Основні види «вірусів»

Розглянемо більше детально основні види шкідливого програмного забезпечення.

Троянська програма – це програма, яка має приховані функції. Така назва виникла тому що перші програми цього типу потрапляли на комп'ютери під виглядом корисних програм, які користувачі завантажували і запускали власноруч. Зараз такий варіант розповсюдження також присутній, часто користувачі самі запускають подібні програми, намагаючись завантажити зламані неліцензійні версії програмного забезпечення чи програми для генерації зламаних серійних ключів. Як наслідок, під видом кейгенів та кряків троянські програми досить часто потрапляють на комп'ютери, ласих до використання неліцензійного програмного забезпечення, користувачів.

Хробак – це програма, яка розмножується, від одного комп'ютера до іншого. Механізми можуть бути дуже різними: електронна пошта, локальна мережа чи USB-накопичувач. Так, хробак може скопіювати свої файли на флешку та створити відповідний файл автозавантаження і як тільки ви під'єднаєте флешку до комп'ютера, на ньому одразу ж активізується хробак. При цьому слід зазначити, що хробаки що розповсюджуються через пошту чи через флешки, практично ні в чому не відрізняються, вони лише використовують різні шляхи поширення.

Бекдор – програма «чорний хід», зазвичай шкідливі програми цього типу дають зловмиснику віддалений доступ та можливість керування комп'ютером користувача. Методи їх дії бувають різними, наприклад така програма може відкрити мережевий порт, за допомогою якого зловмисник отримає повний доступ до ураженого комп'ютера: зможе надсилати різні команди, запускати інші програми.

Дропер – це по суті інсталятор троянської програми. Для чого їх створили? Оскільки троянська програма це багатокомпонентний елемент, який потребує щоб в системі були встановлені певні драйвери та інші компоненти, то цю задачу виконує дропер. Після того як дропер було активовано в системі, він встановлює всі частини троянської програми та активує її.

Завантажувальник – це по-суті троянська програма, мета якої – завантажити з мережі Інтернет іншу троянську програму. Здавалося б, чим завантажувальники відрізняються від троянських програм? Певні відмінності є. Зокрема, характерна риса таких програм – вони дуже маленького розміру (кілька десятків кілобайт), а отже можуть завантажитись і активізуватись дуже швидко. І вже після вкорінення в системі, даунлоадер завантажує основну троянську програму. При цьому може бути завантажений, як дропер, так і окремі компоненти троянця, які будуть методично інсталюватись на комп'ютер. Отже, якщо у вас на комп'ютері був знайдений завантажувальник, то варто шукати і інші троянські програми.

Діалери – це програми-дзвонилки, вони були дуже популярні, у часи активного використання модемів і телефонних ліній. Тоді був дуже хороший бізнес з використанням платних номерів, після дзвінків на які з рахунку користувачів знімались кошти. І якщо, наприклад, комп'ютер на території України був заражений такою програмою, то він власноручно телефонував на номери, наприклад, в США чи Бразилії. Сучасні модифікації діалерів використовують дещо інші механізми, зокрема, це можуть бути дзвінки через Skype, відкриття певних спеціалізованих сайтів.

Руткіт – це спеціальний вид троянських програм, головна мета якого – максимально глибоко інсталюватись у систему, щоб його було якомога важче знайти і видалити. Як правило, руткіти містять драйвери операційних систем і працюють на досить низькому рівні. Руткіти використовуються для маскування всіх інших компонентів троянця від детектування. Тобто руткіт у системі призваний приховати роботу інших компонентів трояна. Головна проблема в тому, що руткіти дуже важко знайти і ще важче видалити з системи. Далеко не кожна антивірусна програма може з цим впоратись.

Рекламний модуль – адваре програми, мабуть найменш небезпечні з усіх шкідливих програм, але через дуже широку розповсюдженість і просто величезну зухвалість їх авторів в останній час вони стали досить неприємними. Як можна здогадатись із назви цього типу шкідників, задача рекламного модуля – показати вам рекламу. Це може відбуватись у різних проявах, наприклад у вас можуть самостійно відкриватись певні сторінки у браузері, які ви не відкривали – це будуть сайти з дивною рекламою або просто сайти, які ви не збирались відвідувати. Тобто зловмисники таким чином підвищують відвідуваність певного сайту або провокують Вас подивитись певну інформацію. Також рекламні модулі можуть показувати різні банери чи навіть вставляти банери на той сайт, де їх не було, або ж підмінювати рекламні повідомлення на сайтах. Наприклад якщо ви шукаєте певну інформацію у гугл, то видача пошукового запиту містить 2 категорії – безкоштовні пошукові запити та рекламні повідомлення, так рекламні модулі можуть підміняти одні рекламні повідомлення на інші і в результаті ви будете бачити не ту інформацію яку запитували, а те, що хоче вам показати власник рекламного модуля. Даний механізм підміни пошукових видач отримав назву «чорного SEO».

<u>Які ж основні джерела зараження ПК та мобільних пристроїв?</u>

По суті, якщо говорити загалом, найголовнішим джерелом вірусів буде той канал, який забезпечує для нас максимальний обмін інформацією Вашого ПК з іншими. Тож, без сумніву, головним джерелом зараження є глобальна мережа Інтернет.

На жаль віруси існують практично для всіх каналів зв'язку і зловмисники охоче використовують ті, якими більш активно користуємось ми. Зараз найбільше користувачі використовують веб-сайти та електронну пошту. Існують віруси, які розповсюджуються через Skype, icq інші месенджери. У свій час існували популярні віруси для RRS клієнтів, однак вони використовуються не так широко. А от браузерами для відвідування сайтів користуються всі без виключення і як наслідок це джерело є найбільш популярним.

Другим по популярності джерелом зараження є електронна пошта. На початку 2000них років практично всі загрози шли саме з електронної пошти. Зараз об'єм заражень через е-мейли не на стільки високий, однак все ж зустрічаються масові розсилки, в яких користувачі отримують листи, які маскуються під звичайну пошту від знайомих чи колег. І наприклад якщо вірус заразив комп'ютер Вашого знайомого і від нього пише вам листа, то вірогідність того що ви відкриєте цього листа дуже висока. Часто відбуваються масові СПАМ-розсилки, які маскують під повідомлення від банків, і взагалі під певну корисну інформацію: фото, архіви, які Вам пропонують подивитись. Звичайно ж після відкриття такого файлу нічого корисного для вас крім зараження Вашого ПК не відбудеться.

Третім за популярністю способом зараження ПК є змінні накопичувачі, перш за все це флеш диски та USB-накопичувачі. Згадаймо, що перші комп'ютерні віруси взагалі почали свою історію саме з змінних накопичувачів, тільки тоді це були дискети – гнучкі магнітні диски. Як інколи зазначається, історія розвивається по спіралі і сьогодні, як і 30 років тому ми переносимо один одному віруси трояни та хробаки через флеш-накопичувачі. Різниця лише у тому, що старі віруси не завжди могли запускатись автоматично і чекали коли

користувачі самі запустять певну програму з диску, сучасні ж віруси можуть запускатись автоматично одразу після підключення флешки до комп'ютера.

Історія комп'ютерних вірусів в Україні

Поговоримо про історію комп'ютерних вірусів в Україні.

Якщо говорити про перші комп'ютерні віруси на території України, то потрібно згадати часи, коли ще у Радянському Союзі з'явились перші IBM-PCсумісні комп'ютери. Можливо існували індивідуальні розробки шкідливих програми і для більш ранніх електронно-обчислювальних машин, які існували в СРСР, однак про них нам достеменно не відомо, оскільки вони не були поширеними і не зустрічались у дикому вигляді, тобто на комп'ютерах реальних користувачів. Якщо ці програми і були, то лише на рівні наукових розробок. Серйозні ж віруси з'явились у СРСР, у тому числі і на території України, у 1988 році. Коли IBM-PC сумісні комп'ютери масово хлинули на радянський ринок, а також почали створюватись їх радянські аналоги, наприклад ЄС-1840 ІСКРА-1030 і НЕЙРОН, тим не менше на цих системах вже були віруси, які у той час були досить простими. Їх задача була в тому щоб просто розмножуватись, робили вони це за допомогою дискет, які використовували користувачі для обміну документами, програмами чи іграми.

Взагалі перший комп'ютерний вірус, який з'явився у Радянській Україні і взагалі у СРСР було детектовано у серпні 1988 року. Він називався С-648. У той час існувала єдина класифікація вірусів і віруси категорії С – заражали *.com файли. Це особливий формат виконувальних файлів MS-DOS, а 648 – це розмір вірусу 648 байт. Як правило при заражені файлу, віруси збільшували його довжину на свій розмір. Часто вірусам давали унікальні назви, так цей вірус називали Venna (Відень), або Віденський вірус, через орієнтовне місце його розробки. Далі з'явились інші віруси, одним із найбільш активних був RS-1701, у цього вірусу був дуже цікавий ефект – опадання букв на екрані монітора. І той і інший вірус були створені у Європі, а дуже багато вірусів у той час створювалось у Болгарії. У 1988-1989 роках почали розроблятись і перші засоби боротьби з вірусами, різноманітні програми по типу Вірус Д1, СЄРУМ та інші, які не мали системного характеру , вони боролись лише з конкретними вірусами, однак оскільки їх було не дуже багато, то такий спосіб був досить ефективним. Тобто в середньому антивірусна програма тих часів містила у собі антивірусні бази для детектування 30-100 вірусів. Більш просунуті могли виявити 300 вірусів, тобто рахунок йшов на одиниці, десятки чи сотні, однак аж ніяк не сотні тисяч чи мільйони загроз як зараз.

Важливо відмітити цікаву особливість: у радянському союзі зростало багато цікавих до всього нового людей, які дуже любили створювати щось нове і знаходити практичне застосування свої навичок. А оскільки ІТ-галузь у радянському союзі була розвинута дуже слабко, то навички програмування було ніде застосувати і самореалізуватися такі молоді люди можливості не мали. Саме тому з'явилась дуже велика і потужна радянська школа створення вірусів, і мабуть, більша частина якої була присутня в Україні, зокрема у Києві та Харкові. Було створено дуже багато технологічно нових вірусів з новими можливостями. Так, на початку 90-х років двадцятого сторіччя хакери з території СНГ писали чи не найбільше вірусних загроз у світі.

Зараз, на жаль, Україна являє собою у певному сенсі «Дикий Захід», де дуже багато чого можна зробити і дуже невелика вірогідність покарання за вчинені злодіяння. Завдяки цьому в Україні створюється дуже багато шкідливого ПЗ. Наші хакери прославляють Україну у всьому світі в негативному сенсі, ми часто на слуху, велика кількість шкідливого ПЗ створюється або ж управляється з України. Як правило, такі атаки проводяться

кібер-угрупованнями на громадян і компанії за межами України, але інколи орієнтовані і на користувачів у нашій країні.

Ситуація із розповсюдженням загроз у нашій країні є дуже сумною. І це пов'язано із певною низкою причин. По перше, щоб ефективно захищатись від шкідливого ПЗ потрібно користуватись різними засобами інформаційної безпеки: оновленими версіями програмного забезпечення, ліцензійним ПЗ, яке поступає із довірених джерел, напряму від розробників. У нас в країні з цим досить складно, практично відсутня культура використання ліцензійного ПЗ, фактично на дуже великій кількості ПК встановлені піратські операційні системи, зокрема Windows XP, яка не оновлюється, а значить не усуваються вразливості в самій операційній системі, що дозволяє вірусам дуже легко самостійно потрапляти на комп'ютери і довго залишатись непоміченими. Нездатність населення купувати дороге антивірусне ПЗ чи інші програми для інформаційного захисту призводить до того, що багато комп'ютерів виявляються просто не захищеними.

По статистиці антивірусної лабораторії Zillya! близько 25-35% комп'ютерів в Україні заражені вірусами, тобто мова йде не просто про комп'ютери які стикалися з вірусами, на які шкідливе ПЗ намагалось проникнути, а саме про зараженість.

Які саме види загроз найчастіше загрожують українцям?

За масовістю – найбільш розповсюдженими є рекламні модулі. Для цього типу шкідливого ПЗ дуже важко провести межу між шкідливим і безпечним програмним забезпеченням. Різноманітні тул бари, програми, які проникають в браузери і збирають статистику про вас, підмінюють результати пошукових видач, показують додаткову рекламу. Найчастіше вони заявляють, що є легальними програмами і створені для: прискорення роботи ПК, Інтернету, збереження паролей чи блокування реклами і багато інших видів діяльності. У зв'язку з цим не має однозначного трактування антивірусними компаніями чи є програма шкідливою чи ні. І якщо ви спробуєте перевірити подібну програму за допомогою багатоядерного он-лайн сканеру, наприклад VirusTotal, до якого зараз підключено 57 різних антивірусів, то переконаєтесь що з 57 – тільки 20 скажуть, що програма є рекламним модулем, інші 37 промовчать – показуючи, що програма нешкідлива. Чи це означає, що погано спрацювали лабораторії 37-ми вендорів, які не додали програму в бази, чи інші 20 вендорів помилились і у них відбулось хибне спрацювання. Насправді, тут мова йде про політику детектування. Про ту вузьку грань поганого і хорошого, яка встановлюється розробниками антивірусів.

На другому місці за популярністю є троянські програмі, які направлені на крадіжку інформації, вимагання грошей з користувачів. Найпопулярнішими є програмі які крадуть доступи до електронних гаманців чи кредитних карт, при чому дані можуть красти як у домашніх користувачів, так і у організацій, коли крадуться доступи до клієнт банків і одразу ці гроші переводяться на підставні рахунки.

На початку 2015 року небувалої активності набули програми-криптувальники, які шифрують дані і вимагають викуп для розблокування. А ще два роки тому популярними були блокувальними комп'ютерів, які лише блокували і могли досить легко бути нейтралізовані. На жаль для шифрувальників використовують криптостійкі алгоритми і гарантувати розшифрування ніхто не може.

Варто згадати що досить значно поширеними все ще є файлові віруси, за останній рік найпоширенішим був virus.sality, який інфікує багато файлів на комп'ютері і здатен переміщуватись через USB-накопичувачі і достатньо хитро протидіяти виявленню його в

системі. Хочу ще раз нагадати, що від файлових вірусів систему можна вилікувати, а троянські програми чи рекламні модулі потрібно просто видаляти з комп'ютеру.

Кібершпигунство

Окремою історією з комп'ютерними вірусами є кібершпигунство. Електронно-обчислювальні системи використовуються не тільки домашніми користувачами, але й бізнесом та органами влади, при цьому у них використовуються такі ж самі IBM-PC сумісні комп'ютери в основному з операційною системою Windows і схожим програмним забезпеченням. Нажаль, більшість комп'ютерів у державних органах також можуть бути атаковані загрозами для домашніх користувачів. У зв'язку з цим ми спостерігаємо багато заражень і втрат саме конфіденційної державної інформації, а інколи навіть секретної. Троянські програми, які проникають в державні органи можуть не тільки красти інформацію, але й проводи різноманітні диверсії. Так у світовій практиці відомі випадки заражень важливих стратегічних об'єктів, які були виведені з ладу чи була змінена їх робота.

Наприклад, дуже гучний скандал відбувся у 2010 році. Це зараження троянською програмою секретного режимного об'єкту. Мова йде про зараження комп'ютера на заводі по збагаченню ураном в Натанзі, Іран. Дана троянська програма впливала на обладнання і перепрограмувала контролери компанії Siemens, які управляли центрифугами реактору для збагачення урану. Вони змінювали швидкість руху центрифуг і порушували сам процес ядерного синтезу. Троянська програма мала дуже багато сучасних новацій та розробок і змогла проіснувати непомітною декілька місяців і в результаті порушила процес збагачення. Використаний за цей проміжок часу уран було просто зіпсовано. Це була дуже серйозна атака на ядерну програму Ірану і, по даним експертів, ядерна програма країни була відкинута назад на декілька років.

В Україні подібний інцидент відбувся у травні 2014 року під час президентських виборів Ряд серверів ЦВК, були заражені троянськими програмами, які змінювали роботу системи і створювали набори файлів, які модифікували вигляд офіційної сторінки результатів виборів, чим намагались спровокувати політичний конфлікт чи поставити під сумнів реальні результати виборів. Зараження систем відбулось по класичній схемі троянізації, ніяких суперскладних програм не використовували. Просто відбулось зараження певних комп'ютерів, потім шкідливе ПЗ перейшло на інші комп'ютери на яких відбувалась постановка троянських задач в середині операційної системи. На одному з серверів у планувальник була поставлена задача створити на диску два файли з конкретним вмістом, що мало призвести до модифікації офіційного сайту.

Хто проводить кібератаки?

Громадськість завжди цікавить запитання хто написав програму? Хто стоїть за кібератакою? І т.д.

На жаль у кіберсвіті існує дуже багато анонімності. По певних деталях в коді вірусу, характеристиками в виконуваних фалах, як правило, можна зробити певні висновки, на якій мові розмовляють хакери, що пишуть код, яких стиль чи методи програмування використовувався. Можливо створена програма схожа на ту, яку виявили раніше, а вже про попередню відомо хто і де її створив. Теоретично якщо правильно налаштовано мережеве обладнання можна запротоколювати джерело атаки на систему, однак на практиці виявити це не завжди є можливим. І тому не дивно що не вдалося одразу виявити винних у атаці на ЦВК.

То ж, сподіваюсь, зараз слова мережевий хробак чи троянська програма не є для вас чимось дивним і не зрозумілим. Ви знаєте класичні загрози і розумієте звідки можна очікувати їх атаку. У наступній лекції ми поговоримо про те, як змінились загрози інформаційної безпеки у сьогоденні та розглянемо одну з найголовніших загроз інформаційної безпеки - соціальну інженерію!