ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА ЇХ ВИКОРИСТАННЯ

Ірина Краснокутська
Сумський державний педагогічний університет імені А.С. Макаренка, м. Суми
val42227@yandex.ru
Науковий керівник – Н.В. Шамшина

ПРО КОМП'ЮТЕРНІ ВІРУСІ ДЛЯ МОБІЛЬНИХ ПРИСТРОЇВ ТА ЗАХИСТ ВІД НИХ

Безпека мобільних пристроїв на сьогодні, чи не одна з найактуальніших проблем всього людства. Адже всього за пару років, комп'ютерними вірусами були заражені близько мільйону мобільних пристроїв.

Комп'ютерні віруси взагалі – це вид шкідливого програмного забезпечення, здатний створювати копії самого себе і впроваджуючи цей код до інших програм, у системні області пам'яті, завантажувальні сектори, а також поширювати свої копії по різноманітних каналах зв'язку, з метою порушення роботи програмно-апаратних комплексів, видалення файлів, приведення в непридатність структур розміщення даних, блокування роботи користувачів або ж приведення в непрацездатність апаратних комплексів комп'ютера [6]. Якщо раніше комп'ютерні віруси дошкуляли користувачам персональних комп'ютерів, які були підключені до мережі, то зараз ця проблема торкнулася користувачів мобільних пристроїв, таких як планшети, смартфоні, мобільні телефони. Здебільшого ці віруси нагадують своїх прародичів, але існують и деякі відмінності. Головне при цьому «знати ворога в обличчя», та знати шляхи його розповсюдження, дотримуватися основних правил безпеки при користуванні мобільними пристроями.

Мобільні віруси – це невеликі програми, призначені для втручання в роботу мобільного телефону, смартфона, комунікатора, які записують, пошкоджують або видаляють дані і поширюються на інші пристрої через SMS та Інтернет [5].

Вперше про мобільні віруси заговорили ще в 2000 році. Вірусами назвати їх було важко, так як це був набір команд, виконуваний телефоном, який передавався через SMS. Такі повідомлення забивали відповідні комірки пам'яті і при видаленні блокували роботу телефону. Найбільшого поширення набули команди для таких телефонів, як Siemens і Nokia [1].

По справжньому, перший мобільний вірус був виявлений лише 14 червня 2004 року Першим мобільним вірусом став мережевий черв'як "Cabir", що має функції поширення по стільникових мережах і зараження мобільних телефонів під управлінням операційної системи Symbian OS. Алгоритм дії цього вірусу наступний: "Cabir" доставляється на телефон у вигляді файлу формату SIS (дистрибутив операційної системи Symbian), маскуючись під утиліту для захисту телефону Caribe Security Manager. При запуску зараженого файлу черв'як виводить на екран напис "Caribe", впроваджується в систему і активізується при кожному завантаженні телефону. Після цього "Cabir" сканує доступні пристрої, що використовують технологію передачі даних Bluetooth, вибирає перший з них і пересилає йому свою копію. Черв'як був створений спеціально для роботи в Symbian OS для мобільних телефонів Nokia [2].

За різними підрахунками, на поточний момент відомо близько 500 мобільних вірусів. Називаються й інші цифри: кілька тисяч. Різночитання в кількості і назвах мобільних вірусів визначаються різними підходами до класифікації у різних антивірусних компаній. Незважаючи на велику кількість мобільних вірусів дійсно небезпечних серед них поки що небагато, як вважають деякі фахівці [4]. Сучасна тенденція є такою, що: чим більш функціональний телефон Ви маєте, тим до більшій кількості погроз він схильний.

Основні види мобільних вірусів:

• черв'яки, що поширюються через специфічні протоколи та сервіси;

• трояни-вандали, що використовують помилки ОС для установки в систему;

• трояни, орієнтовані на нанесення фінансового збитку користувачеві.

Найбільш небезпечні хробаки або черв'яки. Черв'яки – це віруси, які розповсюджуються самі, вони здатні викликати дуже швидке зараження великої кількості систем, порушивши працездатність мобільної мережі або перетворивши її в підконтрольну зловмисникові розподілену мережу («зомбі» -мережу).

Основною метою мобільних вірусів, як і у випадку з комп'ютерними вірусами, є отримання персональної інформації, яку можна продати або використати в особистих потребах. До такої інформації можуть відноситися особисті дані власника телефону, дані самого пристрою, приватні повідомлення, іноді номери кредитних карт.

Основними функціями комп’ютерного вірусу є:

1) Знищення інформації;
2) Крадіжка особистих даних;
3) Цілеспрямована модифікація коду програми, що цікавить порушника [3].

Крадіжка персональної інформації. В даному випадку віруси збирають різні відомості, наявні в телефоні, наприклад, контакти власника телефону, паролі від програм, параметри облікових записів, таких, як Google Play або AppStore. Вся інформація, отримана вірусом, відправляється на сервер зловмисників, де використовується на їх розсуд. Один з найсерйозніших вірусів такого плану – Android.Geinimi. Потрапляючи в систему, він визначає місцеположення смартфона, завантажує файли з Інтернету, зчитує і записує закладки браузера, отримує доступ до контактів, здійснює дзвінки, відправляє, читає і редагує SMS-повідомлення.

Відправка платних SMS-повідомлень, дзвінки на «партнерський номер» без відома власника. В даному випадку за відправку повідомлення або за дзвінок списується серйозна сума коштів з особового рахунку власника телефону. Зрозуміло, гроші потрапляють до рук зловмисників. З найвідоміших подібних загроз можна назвати Android.SmsSend, а також давно відомі RedBrowser і Webster для Java-платформи. Вони маскуються під різні корисні програми, викликаючи тим самим довіру у користувача. Також існують віруси і для інших платформ, наприклад, Symbian OS, Windows Mobile та ін.

Шахрайство за допомогою використання систем інтернет-банкінгу. У даному випадку вірус відкриває доступ до мобільного додатку для роботи з банком або відповідному веб-сайту, або перехоплює SMS-повідомлення, що передаються користувачеві від систем інтернет-банкінгу. Небезпека даного типу може підстерігати власників мобільних телефонів, що працюють на різних платформах. Відомий троян Trojan-Spy.SymbOS.Zbot.a, що працює в сукупності з популярним вірусом Zbot для звичайних ПК.

На сьогодні вірус може розповсюджуватись такими способами, які зображені на рис. 1, рис. 2 [4].

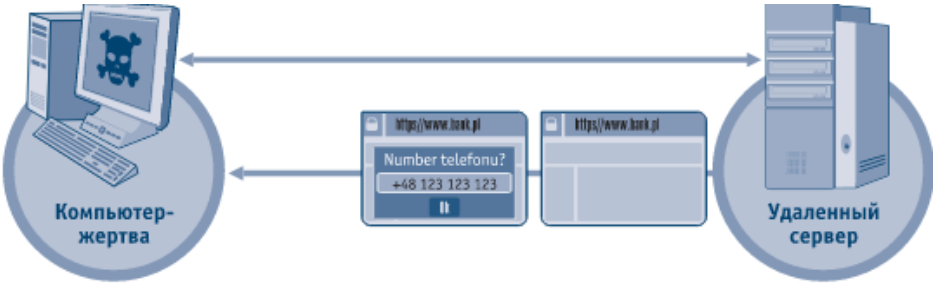

Рис. 1

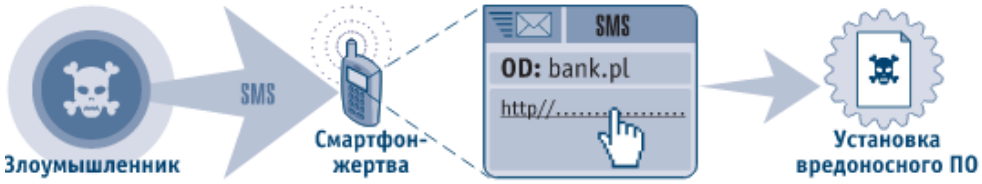

Рис. 2

Шляхи проникнення вірусу в телефон:

- з іншого телефону через Bluetooth-з'єднання;
- за допомогою MMS-повідомлення;
- з ПК (з'єднання через Bluetooth, USB, WiFi, інфрачервоне ...);
- через web- або wap-сайти.

Симптоми зараження:

1. Поява після копіювання і установки яких-небудь файлів (як правило, «ігор») всіляких «глюків» і «багів». Наприклад: безпричинно «зависає» телефон, не запускаються якісь програми, неможливо відкрити папку Прийняті файли.
2. Поява невідомих підозрілих файлів і іконок.
3. Мобільник мимовільно відправляє SMS і MMS, швидко спустошуючи рахунок власника.
4. Блокуються які-небудь функції телефону.

Деструктивні дії мобільних вірусів (одне з неписаних правил свідчить, що вірус, отримуючи управління, може робити в системі все те, що може робити користувач!):

- непомітна для користувача масове розсилання SMS та MMS;
- несанкціоновані дзвінки на платні номери;
- швидке спустошення рахунку абонента (у результаті дзвінків на платні номери і масової розсилки SMS та MMS);
- знищення даних користувача (телефонна книга, файли і т.д.);
- викрадення конфіденційної інформації (паролі, номери рахунків і т.д.);
- блокування функцій телефону (SMS, ігри, камера і т.д.) або апарат в цілому;
- швидка розрядка акумулятора;
- розсилка (від імені власника телефону) заражених файлів всіма можливими способами (e-mail, WiFi, Bluetooth і т.д.);
- при синхронізації телефону з комп'ютером - пересилання на ПК деструктивного коду;
- можливість віддаленого управління апаратом.

Антивірусні компанії давно почали випускати версії своїх програм для захисту мобільних телефонів, але спеціалізоване захисне ПЗ - мобільний антивірус, не завжди допомагає, так як віруси швидко еволюціонують. Найкращим захистом завжди була

пильність користувача. Шкідливий код не може проникнути на мобільний пристрій абсолютно без відома його власника. Тому, щоб уникнути зараження слід дотримуватись таких заходів захисту:

1. Якщо у вас «просунутий» мобільник, користуйтеся антивірусами.
2. Будьте обережні при установці всіляких додатків (особливо часто мобільні віруси «молотять» під гри!). Якщо є можливість, перед копіюванням / установкою чого-небудь на мобільник, перевірте те, що ви збираєтеся копіювати / встановлювати, на стаціонарному ПК антивірусним монітором зі свіжими базами.
3. Не встановлюйте на мобільник незнайомий «контент» невідомого походження.
4. Не дозволяйте запуск незнайомих програм.
5. Не тримайте Bluetooth постійно включеним, включайте його тільки в разі необхідності (а якщо вже доводиться тримати Bluetooth постійно включеним, використовуйте режим Прихований).
6. Якщо вам пересилають по Bluetooth якийсь підозрілий файл, ви завжди можете відхилити його прийом!
7. Не завантажуйте файли з Інтернету відразу на мобільник. Закачайте їх спочатку на ПК, перевірте антивірусом, а вже потім встановлюйте в мобільник.
8. Періодично перевіряйте на наявність вірусів свій мобільний пристрій.
9. Качайте файли тільки на довірених сайтах.
10. Очищуйте кеш пристрою, як найчастіше.

Якщо вірус з’явився, треба видалити заражені файли. Як правило, безпосередньо з мобільника (звичайного, не «смарта») видалити заражені файли не вдається. Для видалення заражених файлів потрібно підключити мобільник до ПК і скористатися яким-небудь файловим менеджером, наприклад, для телефонів Nokia – файловим менеджером, що входять до складу Nokia PC Suite. Після видалення заражених файлів перезавантажте мобільник (вимкніть і знову ввімкніть). Якщо видалення заражених файлів не допомагає, доведеться «перепрошити» телефон, звернувшись до сервісного центру.

Список використаних джерел

1. Компьютерные вирусы [Електронний ресурс]. – Режим доступу: http://avdesk.kiev.ua/virus/83-virus.html
2. Мобильные вирусы [Електронний ресурс]. – Режим доступу: http://www.corporacia.ru/pages/page/show/239.htm
3. Мобильные вирусы: очередной миф или реальная угроза? [Електронний ресурс]. – Режим доступу: http://netler.ru/pc/mobi-vir.htm
4. BYTE/ Россия Електронний ресурс]. – Режим доступу: http://www.bytemag.ru
5. Дрозд О.В. Інформаційна безпека мобільних пристроїв: актуальність, перспективи / О.В. Дрозд // Корпоративні центри мобільної безпеки. – 2013. – №3. – С. 28.
6. Леонтєв В.П. Новітня енциклопедія персонального комп'ютера / В.П. Леонтєв – М.: ОЛМА-ПРЕСС, 2003.

Анотація. Краснокутська І. Про комп’ютерні віруси для мобільних пристроїв та захист від них. *Розглянуто поняття «вірусу», його основні види. Зазначено складові мобільного вірусу та способи зараження ним. Виділені основні правила захисту.*

Ключові слова: *вірус, захист, черв’як, троянський кінь.*

Аннотация. Краснокутская И. Про компьютерные вирусы для мобильных устройств и защиту от них. *Рассмотрено понятие «вируса», его основные виды. Отмечены составляющие мобильного вируса и способы заражения им. Выделены основные правила защиты.*

Ключевые слова: *вирус, защита, червь, троянский конь.*

Abstract. Krasnokutskaya I. About computer viruses for mobile devices and protection against them. *The concept of "virus" and its main types are presented. Noted components mobile virus and their methods of infection. The basic rules of protection are listed.*

Keywords: *virus protection, worm, Trojan.*

Інна Левченко
Сумський державний педагогічний університет імені А.С. Макаренка, м. Суми
Innet1204@yandex.ua
Науковий керівник – С.І. Петренко

ВИХОВНИЙ АСПЕКТ СЕРЕДОВИЩА ПРОГРАМУВАННЯ «SCRATCH»

З розвитком інформаційних технологій все більшої і більшої ролі набуває використання сучасних технічних засобів навчання в школі. Важливе місце в системі технічних засобів навчання займають навчально-розважальні комп'ютерні програми, що розвивають уміння і навики алгоритмізації та програмування.

Одна з таких програм, що набула в освітньому процесі досить широкої популярності є середовище програмування Scratch, яке на сьогодні посідає 24 місце серед всіх найбільш популярних мов програмування, серед яких C, Java, C ++, C #, PHP, Pascal [2].

Scratch – це візуальне об'єктно-орієнтоване середовище програмування для навчання школярів молодших і середніх класів. Його призначено для створення комп'ютерних анімацій, мультимедійних презентацій, анімаційних та інтерактивних історій, ігор, моделей і інших видів роботи [1, с. 6].

Мова Scratch була розроблена у 2007 році в лабораторії Lifelong Kindergarten під керівництвом професора Мітчела Рєзніка з метою спрощення процесу вивчення програмування та створення зрозумілого інструменту, який би дозволив дітям, у яких немає досвіду програмування, вивчити основні принципи об'єктно-орієнтованого і багатопотокового програмування [3].

Спочатку Scratch створювали для учнів віком від 8 до 16 років, але як свідчить практика навіть діти молодшого шкільного віку можуть працювати в цьому середовищі.

На сьогодні сучасна наука втратила свою цілісність. Шкільна освіта – це не що інше як вивчення окремих фрагментів мозаїки, з яких складена картина світу. Враховуючи соціальні дослідження, за якими кожні п'ять років кількість інформації збільшується вдвічі, сучасна школа повинна визначити одними з пріоритетних завдань розвиток частинно-пошукових здібностей школяра та його креативного мислення.

Один з розробників середовища програмування Scratch, Алан Кей вважає, що необхідно як можна раніше дати учневі потужний «інструмент для думання», який би сприяв пізнанню нового і створенню зв'язків між відомим, розвивав не тільки аналітичне, але й синтетичне мислення [1, с.7].