

Baranenko Roman Vasilyovich,
Candidate of technical sciences, assistant
professor, professor of department of
professional and special disciplines,
(Kherson Faculty of Odessa State
University of Internal Affairs, Kherson,
Ukraine)

Zadorozhna Antonina Yuriyivna,
student (Kherson National Technical University, Kherson, Ukraine)

Cybercrime is a very serious problem that gradually covers all spheres of the life in a modern society. Botnets, malicious code, hosted on sites, viruses, trojans, DDoS attacks etc. are main tools of a cybercrime.

Such ways of compromising of the computer network from the outside as an access through weak, stolen or lost credentials; an access through malware; an access through compromising systems of remote access; a weakened access by the third parties; an access through physical penetration; an access via modem; an unauthorized access to the staff of the organization; an access through wireless systems; the direct penetration through the perimeter of systems are considered. The purpose of internal attacks is to gain an access to forbidden, hidden data and resources.

The classification of Trojan attacks is given. Trojans can be used by cybercriminals and hackers who are trying to access the user systems. Unlike computer viruses and worms, Trojans are not capable of distribution. The types of Trojans are considered.

The mechanism of propagation of a virus attack is given. Since the virus is spread by humans, human actions will unknowingly continue to spread the computer virus by exchanging, infecting files, or sending e-mail messages with viruses as attachments inside the e-mail.

The analysis of techniques (scanning methods) for detecting vulnerable machines was performed: random scanning, hit-sheet scanning, topological scanning, local scan of a subnet, scanning by permutation. A list of necessary measures to counter offenders is proposed.

For the organization of effective struggle against terrorist activity in cyberspace, three stages of protection of computer systems and networks are considered: prevention; incident management, mitigation, damage limitation; impact management. In prevention, the use of various forms of prevention or interception is recommended, because it stops the attack that has been launched, counteracts the achievement of the goal. Warning strikes or interceptions may be either cyberspace or physical. The most important duty of specialists at the stage of incident management is to provide guidance and warnings that the attack is taking place. Also, automatic or partial shutdown and redistribution, load rejection strategy, redistribution of survival capability for the most important functions required by the organization are applied. Audit and backup are carried out. There are two main components at the stage of managing the consequences: recovery and response. The response involves identifying and punishing of the perpetrators and mastering lessons in order to enable the organization for a better protection of it in future.

A prototype of the personal computer protection system has been developed and practical recommendations for the protection of personal computers and computer networks from external and internal intrusions are given.

Key words: Internet, cyber security, threats, cyber-attacks.

Кіберзлочинність є дуже серйозною проблемою, яка поступово охоплює всі сфери життєдіяльності сучасного суспільства. Основними інструментами кіберзлочинності є ботнети, шкідливий код, розміщений на сайтах, віруси, трояни, DDoS-атаки тощо.

З розвитком новітніх інформаційних технологій та широкою доступністю засобів комп'ютерної техніки кількість кіберзлочинів та наданих ними фінансових збитків збільшилася в рази. З урахуванням всіх міжнародних телекомунікаційних мереж, що існують у світі, кіберзлочинність не буде обмежено територією однієї держави [1]. Тому ця проблема має тенденцію перерости до транснаціональної наряду з протидією наркотрафіку, торгівлею зброєю та міжнародному тероризму.

Проте доречно зазначити, що є й інші форми кіберзлочинності, які можуть підпадати під ці ознаки. Наприклад, несанкціонований доступ та злом. Тому дослідження

технічних аспектів скоєння злочинних посягань на інформацію та методів протидії їм є предметом цього дослідження.

Дослідженням методів захисту інформації від несанкціонованого доступу та технічних аспектів протидії кіберзлочинності займалися такі вчені: В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа, С.В. Мельник, Д.В. Дубов, М.А. Ожеван, J. Matusitz, J. Harper та інші. Проте низка важливих питань у сфері забезпечення захисту інформації та протидії кіберзлочинності позбавлена гідної уваги дослідників.

Метою роботи є аналіз основних методів протидії кібератакам, що проводяться кіберзлочинцями з метою посягання на непублічну інформацію або отримання несанкціонованого доступу до комп'ютерних систем, що керують об'єктами критичної інфраструктури, з метою проведення терористичних актів.

Несанкціонованим доступом називається будь-який вид доступу без дозволу законного власника або особи, відповідальної за комп'ютер, систему комп'ютерів або комп'ютерну мережу. Також це поняття включає доступ до веб-сайту, програми, серверу, сервісу або іншої системи за допомогою чужого облікового запису [2; 3].

Зазвичай системні адміністратори налаштовують оповіщення про спроби несанкціонованого доступу, щоб вони мали змогу досліджувати причину. Ці сигнали можуть допомогти завадити хакерам отримати доступ до захищеної або конфіденційної інформації.

Атаки, де порушник не має привілеїв для доступу до цільової мережі і/або отримує доступ поза межами мережі (як правило, брандмауера), називають зовнішніми. Зовнішні атаки можуть бути здійснено проти внутрішньої мережі, використовуючи власні комп'ютери цільового об'єкта.

Існує багато способів компрометації комп'ютерної мережі ззовні [4]:

– доступ через слабкі, вкрадені або загублені облікові дані – найбільш поширена форма атаки;

– доступ через шкідливі програми – також загальний режим атаки. Користувач активує «троянського коня» – програму або інші види шкідливого програмного забезпечення, навмисно чи ненавмисно, що відкривають доступ до мережі;

– доступ через компрометації систем віддаленого доступу;

– ослаблений доступ третіх сторін – замість злому цілі зловмисник зламує комп'ютер, який має доступ до цілі;

– доступ через фізичне проникнення – отримання доступу до комп'ютерних мереж шляхом фактичного входу до приміщення з цільовим комп'ютером;

– доступ через модем – деякі організації досі підтримують застарілі системи комутованого зв'язку, що можуть бути дуже небезпечними;

– несанкціонований доступ за співпраці персоналу організації – з погрозами членам персоналу або вербуванням співробітників цільової організації до лав однодумців;

– доступ через бездротові системи. Wi-Fi-з'єднання є особливо проблематичним, оскільки важко встановити безпечну мережу. Також без відома IT-персоналу користувачі можуть налаштувати мережу, яка може надати прямий доступ до внутрішніх систем, оминаючи периметр безпеки мережі;

– пряме проникнення через периметр систем – мабуть, найважчий і найменш загальний підхід.

Атаки на цільову мережу, де порушник має законні привілеї, називають внутрішніми. Метою вторгнення є отримання доступу до заборонених, скритих даних і ресурсів. Внутрішні атаки, як правило, відбуваються набагато частіше, ніж зовнішні.

«Інсайдери» вже мають повноваження та привілеї для цільової мережі, а також прямий доступ до систем комп'ютерів всередині захищеного периметра мережі. «Інсай-

дери» зазвичай мають більше часу й можливостей, щоб дізнатися, як отримати доступ до обмежених систем і директорій. Вони також, ймовірно, знатимуть, які комп'ютери містять матеріал більшої для них цінності:

– несанкціонований доступ ІТ-персоналу – в організаціях не можна назвати несанкціонованим, оскільки ці співробітники, швидше за все, мають привілеї з комп'ютерної безпеки на високому рівні;

– несанкціонований доступ неспівробітників ІТ із привілеями високого рівня – не ІТ-користувачі не повинні, як правило, мати привілеї мережної безпеки на високому рівні, але інколи трапляються такі випадки. В інших випадках не ІТ-користувачі отримують ці привілеї за допомогою злому, домовленості, підкупу, погроз або відвертого злодійства;

– доступ через крадіжки облікових даних інших користувачів – деякі звичайні користувачі отримують доступ до систем, обмежених для інших користувачів;

– доступ до недостатньо забезпечених систем – деякі чутливі системи просто не мають достатнього захисту і можуть бути піддані загрозам зловмисниками без привілеїв високого рівня.

Троянський кінь, або троян, – це тип шкідливих програм, який часто маскується під легальне програмне забезпечення. Трояни можуть бути використані кіберзлодіями й хакерами, які намагаються отримати доступ до систем користувачів. Користувачі, як правило, обманним шляхом в тій чи іншій формі соціальної інженерії завантажують і запускають трояни на своїх комп'ютерах. Після активації трояни можуть дати змогу кіберзлочинцям шпигувати за користувачем, красти конфіденційні дані й отримати бекдор-доступ до всієї системи. Ці дії можуть включати в себе видалення даних, блокування даних, зміну даних, копіювання даних, зрив роботи комп'ютерів або комп'ютерних мереж.

На відміну від комп'ютерних вірусів і «черв'яків», троянські програми не здатні до поширення [5].

Під час установки або запуску з підвищеними привілеями троян, як правило, має необмежений доступ. Трояни бувають таких типів [6]:

• *руйнівний*, що викликає краш комп'ютера або пристрою, змінює або видаляє файли, пошкоджує дані, форматує диски, знищує весь їх вміст, поширює шкідливі програми мережею та може застосовуватися для шпигунства за користувачами й доступу до конфіденційної інформації [7].;

• *використання ресурсів або ідентичності* – це використання машини в складі ботнету (наприклад, задля виконання автоматичної розсилки спаму або для DDoS атаки), використання комп'ютерних ресурсів із метою видобутку корисної криптовалюти [8], використання зараженого комп'ютера як проксі-сервера для незаконної діяльності та/або атак на інші комп'ютери, зараження інших підключених пристроїв у мережі;

• *крадіжка грошей, викуп* – електронні крадіжки грошей, установка здирників, як-от CryptoLocker;

• *крадіжка даних,* в тому числі для промислового шпигунства, паролів користувачів або інформації про платіжні карти, особистої інформації користувача, торгових секретів;

• *шпигунство, або настирливе спостереження* – це спостереження за екраном користувача, перегляд веб-камери користувача, управління комп'ютерною системою віддалено або використання Key Logger – програмного продукту або апаратного пристрою, що реєструє кожне натискання клавіші клавіатури комп'ютера [9].

Троян може вимагати взаємодії зі шкідливим контролером, щоб виконати своє призначення. Цілком можливе сканування комп'ютерів у мережі, щоб знайти будь-який ПК із встановленим трояном, який хакер може контролювати [10].

Деякі трояни користуються вадами безпеки в застарілих версіях Internet Explorer і Google Chrome, щоб використовувати хост-комп'ютер як анонімний проксі-сервер із метою ефективного приховування використання інтернету [11], що дає змогу контролеру використовувати інтернет у незаконних цілях, тим часом як усі докази вказують на заражений комп'ютер або його IP-адресу. Комп'ютер-хост може або не може показати історію інтернет-сайтів, що переглядаються за допомогою комп'ютера як проксі-сервера. Перше покоління троянів-анонімайзерів, як правило, залишає сліди в історії хост-комп'ютера. Пізніші покоління троянів, як правило, ефективніше приховують сліди. Кілька версій Sub7 були поширені в США і Європі й стали найбільш поширеним прикладом таких троянів [10].

Через популярність ботнетів серед хакерів і наявність рекламних послуг, які дають змогу авторам порушувати конфіденційність своїх користувачів, трояни поширюються. Згідно з результатами опитування, проведеного BitDefender із січня по червень 2009 р., троян – «тип шкідливих програм, що знаходиться на підйомі й становить 83% світового шкідливого ПЗ, виявленого в світі». Трояни мають відносини з черв'яками, оскільки вони поширюються за допомогою черв'яків і ширяться інтернетом разом із ними [12]. BitDefender заявив, що близько 15% комп'ютерів є членами ботнету, як правило, набираються за допомогою троянської інфекції [6; 13].

Наступний тип – комп'ютерний вірус, що приєднується до програми або файлу та дозволяє їй переходити від одного комп'ютера до іншого, в результаті чого відбувається поширення вірусної інфекції. Як і людський вірус, комп'ютерний вірус може варіюватися за тяжкістю: деякі з них можуть викликати лише злегка дратівливі ефекти, а інші можуть призвести до пошкодження обладнання, програмного забезпечення або файлів. Майже всі віруси додано до виконуваного файлу, а це означає, що вірус може існувати на комп'ютері, але не може заразити комп'ютер, поки користувач його не запустить або не відкриє шкідливої програми.

Важливо зазначити, що вірус не може поширюватися без дій людини. Оскільки вірус поширюють люди, вони будуть несвідомо продовжувати поширення комп'ютерного вірусу шляхом обміну, інфікування файлів або відправки повідомлень електронної пошти з вірусами у вигляді вкладень в електронній пошті [14].

Віруси можна поділити на класи за методом, який використовується для зараження комп'ютера [15]: файлові віруси, віруси завантажувального сектора, макровіруси та скрипт-віруси. Будь-яка програма в рамках цього підкласу може мати додаткові функції трояну.

Комп'ютерний черв'як подібний до вірусу за дизайном і вважається підкласом вірусу. Черв'яки поширюються від комп'ютера до комп'ютера, але, на відміну від вірусу, вони мають змогу поширюватись без будь-яких дій людини. Черв'як використовує файл або інші функції для транспортування системою.

Найбільшою небезпекою черв'яка є його здатність копіювати себе в системі, тому замість відправки одного черв'яка комп'ютер може посилати сотні або тисячі копій самого себе, створюючи величезний руйнівний ефект. Одним із прикладів черв'яка є відправлення власних копій усім контактам в електронній поштовій скриньці. Потім черв'як розмножується й розсилає себе всім користувачам, перерахованим у кожній з адресних книг одержувачів [14].

Більшість відомих черв'яків поширюються у вигляді файлів, що відправляються як вкладення електронної пошти, за допомогою посилання на веб або FTP-ресурс, через посилання, відправлене в повідомленні ICQ або IRC, через P2P мережі загального доступу до файлів тощо [14].

Через природу копіювання черв'яка та його здатність подорожувати мережами кінцевим результатом здебільшого є те, що черв'як споживає занадто багато системної пам'яті

(або пропускної здатності мережі), внаслідок чого веб-сервери, мережні сервери та окремі комп'ютери припиняють відповідати на запити. Атаки таких черв'яків, як гучний Pro Blaster Worm, дають змогу зловмисникам керувати комп'ютером віддалено [14].

Варто також зазначити, що багато черв'яків використовують більше одного методу, щоб поширювати власні копії мережами.

Правила класифікації виявлених об'єктів із великою кількістю функцій мають бути використані для класифікації цих типів черв'яків. Цей підклас шкідливих програм включає в себе такі моделі поведінки: Email-Worm, IM-Worm, IRC-Worm, Net-Worm, P2P-Worm, вірус, черв'як.

DoS-атака також є особливою формою кібератаки, яка фокусується на перериванні мережного сервісу, що досягається відправленням зловмисниками великих обсягів трафіку або даних через цільову мережу, поки мережа не перевантажується («відмова в обслуговуванні»). Як правило, DoS-атака здійснюється одним комп'ютером або одним центральним розташуванням комп'ютерів. Популярна категорія атак DoS – розподілена атака на відмову в обслуговуванні (DDoS), що відрізняється від звичайної DoS-атаки кількістю комп'ютерів, що беруть у ній участь. Ці комп'ютери працюють разом за допомогою інтернету для передачі трафіку до цільової мережі.

Інший термін, що зазвичай асоціюється з атаками DoS, − «ботнет», що являє собою групу комп'ютерів, які зловмисник взяв під контроль із метою реалізації власних злочинних посягань. Часто справжній власник комп'ютера навіть не здогадується, що його комп'ютер було зламано. Скомпрометовані комп'ютери називаються «ботами» або «зомбі», тому що вони знаходяться під впливом/керуванням іншого комп'ютера. Використовуючи бот-мережу, зловмисник має обчислювальну потужність, необхідну для запуску DDoS-атаки, що дає йому змогу легше вивести цільову мережу з ладу.

Є кілька способів виконати DoS-атаку [16]: відправка неправильної форми пакетів даних до мережі; переповнення буфера – затоплення серверу переважаючою кількістю даних; обман комп'ютерів із метою відповідей на фальшиві запити, внаслідок чого генерується багато трафіку; порушення фізичного з'єднання, наприклад, кабелю або джерела живлення.

Зловмисники можуть використовувати різні техніки (так звані методи сканування) для того, щоб знайти вразливі машини. Найчастіше вживаними способами є [17]:

– *випадкове сканування.* Комп'ютер, який заражено шкідливим кодом, обирає IP-адреси випадково з IP-адресного простору і перевіряє їхню вразливість. Коли вірус знаходить вразливий комп'ютер, він проводить копіювання свого коду на нього й намагається заразити його. При цьому створюється значний трафік. Перевага цього методу сканування в тому, що шкідливий код може поширюватися дуже швидко. Проте висока швидкість, до якої розганяється поширення шкідливого коду мережею, не може тривати вічно. Після невеликого періоду часу швидкість поширення зменшується, адже кількість нових IP-адрес, які можуть бути виявлені, зменшується з часом;

– *хіт-лист сканування.* Ще задовго до початку сканування зловмисники збирають список великої кількості потенційно вразливих комп'ютерів. Потім вони починають сканування цього списку. Коли знаходять один комп'ютер, то встановлюють на нього шкідливий код і виконують поділ списку навпіл. Потім вони надають одну половину щойно скомпрометованому комп'ютеру, а іншу половину продовжують сканувати власноруч. Заражений хост починає сканування свого списку, намагаючись знайти інший вразливий комп'ютер. Коли він знаходить, то реалізує подібну процедуру, і таким чином хіт-лист сканування відбувається одночасно з стійко зростаючою кількістю заражених комп'ютерів. Цей механізм гарантує, що шкідливий код встановлюється на всіх вразливих комп'ютерах, що містяться в списку, за короткий проміжок часу;

– *топологічне сканування* використовує інформацію, що міститься на зараженому комп'ютері, щоб знайти нові цілі. Точність цього методу дуже висока, а його продуктивність схожа на хіт-лист сканування. Топологічне сканування може створити велику армію нападників дуже швидко й таким чином може прискорити поширення шкідливого коду;

– *локальне сканування* підмережі діє за брандмауером у районі, який вважається зараженим шкідливою програмою сканування. Вражений хост шукає цілі у своїй власній локальній мережі, використовуючи інформацію, яку сховано в локальних адресах. Одна копія програми сканування працює за брандмауером і намагається зламати всі вразливі машини, які в іншому разі було б захищено файєрволом. Цей механізм може бути використано в поєднанні з іншими механізмами сканування;

– *сканування перестановкою* передбачає, що всі машини спільно використовують загальний псевдовипадковий список перестановки IP-адрес, який може бути побудовано з використанням будь-якого блочного шифру з 32 біт із заздалегідь обраним ключем [18]. Якщо хост було заражено або під час сканування хіт-списку, або локального сканування підмережі, він починає сканування відразу після його місця в списку перестановок і переглядає цей список, щоб знайти нові цілі. В іншому разі, якщо хост було заражено під час сканування перестановкою, він починає сканування в довільний момент часу. Щоразу, коли він стикається з уже зараженим комп'ютером, він вибирає нову точку випадкового запуску в списку перестановок і починає роботу звідти. Зламаний вузол може розпізнати вже заражений комп'ютер серед неінфікованих, такі комп'ютери реагують на сканування по-іншому. Процес сканування зупиняється, коли заражений хост зустрічає послідовно зумовлену кількість вже інфікованих комп'ютерів, не знаходячи нових цілей протягом визначеного періоду часу. Тоді генерується новий ключ і починається нова фаза сканування. Основні цілі цього механізму: це дає змогу уникнути непотрібних реінфекцій тієї ж самої цілі, тому що, коли заражений хост розпізнає вже ослаблений комп'ютер, він змінює спосіб сканування відповідно до процесу, описаного раніше. Цей механізм підтримує плюси випадкового пошуку, адже сканування нових мішеней відбувається випадково – це скоординоване сканування з надзвичайно гарною продуктивністю, бо механізм рандомізації дає змогу отримувати високі швидкості сканування [19].

За допомогою зовнішніх атак часто буває дуже важко своєчасно вжити дієві заходи протидії порушникам, тому пріоритет має бути віддано таким діям [20]:

1. виявити й захистити вразливі системи; за потреби вимкнути системи живлення;

2. визначити точку вторгнення й закрити її; при необхідності вимкнути системи живлення;

3. очистити вражені системи для backdoor програмного забезпечення або руткітів, якщо немає впевненості, що всіх їх було очищено, відновити пошкоджені системи з резервних копій;

4. зберегти всі ключові логи на комп'ютерах, міжмережних екранах та інших мережних пристроях;

5. змінити всі паролі та інші облікові дані – в пріоритеті адміністративні та високо-привілейовані облікові записи, в тому числі ті, що призначено для таких сервісів, як система резервного копіювання;

6. перевірити стан оновлення безпеки всіх систем і зробити новий патч.

Внутрішні атаки важче контролювати, оскільки порушник не може бути виключений із периметра мережі і може мати законні привілеї мережі. Тому усунення наслідків атаки передбачає такі заходи [20]:

1. виявити й захистити вразливі системи; у разі потреби вимкнути системи живлення або ізолювати систему;

2. вимкнути всі облікові записи користувачів, підозрюваних у хакерстві;

3. створити комп'ютерні судово-медичні зображення основних порушень системи. Вони будуть необхідні, щоб визначити джерело будь-якого внутрішнього вторгнення і вжити правових заходів згодом;

4. зберегти всі ключові логи на комп'ютерах, міжмережних екранах та інших мережних пристроях;

5. підвищити фізичні міри безпеки. переконатися, що порушники не присутні в приміщеннях організації;

6. очистити вражені системи для backdoor програмного забезпечення або руткітів. Якщо немає впевненості, що всіх їх було очищено, відновити пошкоджені системи з резервних копій;

7. змінити всі паролі та інші облікові дані – в пріоритеті адміністративні та високо-привілейовані облікові записи, в тому числі ті, що призначено для таких сервісів, як система резервного копіювання;

8. перевірити стан оновлення безпеки всіх систем і зробити новий патч.

Зазвичай зловмисники використовують трояни з метою підвищення обчислювальної потужності. Проте їх досить легко розпізнати на комп'ютері. Гарний приклад тому – видобування криптовалюти або підготовка до DDoS-атаки. В кожному з цих випадків користувач може помітити зниження продуктивності тієї чи іншої системи комп'ютера.

Для того, щоб уникнути потрапляння вірусу до комп'ютеру, необхідно дотримуватись деяких досить простих рекомендацій [18]:

– встановити якісний антивірус;

– встановити антишпигунське програмне забезпечення, що працює в режимі реального часу;

– постійно оновлювати антивірусне програмне забезпечення;

– проводити щоденне сканування системи;

– відключити автоматичний запуск програм;

– відключити автоматичне відображення зображень в Outlook або інших поштових клієнтах;

– не натискати на вкладення підозрілих листів електронної пошти;

– використовувати «захист посилань», вбудований до браузера;

– використовувати апаратний брандмауер;

– запустити захист DNS.

Найкращий спосіб видалити цей вірус із системи – знайти та видалити троян із системи. Під час видалення троянів вручну необхідно впевнитись у тому, що видалено абсолютно всі частини вірусу, а також необхідно видалити всі програми, які троян міг пошкодити. В цьому може допомогти антивірусне програмне забезпечення або програми безпосередньо для видалення троянів.

Оскільки троянам необхідний обов'язковий запуск користувачем, рекомендовано не відкривати файли невідомого походження з розширенням .exe, .vbs, .bat тощо.

Попередження зараження комп'ютера вірусом або черв'яком досить схоже на боротьбу з троянами. Розглянемо деякі з типових симптомів комп'ютерного черв'яка: низька продуктивність комп'ютера, збої в роботі, несанкціонований запуск програм або автоматичний запуск, нерегулярна продуктивність веб-браузера, незвична поведінка комп'ютера (повідомлення, зображення, звуки тощо), мережний екран попередження, відсутні/змінені файли, поява дивних/ненавмисних настільних файлів або іконок, помилки операційної системи і повідомлення про помилки системи, електронні листи, надіслані контактам без відома користувача.

Існує кілька кроків, які треба здійснити задля видалення комп'ютерного черв'яка. Важливо відключити комп'ютер від інтернету і локальних мереж, перш ніж здійснювати будь-які інші дії для видалення черв'яка. Для того, щоб запобігти поширенню черв'яка, треба використовувати незаражений комп'ютер для завантаження оновлень або необхідних програм для подальшого встановлення їх на зараженій машині через зовнішній пристрій. Після того як комп'ютер було відключено від мереж, необхідно переконатися, що всі антивірусні сигнатури оновлено, просканувати комп'ютер із використанням антивірусного програмного забезпечення, видалити шкідливі програми й очистити або видалити заражені файли, оновити операційну систему комп'ютера до останньої версії й установити всі патчі для програмного забезпечення і додатків.

Заради активної протидії DDoS-атакам необхідно використовувати пристрої або відповідне програмне забезпечення для аналізу мережного трафіку. Одним із найбільш популярних підходів є вибірка потоку, оскільки практично всі маршрутизатори підтримують якусь форму технології Flow, наприклад NetFlow, IPFIX або SFlow. У цьому процесі маршрутизатор збирає пакети й експортує датаграму, що містить інформацію про пакунок. Це зазвичай доступна технологія, що добре масштабується і є цілком достатньою, щоб визначити тенденції мережного трафіку.

Пристрій для аналізу вмісту має оцінити поведінку потоку трафіку протягом тривалого періоду, щоб переконатися, що щось не так, і уникнути помилкових спрацьовувань.

Загальний захист від DDoS-атак використовує пристрій аналітики потоку, який реагує на виявлений інцидент, перенаправляючи трафік жертви до пристрою пом'якшення. Цей метод добре масштабується для збору трафіку для аналізу, а реактивна модель тільки перенаправляє потенційно поганий трафік, що дає змогу системі деякий час працювати.

Як альтернатива віддзеркалення пакетів даних забезпечує повну деталізацію для аналізу, але не обов'язково на шляху руху. Це дає змогу швидко виявити аномалії в русі, які, можливо, вводяться з інших точок входу до мережі.

Періодична перевірка продуктивності безпеки мережі має вирішальне значення для забезпечення того, щоб рішення в області безпеки будуть витримувати різні одночасні атаки [18].

З метою організації ефективної боротьби з терористичною діяльністю в кіберпросторі буде корисно розглянути три етапи захисту комп'ютерних систем та мереж:

1. профілактика: як можна вберегтись від запуску атаки?
2. управління інцидентами, пом'якшення атаки, обмеження збитків: атака досягла мети. Як можна підготуватися й провести захист під час нападу? Як можна перемогти атаку без втрат? Як визначити й обмежити збитки?
3. управління наслідками: що робити після нападу?

Профілактика. Основний підхід полягає в розробці такої системи, яку буде захищено від нападу з самого початку. Якщо це буде зроблено належним чином, атакам можна запобігти, тому що вони будуть сприйматися як марні, або якщо атаки вже запущено, вони не зможуть викликати жодних пошкоджень.

На жаль, для більшості IT-систем безпека не є основним критерієм дизайну. Оскільки майже всі кіберсистеми не було спочатку розроблено з урахуванням вимог безпеки, нині широко використовуються величезна кількість небезпечних систем. Проблема поширюється через те, що критерії безпеки часто конфліктують із проектними критеріями, які найкращим чином сприяють первинним намірам і потребам організації. Доступ і пропускна здатність є прикладами таких критеріїв проектування. Додавання захисту не тільки потребує великих коштів, але також може призвести до зниження ефективності й функціональності.

Різні форми попередження або перехоплення також можуть бути можливими. Перехоплення зупиняє атаку, яку було запущено, протидіє досягненню мети. Ці заходи можуть розглядатися як дієві форми профілактики. Попереджувальні удари або перехоплення можуть бути або в кіберпросторі, або фізичні.

З трьох основних етапів оборони профілактика має більш активну форму. Необхідно організувати виявлення зловмисників або потенційних зловмисників і переконати їх у тому, що існує висока ймовірність того, що їх буде покарано.

Більшість форм активної оборони мають проводитися урядами. Міждержавне співробітництво, ймовірно, буде стимулом для подальшого розвитку активних захисних стратегій в таких областях, як, наприклад, обмін розвідувальною інформацією. Здебільшого приватні особи, що займаються активною обороною, ризикують бути ідентифікованими і помилково сприйматися як злочинці.

Із позиції ризику окремі терористи й терористичні організації (навіть ті, яких підтримують національні держави) відрізняються від національних держав. Терористи й терористичні організації мають мало активів і жодної суверенної території для захисту від фізичних або інших форм контратак або ембарго. В результаті вони не чутливі до більшості можливих наслідків від національних держав, які можуть бути спричинені виявленням кібератак.

З іншого боку, з огляду на можливості катастрофічного тероризму для оборони вкрай важливо спробувати запобігти атакам, виявити й затримати чи іншим чином покарати потенційних зловмисників.

Управління інцидентами, пом'якшення атаки, обмеження збитків. Найголовнішим обов'язком фахівців на цьому етапі оборони є надання вказівок і попереджень, що напад відбувається. Це легше зробити на цьому етапі, ніж на стадії профілактики. Проте це важко, і виявлення вторгнень стає активною областю в галузі досліджень і розробок. Тож недивно, що виявлення й оповіщення є більш важкими й схильними до помилкових спрацьовувань на ранніх стадіях атаки, до того як було завдано значної шкоди.

Для того, щоб запобігти проникненню загрози ззовні до системи, зазвичай зводяться бар'єри для укріплення з використанням як кібер-, так і фізичних підходів. Паролі є найстарішою технікою, яка досі широко використовується. Пізніше стали використовуватися брандмауери й проксі-сервери. Як і всі форми кібероборони, їх можна перемогти, хоча вони можуть витримати багато спроб нападів. Фізичний захист має враховувати кілька форм проникнення або спроби ізолювати систему. До них належать напад на електроніку за допомогою електромагнітних імпульсів, спроби закоротити кінці проводів. Можлива широка різноманітність форм фізичного захисту, починаючи від парканів і закінчуючи біометрією.

Якщо систему атакують ззовні, чергова лінія оборони й стримування є внутрішньою. У цьому разі необхідно обмежити проникнення й пошкодження, захистити живі активи, а також захистити від збору інформацію, щоб допомогти з відновленням й реакцією після нападу. Підходи включають створення внутрішніх фізичних бар'єрів і кібербар'єрів через роздробленість, контроль доступу, створення помилкових цілей, підтримання охоронюваних звільнень і приховування активів. Усі вони мають як статичні (попередньо встановлені й незмінні під час атаки), так і динамічні варіанти.

Інший підхід полягає в автоматичному або частковому відключенні й перерозподілі. Система, яка розуміє, що знаходиться під атакою, починає зводити внутрішні бар'єри, які не були б потрібними під час нормальної роботи, намагаючись ізолювати ті частини системи, які було скомпрометовано. Також система включає стратегії скидання навантаження, перерозподілу можливості виживання для найбільш важливих функцій, необхідних організації.

Особливу увагу необхідно приділити збереженню та збору інформації під час нападу. Це робиться в основному шляхом аудиту та резервного копіювання. Необхідно знайти найостаннішу «чисту» (до атаки) версію системи з метою сприяння ефективному відновленню й поновленню операцій. Це легко можна зробити, якщо напад має чіткий і точний час початку, а резервне копіювання проводиться на регулярній основі. Більш підступними є атаки, які накопичуються повільно й непомітно. Під час таких атак набагато складнішою проблемою є ідентифікація стану, коли інформацію було ще не пошкоджено й система була вільна від шкідливого коду. Важливо також мати сильні функції аудиту для визначення факту, коли атака почалася, і збирати інформацію, яка може допомогти у виявленні й затриманні зловмисника.

Підвищення безпеки для систем SCADA/DC створює особливо складні проблеми. Ці системи часто малі й самодостатні, з обмеженою потребою в електроенергії (в тому числі резервному копіюванні). Заходи безпеки можуть привести до зниження продуктивності або бути проблематичними в синхронізації інших більш широких процесів. Крім того, більшість цих систем використовується в приватному або змішаному секторах (наприклад, в аеропортах). Їхні власники й оператори можуть не мати достатніх ресурсів для забезпечення безпеки більш ефективними способами.

З позиції боротьби з кібертероризмом, можна припустити, що напад на фізичні цілі через системи контролю та управління призведе до масових жертв, пошкоджень, страху, що на користь терористам. Багато цих систем вразливі для маніпуляцій із сигналами керування.

Велика частина діяльності на цій оборонній стадії є пасивною й може бути описана як «термінал захисту», тому що він перебуває в руках власників і операторів частин кіберпростору, які в основному знаходяться в приватному секторі.

Управління наслідками. Є дві основних складових частини на цьому етапі оборони: відновлення й реагування. Відновлення значною мірою передбачає відтворення IT-активів, тому організація може працювати якомога ближче до нормального стану. Це пасивна форма захисту. Реагування передбачає виявлення й покарання винних і засвоєння уроків, щоб дати змогу організації краще захистити себе в майбутньому. Таким чином, це більш активна форма захисту.

Зразок завдань, які підпадають під відновлення, може включати у себе:

– видалення або відключення ворожих або дефектних утворень;

– обстеження, оцінка збитків від того, що було порушено або змінено;

– автоматичний або напівавтоматичний процес оцінки й перерозподілу того, що залишилося;

– пріоритезацію функцій для відтворення;

– відновлення на доаварійний статус до атаки таким чином, аби не зруйнувати доказів проведення кібератаки.

Ретельно задумані й виконані атаки можуть зробити відновлення більш важким. Наприклад, атаки, що пошкоджують дані або вставляють до них шкідливий код, можуть бути виконані таємно протягом тривалих періодів часу, або в масках, тому адміністраторам безпеки буде важко знайти незабруднені версії резервного копіювання. Така «експансія» може мати місце протягом тривалого часу, одночасно з додаванням багатьох законних угод, які власник не захоче втратити під час відновлення. Нині більшості організацій, які постраждали від короткострокових атак, вдалося відновити інформацію досить швидко й ефективно [21].

Зазвичай адміністратори в компаніях встановлюють дуже сильну політику безпеки, яка включає міри з розподілу мереж на підмережі. При цьому всі можливі пакети між підмережами передаються тільки через брандмауер. Це стосується також і вхід-

ного трафіку з інтернету. В цьому разі брандмауер може попередньо просканувати інформацію, що передається, на наявність вірусів чи шкідливого програмного забезпечення.

Задля уникнення можливості поширення вірусів одним з основних заходів безпеки є відключення USB-портів. Відключення можна провести в кілька етапів: відключення через операційну систему, відключення через BIOS (якщо модель дозволяє) і найбільш радикальний, а тому і найбільш дієвий спосіб – відключення USB-порту фізично від материнської плати комп'ютера.

Не рекомендовано давати користувачам доступ до системного диску комп'ютера, оскільки вони можуть зі встановленням програми занести до нього вірус. Краще б було заборонити користувачам самостійно встановлювати програми, якщо політика компанії це дозволяє. Ідеальною є компанія, в якій усі можливі інсталяції програм, необхідних для співробітників, розміщуються на одному з серверів. Кожна з цих інсталяцій пройшла перевірку на віруси. І, коли в користувача виникає потреба у встановленні нового програмного забезпечення, він може підключитись до цього серверу або підійти до нього фізично і встановити собі на комп'ютер програму власноруч, не викликаючи при цьому адміністратора. Цілком природно, що всі дії користувачів записуються, і для встановлення програмного забезпечення необхідно ввести логін та пароль користувача з відповідними правами доступу.

Для боротьби з фізичними вторгненнями рекомендовано на кожному порту комутаторів та маршрутизаторів вписати конкретні MAC-адреси комп'ютерів, які мають підключитись. Якщо мережні пристрої не мають такої змоги, необхідно вписати список усіх адрес комп'ютерів до брандмауеру.

Зазвичай багатьох наслідків проведення кібератак можна було б уникнути, якщо б хтось з персоналу організації-цілі не відкрив файл із вкладенням або вчасно видалив підозрілий файл із флешки. Тому для організацій, де більшість персоналу – люди, які мають тільки базові навички роботи з комп'ютерами, було б доцільно періодично проводити інструктаж із кібербезпеки, який включає пояснення визначень вірусів та іншого шкідливого програмного забезпечення та методів протидії їм.

Процес проектування системи захисту персонального комп'ютера умовно можна поділити на **етапи**, наведені нижче.

Фізичний захист. Установка пароля BIOS та запобігання доступу до комп'ютера або до його змінних пристроїв. Не варто використовувати зовнішній жорсткий диск для важливої інформації, оскільки він представляє собою ще одну вразливість: його може бути вкрадено або загублено.

Проте шифрування може бути ефективним засобом проти крадіжки. Шифрування окремих файлів дає мало результату, необхідно шифрувати весь обліковий запис користувача. Однак це може вплинути на продуктивність комп'ютера.

Брандмауер. Бажано мати брандмауер як на комп'ютері, так і на маршрутизаторі. Більшість інтернет-провайдерів пропонують безплатний маршрутизатор і модем. Такі маршрутизатори не обов'язково мають більш-менш пристойний брандмауер. Технічно підкована людина може навіть оновити прошивку на багатьох маршрутизаторах із метою підвищення безпеки всередині мережі.

Більшість операційних систем нині має вбудований брандмауер. Він блокує несанкціоновані з'єднання, захищає операційну систему та інше програмне забезпечення на комп'ютері від шкідливих програм, які використовують вразливості в системних службах, що працюють із мережами.

Налаштування системи. Windows створює певний рівень прав та привілеїв залежно від типу користувача. Рекомендовано використовувати стандартний обліковий

запис користувача (а не адміністраторський). У такому разі шкідлива програма не матиме доступу до системи.

Рекомендовано вимкнути Java. Більшість користувачів має стару версію Java. Java має чимало дірок у безпеці, аби нашкодити комп'ютеру. Java-апплети використовуються дуже рідко сьогодні, тому тільки вузькому колу користувачів вона справді необхідна. Якщо на комп'ютері немає програмного забезпечення, яке запускається за допомогою JVM, краще видалити Java взагалі, але якщо вона необхідна, треба вимкнути браузерний плагін Java для того, щоб захистити комп'ютер.

Програмне забезпечення.

Антивірус. Краще використовувати відомі антивірусні продукти, створені великою компанією з підтримки безпеки, оскільки вони зазвичай мають найбільшу та найповнішу базу сигнатур. Необхідно налаштувати автоматичне сканування системи та автоматичне оновлення бази.

Антишпигунське ПЗ. Шпигунське програмне забезпечення може збирати особисту інформацію, змінювати конфігурацію комп'ютера або додавати небажані спливаючі вікна й рекламу. Такого програмного забезпечення після встановлення досить важко позбутись, тому краще використовувати як профілактику антишпигунське програмне забезпечення.

Захист браузера. Перед тим, як почати користуватись інтернетом, треба захистити браузер. Для цього існують плагіни, що йдуть у пакеті з антивірусним програмним забезпеченням, або їх можна закачати та встановити окремо.

Рекомендації для користувачів. Проте дотримання усіх цих вимог не забезпечує стовідсоткового захисту, оскільки здебільшого зараження системи відбувається тільки через дії користувача. Тому для користувачів сформулюємо низку рекомендацій:

– необхідно бути обережними в інтернеті й не натискати підозрілі посилання;

– використовувати безпечні паролі та не копіювати їх для різних сервісів. Паролі мають буди різними для кожного сайту/системи;

– остерігатися фішингу та соціальної інженерії;

– бути обережними з програмами, які завантажуються та запускаються з мережі;

– не довіряти відкритим точкам доступу Wi-Fi;

– постійно оновлювати все програмне забезпечення до нових версій;

– відключати інтернет-з'єднання, коли не має потреби в користуванні ним.

Наведено практичні рекомендації щодо захисту персональних комп'ютерів та комп'ютерних мереж від зовнішніх та внутрішніх вторгнень. Розглянуто способи профілактики кібератак, обмеження пошкоджень під час нападу та ліквідації наслідків. Запропоновано прототип системи захисту комп'ютера.

Список використаних джерел:

1. Клочко А.М. Проблемні питання транснаціональної кіберзлочинності. Актуальні питання розслідування кіберзлочинів: матеріали Міжнародної науково-практичної конференції (м. Харків, 10 грудня 2013 р.). Х.: ХНУВС, 2013. С. 34−36.

2. Forms of Cyber Terrorism. URL: http://maryamheidari.blogspot.com/2010/04/forms-of-cyber-terrorism.html

3. Unauthorized access. URL: http://www.computerhope.com/jargon/u/unauacce.htm

4. Unauthorized access. URL: http://itsecurity.telelink.com/unauthorized-access-2/

5. Trojans. URL: https://usa.kaspersky.com/internet-security-center/threats/trojans#.WEbvB_l97IU

6. Trojan horse (computing). URL: https://en.wikipedia.org/wiki/Trojan_horse_(computing)

7. Hackers, Spyware and Trojans – What You Need to Know. URL: https://www.comodo.com/resources/home/spyware-trojans.php

8. Robert McMillan (2013): Trojan Turns Your PC Into Bitcoin Mining Slave, Retrieved on 2015-02-01.

9. Keystroke logging. URL: https://en.wikipedia.org/wiki/Keystroke_logging

10. Jamie Crapanzano (2003). Deconstructing SubSeven, the Trojan Horse of Choice. SANS Institute, Retrieved on 2009-06-11.

11. Vincentas (11 July 2013). Trojan Horse in SpyWareLoop.com. Spyware Loop. Retrieved 28 July 2013.

12. BitDefender Malware and Spam Survey finds E-Threats Adapting to Online Behavioral Trends. URL: https://www.bitdefender.com/news/bitdefender-malware-and-spam-survey-finds-e-threats-adapting-to-online-behavioral-trends-1094.html

13. Datta Ganesh. What are Trojans? URL: http://securaid.com/windows/2014/08/what-are-trojans/

14. The Difference Between a Computer Virus, Worm and Trojan Horse. URL: http://www.webopedia.com /DidYouKnow/Internet/virus.asp

15. Viruses and worms. URL: https://securelist.com/threats/viruses-and-worms/

16. History of Computer Crime | Cyber Security. URL: .http://www.personal.psu.edu/users/j/m/jms6423/Engproj/Types%20of%20Attacks.html

17. Nicholas C Weaver, Warhol Worms: The Potential for Very Fast Internet Plagues. URL: http://www.iwar.org.uk/comsec/resources/worms/warhol-worm.htm

18. Weaver N. Potential Strategies for High Speed Active Worms: A Worst Case Analysis. URL: http://citeseerx.ist.psu.edu/viewdoc/ summary?doi=10.1.1.218.2524

19. Charalampos Patrikakis, Michalis Masikos, and Olga Zouraraki, Distributed Denial of Service Attacks. The Internet Protocol Journal. Volume 7, Number 4. URL: . http://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-30/dos-attacks.html

20. Police and Justice Act 2006. URL: http://www.legislation.gov.uk/ukpga/2006/48/part/5/crossheading/computer-misuse

21. URL: http://www.personal.psu.edu/users/j/m/jms6423/Engproj/Types%20of%20Attacks.xhtml