ISSN 2224-087X. Електроніка та інформаційні технології. 2017. Випуск 7. С. 93–104
Electronics and information technologies. 2017. Issue 7. P. 93–104

УДК 004.49:004.77

АКТУАЛЬНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА СПОСОБИ ЇХНЬОГО ВИРІШЕННЯ

Ю. Корчак, Ю. Фургала

Львівський національний університет імені Івана Франка,
вул. Ген. Тарнавського, 107, 79017 Львів, Україна
yurakorchak@yahoo.co.uk

Проаналізовано сучасний стан глобальної інформаційної безпеки, описано нові кіберзагрози, напрями та методи боротьби з ними. Інтегрування технологій повсюдної безпеки дасть змогу замовникам і надавачам послуг використовувати переваги загрозоорієнтованого захисту, оскільки саме такий тип захисту найбільш актуальний для протидії сучасному динамічному ландшафту загроз. Тільки в разі запровадження повсюдного захисту можна без зайвих ризиків використовувати можливості, які надає цифрова економіка і всеосяжний інтернет. Особливу увагу також звернено на таке шкідливе програмне забезпечення, як руткіти, які значно небезпечніші, ніж віруси.

Ключові слова: інформаційна безпека, кібератака, мережева інфраструктура, хакер, вірус, руткіт.

Сучасний стан з кіберзагрозами у світі, основні напрями кібератак.

За підрахунками компанії Symantec загальний збиток від кібератак по всьому світі 2015 р. становив 158 млрд дол. Експерти зазначили, що загалом у світі за 2015 р. від дій хакерів постраждало 594 млн осіб – у середньому на кожну з них припало 358 дол. збитку. Також експерти підрахували, що на усунення технічних збоїв, спричинених діями хакерів, витрачали в середньому 21 год. [1].

Рік 2015 справді був досить показовим та "багатим" на кібератаки і засвідчив, що навіть найнадійніший захист великих міжнародних корпорацій може зазнати зламу. Навіть добре захищені компанії не вистояли перед нападом хакерів, зокрема, такі: американська Служба управління персоналом; американська компанія з медичного страхування Anthem and Premera; мережі готелів Mandarin Oriental, Hilton і Trump Hotels; британська телекомунікаційна компанія TalkTalk; гонконзький інтернет-магазин VTech [2].

Ще 2014 р. група хакерів зламала сервери відомої кінокомпанії Sony Pictures, поступово викладаючи в мережу особисті дані співробітників, піратські копії фільмів та іншу секретну інформацію. Атака завдала збитків, від яких кінокомпанія оговтується досі. У 2015 р. особливої популярності набули кібербанди, які займаються здирництвом, – такі як хакери групи під назвою DD4BC, які використовували DDoS-атаки для вимагання грошей від інтернет-компаній, корпорацій і приватних людей.

У жовтні 2015 р. на телекомунікаційну компанію TalkTalk вчинено чергову потужну DDoS-атаку. Веб-сайт провайдера на декілька годин вийшов в оф-лайн. І за цей час зловмисники встигли вкрасти дані клієнтів компанії: номери телефонів, адреси, контактні дані й навіть номери кредитних карток, банківські реквізити. Оскільки в

компанії близько 4 млн клієнтів, то масштаби проблеми достатньо глобальні. Після нападу хакерів акції TalkTalk знизилися на 10 %. Та й загалом затрати на подолання наслідків досягли близько 35 млн фунтів.

Це вже третя за рік кібератака на сервери TalkTalk. Не відомо, чи була вся персональна інформація клієнтів зашифрована.

Унаслідок слідства поліція Скотленд-Ярду арештувала п'ятьох осіб. Серед них – 18-річний підліток, який виклав у мережу близько мільйона користувацьких даних. Наймолодшого підозрюваного – 15-річного хлопця – арештували на поліційній дільниці графства Антрім і надалі передали на поруки рідним. Найстаршому із затриманих – 20 років.

Порівняно з американським британське законодавство лояльніше ставиться до порушень подібного типу.

Викрадення даних про кредитні картки в готелях Mandarin Oriental Hotel Group засвідчило, наскільки слабкою може бути безпека в POS терміналах. Дані були вкрадені з кредитної картки за допомогою "ізольованого номера" систем платіжної картки в готелях Європи і США після того, як мережу компанії зламали. Керівництво готелів стверджує, що вкрадено лише дані про саму кредитну картку. Особиста інформація про відвідувачів, номери рахунків, паролі й усе решта залишилось недоторканим.

Програмне забезпечення деяких готелів Mandarin Oriental було інфіковано шкідливим ПЗ. Проте спеціалісти виявили і ліквідували вірус. Тепер компанія активно співпрацює з правоохоронними органами і підвищує рівень кібербезпеки своїх готельних комплексів. Подібного нападу зазнали й інші мережі готелів, наприклад, Hilton, Starwood Hotels, Trump Hotels.

Зростають апетити кібербанди DD4B, яка використовує DDoS-атаки для вимагання Bitcoin (цифрової чи крипто-валюти, яка не підтримується центральним банком чи урядом країни). За допомогою маневрів з Bitcoin хакери грали в он-лайн казино і букмекерських канторах, займались вимаганням у великих фінансових закладах США, Європи, Азії, Австралії і Нової Зеландії.

У квітні 2015 р. компанія з інформаційної безпеки FireEye звинуватила китайський уряд у тому, що він чи не керує кібершпигунською компанією, і це триває вже десятиліття. Основна мета компанії – викрадення засекреченої інформації, яка належить організаціям у Південно-Східній Азії та Індії. Те, що подібного типу DDoS-атаки виходять на державний рівень, підтверджують останні події осені 2016 р., пов'язані з президентськими виборами в США. За вказівкою і зі сприянням уряду Росії хакери провели DDoS-атаки на сервери Демократичної партії США з метою впливу на майбутнє волевиявлення громадян США щодо вибору свого президента. У 2015 р. компанія Symantec розсекретила корпоративну шпигунську групу Morpho, яка за останні декілька років загрожувала низці великих корпорацій.

У 2015 р. влада США арештувала дев'ять підозрюваних торгових трейдерів, які, за попередніми даними, перебували у змові з кібербандою DD4B. Підозрювані сподівалися, що хакери здобудуть для них секретну комерційну інформацію з новинних ресурсів.

Сьогодні британські співробітники правоохоронних органів працюють із партнерами з державного і приватного сектора, щоб допомогти компаніям і британським споживачам боротися з кіберзлочинами.

Після численних потужних атак на корпорації по всій Великій Британії організація NCA розпочала активно допомагати мережевим адміністраторам управляти клю-

човими частинами британської інтернет-інфраструктури. Британський уряд узяв участь у декількох міжнародних операціях, спрямованих на боротьбу з кіберзлочинами. Зокрема, правоохоронні організації, урядові команди з кібербезпеки і приватні організації брали участь у ліквідації ботнету (скорочення від двох англійських слів – robot і network) Dorkbot. За допомогою цієї шкідливої програми зловмисники інфікували комп'ютери багатьох користувачів з усього світу. Вірус поширюється через соціальні мережі, спам, тверді носії. Фактично дія Dorkbot нагадує класичний троян – порушується робота антивірусних продуктів, блокується оновлення. Шкідлива програма отримує інструкції від хакерів через протокол IRC.

Агентство NCA спільно з європейськими агентствами зі злочинів зупинило роботу серверів, які використовував цей ботнет. Також проведено низку арештів у 140 аеропортах різних країн. Під час цієї міжнародної правоохоронної операції затримано близько 130 підозрюваних.

У червні 2015 р. ФБР закликало компанії до особливої пильності. Співробітники служби безпеки повідомили про те, що в мережі поширився тип шкідливого програмного забезпечення, яке шифрувало дані компанії. За надання ключа декодування зловмисник, який запустив процес, звичайно вимагав гроші.

Цей тип шифрування достатньо складно виявити, оскільки він належить до сім'ї CTB-Locker з її новими версіями (CryptoWall, TorrentLocker і BandaChor). Сім'я CTB-Locker використовує розумні методи ухилення від захисного програмного забезпечення, уникає виявлення фішингових листів.

Лабораторія McAfee радить організаціям у пріоритеті вивчати ознаки електронних фішингових листів, а також використовувати інструменти типу Intel Security Phishing Quiz.

Рік 2015 ще раз засвідчив важливість посиленої кібербезпеки. Недооцінювати серйозність DDoS-атак не тільки досить небезпечно, а й дорого. За попередніми даними британської компанії Neustar, втрати можуть досягти 100 тис. фунтів за годину.

Найбільш знаковою з останніх подій осені 2016 р. стала DDoS-атака на низку американських сайтів, яка за масштабом перевищила рівень загрози колишнього нападу на нью-йоркські вежі-близнята. Жодна з відомих хакерських груп технічно неспроможна вчинити такий злочин, він під силу тільки державі з відповідними технічними можливостями [3].

За підсумками розслідування кібернападу на американський сектор інтернету, який зруйнував чимало сайтів, компанія Dyn повідомила, що йдеться про "дуже складну кібератаку". Головний офіс компанії розміщений у США, вона надає послуги в мережі інтернет і працює у сфері розподілу доменних імен.

Фахівці компанії опублікували інформацію попередніх висновків про DDoS-атаку, яка відбулась 21 жовтня 2016 р., що позначилось на роботі її DNS-серверів, на яких містяться субдомени клієнтів компанії. Інформацію про час і характер атаки працівники Dyn розмістили у своєму блозі, а також наголосили, що розслідування триває, проте всі його деталі "не будуть оприлюднені, щоб у майбутньому забезпечити необхідний рівень захисту". До розслідування долучились ФБР і міністерство національної безпеки США.

За даними компанії, усього зафіксовано три етапи кібернападу, останній з яких співробітникам Dyn вдалося пом'якшити, він відчутно не позначився на роботі клієнтських сервісів. Під кібератаку потрапили сервери не тільки на Східному узбережжі США, а також в інших штатах країни.

“На цей момент ми знаємо, що це була дуже складна, вкрай дисперсна атака за участю десятків мільйонів IP-адрес”, – зазначили фахівці Dyn. У цьому випадку злочинці застосовували шкідливу програму Mirai, яка перетворює інфіковані системи в ботнети, тобто в мережі, що їх зловмисники створюють завдяки встановленню вірусних програм на комп’ютерах користувачів. У підсумку були інфіковані прилади, приєднані до інтернету, – від принтерів до роутерів. Через них на сервери компанії Dyn злочинці консолідовано спрямували гігантський трафік, з яким системи компанії впоратись не змогли.

Наслідки DDoS-атаки відчули на собі інтернет-магазин Amazon, мережа мікроблогів Twitter, потокова музична служба Spotify, ігрова мережа PlayStation Network, онлайн-кінотеатр Netflix, американський телекомунікаційний гігант AT&T, електронна платіжна система PayPal, засоби інформації CNN, “The New York Times”, “The Wall Street Journal” та інші відомі інтернет-ресурси.

Опублікований за 2015 р. звіт світового лідера в галузі інформаційних технологій компанії Cisco Systems з інформаційної безпеки містить аналіз інформації про кіберзагрози і тенденції інформаційної безпеки [4]. Звіт також свідчить про життєву необхідність своєчасного виявлення загроз для успішної протидії кібератакам, що їх учиняють професіональні, добре мотивовані зловмисники. Наприклад, експлойт-набір Angler є поширеним видом кіберзагроз, які й надалі створюватимуть проблеми в міру того, як з розвитком цифрової економіки і всеосяжного інтернету зростатимуть нові вектори атаки та можливості монетизації кіберзлочинів зловмисниками.

Зі звіту випливає, що зменшення часу на виявлення шкідливого ПЗ стає щораз важливішим. Це зумовлено, насамперед, новими вразливостями технології Adobe Flash, еволюціонуванням програм-вимагачів і поширенням мутуючого шкідливого ПЗ Dridex. Унаслідок цифровізації бізнесу і розвитку всеосяжного інтернету шкідливе ПЗ і кіберзагрози стають поширенішими й проникають усюди. Наголосимо, що середній в індустрії інформаційної безпеки час виявлення загрози тепер становить 100–200 днів. Для порівняння: середній час виявлення загрози системою Cisco AMP (Advanced Malware Protection) – 46 год.

Результати проведених Cisco досліджень засвідчують важливість впровадження інтегрованих вирішень замість окремих продуктів, роботи з довіреними виробниками і співробітництва з надавачами послуг у галузі інформаційної безпеки. Крім того, деякі експерти в галузі геополітики стверджують, що для підтримки глобального економічного розвитку необхідна відповідна глобальна структура керування безпекою кіберпростору. У цьому звіті Cisco виділяє такі виклики в галузі інформаційної безпеки.

Набір Angler – один з найвишуканіших і найбільше поширених експлойт-наборів. Насамперед, це пов’язано з тим, що він об’єднує новаторські методики, які спільно використовують вразливості Flash, Java, Internet Explorer і Silverlight. Також завдяки застосуванню технології тіньових доменів (до речі, левова частка усієї активності тіньових доменів зв’язана саме із Angler) цей набір виводить методики ухилення від виявлення на новий рівень.

Експлойт-програми, які використовують вразливості Adobe Flash (такі експлойти інтегровані, наприклад, у набори Angler і Nuclear), знову набувають популярності. Це зумовлено як недостатньою автоматизацією процесів керування оновленнями ПЗ, так і тим, що багато користувачів не приділяють достатньої уваги своєчасному оновленню своїх програм.

Згідно з базою даних Common Vulnerabilities and Exposure (CVE), у першій половині 2015 р. зафіксовано на 66 % більше випадків використання вразливостей Adobe Flash Player, ніж за весь 2014 р.

Програми-вимагачі є надзвичайно прибутковою сферою діяльності кіберзлочинців. Саме цим пояснюють постійний розвиток і появу нових варіантів таких програм. Діяльність програм-вимагачів налагоджена до повної автоматизації і відбувається через так званий темний інтернет. Щоби приховати платіжні операції від правоохоронних органів, викуп беруть у так званій крипто-валюті, наприклад, біткоїнах.

Створювачі вірусних компаній Dridex, що часто мутують, демонструють унікальне розуміння того, яких заходів необхідно вживати, щоб уникнути виявлення. Як методи ухилення застосовують постійний запуск нових компаній і часту зміну відправників, адресатів, вкладень, поштових агентів, змісту електронних листів. Через це традиційні антивірусні системи вимушені заново виявляти кожний новий варіант цього вірусу.

Технологічна гонка між зловмисниками і виробниками вирішень для інформаційної безпеки набуває обертів, і така ситуація лише підвищує ризики для організацій та приватних осіб. Виробники повинні виявляти підвищену пильність під час розроблення інтегрованих вирішень для безпеки, покликаних допомогти організаціям реалізувати запобіжні заходи захисту і правильно об’єднати в єдину систему людей, процеси і технології.

Використання окремих, почасти різнорідних вирішень для інформаційної безпеки породжує певні проблеми для організацій. З огляду на це більшої актуальності набуває архітектура комплексного захисту від загроз, який охоплює реалізацію концепції повсюдної безпеки і забезпечує ефективність у будь-якій контрольній точці периметра захисту.

Поки індустрія інформаційної безпеки стикається з проблемами, що пов’язані з фрагментацією, яка зростає, динамічним ландшафтом кіберзагроз і дефіцитом спеціалістів, бізнес повинен вкладати ресурси в ефективні, життєздатні і надійні вирішення та послуги у сфері інформаційної безпеки.

Нові технології для убезпечення від загроз в інформаційному просторі.

На прикладі відомої компанії у сфері інформаційної безпеки та інформаційних технологій Cisco Systems розглянемо новочасні способи захисту від кіберзагроз в інформаційному просторі. Ця компанія на щорічній конференції Cisco Live (відбулася 2015 р. у Сан-Дієго, США) представила нові вирішення, покликані гарантувати безпеку і значно поліпшити можливості моніторингу й контролю на всій розширеній мережі – від центрів опрацювання даних, хмарних інфраструктур і віддалених офісів до кінцевих пристроїв [5].

Як очікують, протягом наступного десятиліття ринок всеосяжного інтернету (Internet of Everything (IoE)) може дати прибуток у 19 трлн дол. США, а можливості, які він створить для надавачів послуг, оцінюють у 1,7 трлн дол. США. Крім того, за прогнозом Cisco, опублікованим у щорічному звіті “Наочний індекс розвитку мережевих технологій” (Cisco® Visual Networking Index, Cisco VNI) за 2015 р., у період 2014–2019 рр. кількість міжмашинних з’єднань і персональних пристроїв, приєднаних до інтернету, зросте з нинішніх 14 млрд до понад 24 млрд. Водночас, однак, зростає активність кіберзлочинців, вони удосконалюють методи та технічну оснащеність. Це

зумовлено тим, що фінансові вигоди, які отримують злочинці, також збільшуються, і нині, за різними оцінками, становлять від 450 млрд до 1 трлн дол. США.

Спростити процеси гарантування інформаційної безпеки в умовах розподілених організацій, удосконалити технології виявлення загроз навіть у найвіддаленіших ділянках обчислювальних інфраструктур – ось чого намагалась досягнути компанія Cisco, розробляючи вирішення для захисту всього простору розширеної мережі. Для поліпшення можливостей моніторингу були впроваджені додаткові сенсори, для підсилення захисту – контрольні точки, для зменшення часу виявлення і часу реагування – система всеосяжного, поліпшеного захисту від загроз. Працюючи разом, ці засоби ефективно протидіють кібератакам. Завдяки технологіям повсюдної безпеки вирішення компанії Cisco забезпечують масштабований захист, що ефективно протидіє широчезному спектру кіберзагроз протягом усього життєвого циклу атаки.

Компанія *Cisco* надає такі оновлення для всього набору мережевих вирішень:

– у тому, що стосується кінцевих пристроїв: за допомогою об'єднаних можливостей вирішень Cisco AnyConnect® і Cisco AMP для кінцевих пристроїв замовники, які використовують Cisco AnyConnect 4.1 VPN Client, тепер можуть легко використовувати і нарощувати можливості неперервного й ретроспективного захисту кінцевих пристроїв з VPN від удосконалених загроз;

– в офісах та філіях: вирішення на базі функцій FirePOWER для маршрутизаторів *Cisco* з інтегрованими сервісами (Cisco® Integrated Services Routers (ISR)) представляють централізовано керовану систему запобігання вторгненням нового покоління (NGIPS) і систему поліпшеного захисту від загроз (Cisco® AMP). Ці вирішення орієнтовані на такі обчислювальні інфраструктури, де не завжди можна застосовувати виділені пристрої для забезпечення безпеки.

Компанія *Cisco* впроваджує численні технології безпеки безпосередньо в мережеву інфраструктуру. Це дає змогу отримати поліпшені можливості моніторингу для швидкої ідентифікації користувачів і пристроїв, які потенційно можуть бути зв'язані з порушеннями нормальних робочих процесів і навіть загрозами для мережі та додатків. Нові можливості охоплюють:

– поліпшене інтегрування між вирішеннями Identity Services Engine (ISE) і Lancope StealthWatch. Тепер співробітники служб безпеки можуть не тільки відзначати окремі IP-адреси, а й ідентифікувати вектори загроз, застосовуючи контекстні дані системи ISE, у тому числі інформацію про те, як користувачі і пристрої отримують доступ і взаємодіють з мережевими ресурсами організації. Ця можливість суттєво поліпшує контекстуальне виявлення загроз, а їхню пришвидшену ідентифікацію забезпечує технологія StealthWatch;

– підтримку NetFlow на платформах Cisco UCS®. Переваги концепції "мережа як сенсор" тепер поширились на фізичні і віртуальні сервери. Це надає замовникам можливості поліпшеного контролю за мережевим трафіком, а також спеціальну аналітичну інформацію про загрози для центрів опрацювання даних;

– завдяки новим вбудованим можливостям із забезпечення повсюдного захисту, обчислювальні мережі Cisco тепер можуть самостійно автоматизувати і застосовувати політики безпеки. Замовники отримали змогу виділити в розширеній мережі підприємства окремі групи додатків і користувачів, задати відповідні політики і визначити, які користувачі мають право працювати з певними додатками і який трафік є допус-

тимим у мережі. Крім того, на базі цих вирішень можуть бути автоматизовані певні функції безпеки;

– інтегрування технологій TrustSec+ISE і StealthWatch. Вирішення StealthWatch тепер може вносити зміни в сегментацію і, отже, блокувати підозрілі мережеві пристрої для швидкої протидії ідентифікованим загрозам. Після цього вирішення ISE може за потреби змінити відповідним способом політики доступу для маршрутизаторів, комутаторів і бездротових LAN-контролерів Cisco, оснащених технологією TrustSec.

Також Cisco анонсувала ще декілька нововведень:

– вирішення Hosted Identity Services (забезпечує надійний, цілодобовий доступний хмарний сервіс для Cisco Identity Service Engine – платформи керування політиками безпеки, яка уніфікує, автоматизує і захищає функції контролю мережевого доступу). Новий сервіс упорядковує роботу з мобільними пристроями організації, забезпечує рольове, контекстно-орієнтоване застосування ідентифікації користувачів і пристроїв, які мають доступ до роботи в мережі. Крім того, завдяки цьому вирішенню пришвидшуються процеси впровадження, що дуже важливо за масштабування бізнесу;

– вирішення pxGrid Ecosystem. Екосистема pxGrid Ecosystem розширилася на одинадцять нових партнерів і об'єднала декілька нових груп технологій, які охоплюють, наприклад, хмарну безпеку й керування продуктивністю мереж і додатків. Вирішення pxGrid – це розроблена компанією Cisco архітектура обміну контекстною інформацією, завдяки якій різні платформи, що гарантують інформаційну безпеку, можуть обмінюватися даними для поліпшення загальної ефективності своєї роботи з виявлення загроз і протидії їм.

З урахуванням потреб надавачів послуг, яким потрібна відкрита, гнучка і програмована інфраструктура, компанія Cisco розширила можливості удосконаленого загрозоорієнтованого захисту, і тепер вони доступні для вирішень *Evolved* Programmable Network (EPN). Платформа Cisco EPN – це надійна основа, яка ґрунтується на відкритій мережевій архітектурі та спроектована для того, щоб використовувати всі переваги технологій програмно-визначених мереж (Software Defined Networking (SDN)) і віртуалізації мережевих функцій (Network Functions Virtualization (NFV)). Вона дає змогу зменшити час окупності, витрати і технічні складнощі, зв'язані із впровадженням нових сервісів.

Нові вирішення компанії Cisco для безпеки надавачів послуг містять такі пропозиції:

– інтегрована платформа Cisco Firepower™ 9300 – це високопродуктивне, масштабоване, модульне, багатофункціональне вирішення операторського класу, спроектоване спеціально для надавачів послуг. Ця платформа може гарантувати безпеку великих потоків даних, необхідних для форсованої роботи сервісів, і повністю відповідає вимогам, які ставлять до обладнання операторського класу;

– розширення можливості поліпшеного оркестрування і хмарних технологій надають змогу легко інтегрувати нові вирішення *Cisco* для інформаційної безпеки з архітектурою Cisco зі сторонніми SDN/NFV вирішеннями, а також з Cisco's Adaptive Security Appliance Virtual (ASAv), Cisco's Network Service Orchestrator (NSO) і Application-Centric Infrastructure (ACI). Ці можливості оркестрування і хмарних технологій також охоплюють інтерфейси API для інтегрування з системами підтримки бізнесу

(Operation Support Systems/ Business Support Systems), а також хмарними вирішеннями типу “безпека як послуга”;

– удосконалені можливості – наприклад, захищені контейнери забезпечують розміщення сервісів безпеки і додатків, які планують у перспективі.

Руткіти, методи боротьби з ними.

У сучасному світі, як відомо, ІТ-технології використовують практично всюди для автоматизації завдань, які повторюються, починаючи з купівлі товарів в інтернеті та закінчуючи зніманням грошових засобів з рахунку, спрощуючи таким способом наше життя. Поряд з перевагами ці системи мають і низку проблем. Практично кожен користувач персонального комп’ютера знає про шкоду вірусів. Навіть люди, які недостатньо ознайомлені з принципами роботи комп’ютерів, знають про те, що їхні дані можуть зазнати пошкодження, видалення чи крадіжки, тому необхідно створювати резервні копії.

Хоча й існує велика кількість антивірусних програм, є інша, небезпечніша за природою категорія шкідливого програмного забезпечення, яке називають руткітами (англ. *rootkit*) [6]. Шкідливе ПЗ може працювати як додаток у користувацькому просторі чи як частина операційної системи. Руткіти найчастіше зачисляють до другої категорії, що надає їм більше можливостей, робить їх небезпечнішими і максимально утруднює їхній пошук та нейтралізацію. Невідома особа, яка отримала контроль над вашою системою, яка працює з нею найчастіше одночасно з вами, може завдати шкоду й отримати доступ до вашої особистої інформації. Програми для запису подій клавіатури дають змогу вкрасти паролі, номери кредитних карток, персональні дані, дані про фінансові операції з таблиць, конфіденційні дані, які належать до діяльності компанії тощо.

Руткіти є невеликими наборами інструментів, утиліт і сценаріїв. Головна мета їхнього розміщення в системі – отримання прав адміністратора, тому систему можуть використовувати або віддалено для збирання секретних даних, або для проведення атак щодо інших систем, розміщення руткіта й отримання доступу до них.

Звичайно руткіт містить у складі набір мережевих сніферів, інструментів для дослідження журналу, сценаріїв для чищення системного журналу, системних утиліт для визначення IP-адрес, аналога утиліти netstat, утиліт для зупинки процесів, які виконуються, сценаріїв для приховання коду і своєї стиснутої копії для реплікації.

Коротко розглянемо відмінні ознаки вірусів і руткітів (див. таблицю). Як бачимо, деякі риси вірусів/троянів і руткітів подібні (загалом і ті, й інші можуть або спричинити втрату даних, або захоплювати і збирати конфіденційні дані, такі як імена користувачів, паролі, адреси електронної пошти тощо), проте є і принципові відмінності між ними. Хоча вірус звичайно і працює у “невидимому режимі”, приховуючи свою наявність інфікуванням виконуваних і системних файлів, він, зазвичай, працює як додаток, тому антивірусні програми здатні виявити і видалити його. Троян, який є удосконаленим вірусом, приховується в системі складнішим способом.

Руткіт, з іншого боку, заміняє собою частину операційної системи для приховання й отримання максимально можливого контролю над системою. Тому він має змогу провадити моніторинг процесів, які відбуваються в системі, поряд з виконанням будь-яких дій. Його також можна використовувати для розміщення інших руткітів та вірусів у системі. Руткіти дають змогу віддалено керувати комп’ютером, звичайно також використовуючи його як поширювача комерційного спаму.

Характерні ознаки вірусів та руткітів

Вірус	*Руткіт*
Найчастіше виконується як користувацький процес. Звичайно отримує доступ до системи з правами користувача	Найчастіше виконується як частина ОС/ядра. Отримує доступ до системи з правами адміністратора/користувача *root*
Не відкриває шляхів для віддаленого адміністрування	Відкриває шляхи для віддаленого адміністрування – *viz*., порт, *IP* тощо
Не надає можливостей для віддаленого доступу	Надає можливість віддаленого доступу для зломника
Досить легко виявити і видалити з системи	Дуже складно виявити і видалити із системи
Призначений для руйнування роботи системи і пошкодження даних	Призначений для крадіжки конфіденційних даних

Інфікування/встановлення. Руткіти використовують методи, які аналогічні до застосовуваних вірусами для проникнення в систему; оскільки ж для руткітів необхідні привілеї рівня ОС, то методи їхнього розміщення незначно відрізняються.

Якщо зломник має фізичний доступ до системи, то він може спробувати підібрати нескладний пароль. Якщо є змога завантажити систему з твердого носія, який належить хакеру (CD, USB), він може спробувати застосувати різноманітні техніки для отримання пароля користувача root з системи, яка встановлена на жорсткому диску.

Хакер може віддалено визначити вразливість ОС і мережевих додатків, не оновлених вчасно, після чого атакувати їх. Він також може використовувати веб-сторінку із вбудованим сценарієм для проникнення в систему через браузер.

Багато додатків, які шпигують за користувачем (spyware), можна використовувати як надійні засоби встановлення руткітів у систему.

Дуже часто руткіт упакований у вигляді файла архіву, що сам розпаковується, дані з якого витягаються відразу ж після потрапляння в систему. Зазвичай невеликий набір програм для встановлення, які стежать за роботою руткіта та які отримують права адміністратора і приховують свою наявність у системі, перебувають також у стиснутому стані.

Деякі особливо складні руткіти мають можливість визначення антивірусного та антишпигунського програмного забезпечення та зміни принципу його роботи разом із модифікацією виведення для приховування своєї наявності в системі. Наприклад, деякі руткіти копіюють набір своїх інструментів у корінь файлової системи, проте їх неможливо виявити за допомогою виведення списку файлів, оскільки руткіт змінює поведінку відповідних системних команд.

Оскільки зломники постійно намагаються оптимізувати розмір коду руткітів, то для їхнього встановлення й активації потрібний дуже малий проміжок часу. Руткіти призначені для максимального поширення, тому практично всі вони містять свою копію. У процесі роботи вони використовують усі можливі механізми для дослідження локальної мережі і пошуку інших вразливих систем.

Якщо в ході проектування локальної мережі аспект безпеки недостатньо пропрацьовано, то отримання руткітом адміністративних привілеїв на одному з вузлів цілком достатньо для його поширення на інші системи в мережі. Сучасні руткіти здатні визначати наявність з’єднання з інтернетом, отримувати останню версію руткіта і копіювати її на всі інфіковані машини, а далі намагатися знайти в інтернеті інші вразливі чи недостатньо добре налаштовані системи.

Виявлення. Як уже зазначено, виявлення руткіта є справді складним завданням, яке потребує від адміністраторів додаткових дій порівняно з аналогічним завданням для вірусів і троянів. Хоча деякі руткіти і блокують за допомогою найновіших антивірусних інструментів, більшість руткітів невразливі для них. Оскільки руткіт стає частиною операційної системи, елементарні методи завантаження системи з диска чи USB-носія для відновлення системи дуже корисні для завантаження свіжої неінфікованої версії операційної системи і використання інструментів для виявлення руткітів без протидії з їхнього боку. Крім того, багато інструментів для виявлення руткітів тільки визначають їхню наявність, однак не можуть їх видалити, тому необхідне ручне втручання для очищення системи.

Інструменти для виявлення руткітів повинні використовувати нові методи замість простих перевірок файлів чи процесів, оскільки руткіт у процесі роботи може вплинути на ці застарілі методи і алгоритми. Ліпшим варіантом є фіксування зображення системи в різні моменти її роботи та порівняння із зображенням, отриманим програмою відразу після встановлення системи.

Нові інструменти використовують інтелектуальні алгоритми для виявлення змін у стані системи, тому не потребують дослідження системи в початковому стані. Існують різні алгоритми виявлення руткітів, такі як метод на основі сигнатур, який застосовують для виявлення вірусів, чи метод на основі встановлення недоторканості, за якого файли, процеси і модулі ядра перевіряють на бінарну незмінність. Є інший ефективний метод, коли за допомогою програми знімають дамп пам'яті, який досліджують надалі для пошуку аномалій, сигнатур чи змін, прямо чи дотично зв'язаних із функціонуванням руткітів.

Існує багато комерційних і вільних програм для виявлення руткітів. Розглянемо декілька популярних інструментів.

Компанії McAfee і Symantec пропонують продукти, які дають змогу захиститися від розміщення руткітів і виявити деякі з них. Однак для виявлення руткітів потрібні окремі спеціалізовані інструменти.

У світі вільних програм відомим інструментом, який має перевагу над більшістю інших, є chkrootkit. Він дає змогу проводити детальні бінарні перевірки, перевірки модифікацій файлів і дослідження модулів ядра. Програма відмінно працює в широкому спектрі дистрибутивів Linux і є необхідним інструментом у наборі адміністратора.

Аналогічно, Tripwire є важливим інструментом з відкритим вихідним кодом, який дає змогу проводити вичерпні перевірки MD5-хешей і виявляти аномалії, такі як відкриті з'єднання для віддаленого керування і локальні експлойти.

Також Rootkit Hunter – ще один відомий інструмент з продуманим сценарієм, здатний виявляти багато руткітів. Він також може виявляти некоректні права доступу до файлів і модулів ядра, надаючи можливість проведення щоденних перевірок. За появи нового руткіта досвідчений системний адміністратор може вивчити його і розробити сценарій для його виявлення.

Важливо, що створювачі шкідливого ПЗ звичайно також вивчають ці механізми і вносять необхідні модифікації в нові версії своїх руткітів для запобігання їхньому виявленню за допомогою спеціалізованих інструментів.

Аналогічно до вірусів, на жаль, існує багато руткітів і для Windows, і для комерційних дистрибутивів Linux. Оскільки ядро довгий час не зазнавало кардинальних змін, то для зломників звичайно не було складно розробити руткіти, які поширюватимуться.

Як зазначено вище раніше, руткіти надають можливість доступу до системи відкриванням портів, створенням процесів рівня ядра, що дає змогу злодію повністю віддалено контролювати систему, навіть через інтернет.

Є декілька по-дружньому налаштованих руткітів, які співпрацюють один з одним. Якщо руткіт під час впровадження в систему виявляє у ній наявний руткіт, він оновлює його для поліпшення роботи. Відомо декілька руткітів, які працюють як шлюзи для розміщення вірусів і троянів у локальній мережі; спочатку у систему впроваджується руткіт, резервує місце, виявляє привілеї користувача, отримує контроль над файловою системою, відключає антивірусні програми, відкриває доступ для відправлення вірусів і переходить у невидимий режим роботи.

Нове покоління руткітів відоме діями за встановленням фальшивих SSL-сертифікатів і спробами розшифровування HTTP-трафіка для отримання інформації про кредитні картки, яка звичайно передається зашифрованим каналом. Існують руткіти, які компрометують систему проведенням за їхньою допомогою атак перехоплення за участю людини щодо інших систем, що утруднює розслідування з пошуку реального зломника.

Висновки.

Отже, наявні засоби глобального керування кіберпростором не в стані контролювати проблеми ландшафту загроз, який постійно ускладнюється, і геополітичні виклики. Основна проблема зумовлена тим, що державні органи збирають дані про громадян і організації та розподіляють ці дані між різними підвідомчими сферами. Проте міжнародні відносини мають обмежений характер, і це стає суттєвою перешкодою у створенні єдиної сфери контролю за глобальним кіберпростором. Сумісна структура керування безпекою кіберпростору, яка охоплює інтереси багатьох зацікавлених сторін, – ось що необхідно для розвитку бізнес-інновацій і зростання світової економіки.

Відповідальний виконавчий директор компанії Stroz Friedberg Сет Берман зазначив: “Неможливо повністю знищити кіберзлочини, але можна суттєво знизити ризик нападу з боку хакерів. Якщо обмежити “рух” зловмисників по мережі, у компаній буде більше часу для того, щоб застосувати заходи у відповідь” [2].

Як приклад, надані компанією Cisco вирішення для безпеки надавачів послуг розроблені із застосуванням унікального підходу, орієнтованого на професійні вимоги надавачів послуг. Ці вирішення формують спеціальну загрозоорієнтовану систему захисту, яка динамічно гарантує безпеку робочих процесів із їхньою появою, а також гнучко розподіляється на фізичні, віртуальні та хмарні інфраструктури.

Розробка системи безпеки інфраструктури, яка постійно вдосконалюється, також необхідна для зупинки поширення і запобігання шкоди, спричинюваної таким шкідливим програмним забезпеченням, як руткіти. Сучасні системи виявлення проникнення (IDS) часто можуть зупиняти поширення руткітів уже на підході до мереж.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. В 2015 году по всему миру хакеры нанесли ущерб в 158 млрд долларов // Компьютеры, сети, программирование. – 2016. – № 4. – С. 6.

2. Кибербезопасность 2015 года // Компьютеры, сети, программирование. – 2016. – № 7. – С. 2–4.
3. *Левків Я.* Масована кібератака РФ на США [Електронний ресурс]. – Режим доступу : www.galinfo.com.ua.
4. Усложняющиеся кибератаки // Компьютеры, сети, программирование. – 2015. – № 8. – С. 7–9.
5. Технологии, обеспечивающие повсеместную безопасность // Компьютеры, сети, программирование. – 2015. – № 8. – С. 5–7.
6. Вирусы и руткиты // Компьютеры, сети, программирование. – 2014. – № 4. – С. 15–18.

Стаття: надійшла до редакції 09.01.2017,
доопрацьована 16.01.2017,
прийнята до друку 18.01.2017.

ACTUAL INFORMATION SECURITY ISSUES AND SOLUTIONS

Yu. Korchak, Yu. Furgala

Ivan Franko National University of Lviv,
107 Tarnavsky St., UA–79017 Lviv, Ukraine
yurakorchak@yahoo.co.uk

The paper analyzes the current state of the global information security, describes the new cyber threats, trends and methods to combat them. Integrating ubiquitous security technology will enable customers and service providers to take advantage focused on threat protection, since this type of protection most relevant to counter today's dynamic threat landscape. Only for the widespread introduction of protection possible without unnecessary risk to use the opportunities offered by the digital economy and Internet of Everything. The authors also drew attention to a malware like rootkits, which are much more dangerous than viruses.

Key words: information security, cyber attacks, network infrastructure, hacker, virus, rootkit.