СЕКЦІЯ 10

SECTION 10

МАТЕМАТИЧНІ МЕТОДИ, МОДЕЛІ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЕКОНОМІЦІ MATHEMATICAL METHODS, MODELS, AND INFORMATIONAL TECHNOLOGIES IN ECONOMICS

УДК 339:004.9

Пашнєв Д. В.
к. ю. н., доцент,
провідний науковий співробітник науково-дослідної лабораторії з проблем інформаційних технологій та протидії злочинності у кіберпросторі,
Харківський національний університет внутрішніх справ
Колмик О. О.
науковий співробітник науково-дослідної лабораторії з проблем інформаційних технологій та протидії злочинності у кіберпросторі,
Харківський національний університет внутрішніх справ

ШКІДЛИВЕ РЕКЛАМНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ЙОГО ВИДИ ТА ЗАХИСТ ВІД НЬОГО

Реклама – двигун прогресу і в умовах розвитку ринкової економіки цей механізм носить позитивний характер, якщо служить своїй меті – маркетинговому просуванню товару на ринок. В епоху розвитку сучасних інформаційних технологій з'явилися нові способи підвищення ефективності рекламної діяльності.

Рекламне програмне забезпечення (далі – РПЗ) або «adware» (від англійських слів «advertisement» – реклама, «software» – програмне забезпечення) – це програма, діяльність якої зводиться до демонстрації рекламних повідомлень в браузерах, мережевих додатках та окремих вікнах на екрані комп'ютера або іншого пристрою, перетворюючи таким чином його повністю або частково в банер для показу реклами. І в принципі від використання такого механізму для розповсюдження інформації про товари та послуги немає шкоди, в нормальній ситуації користь отримують всі сторони: користувач – від отримання інформації про товар, який, можливо, йому потрібен, а продавець, замовник реклами і володілець ресурсу або додатку, у якому розміщене РПЗ – від отримання прибутку.

Але бувають і інші ситуації, коли робота такого РПЗ наносить певну шкоду користувачу пристрою. Така ситуація виникає, коли функціонування РПЗ відбувається поза бажанням користувача пристрою повністю або воно має приховані від користувача функції, а також у разі відсутності простого механізму вимкнення дії такого програмного забезпечення.

Найчастіше РПЗ за рахунок відволікання ресурсів сповільнює завантаження веб-сторінок, знижує продуктивність операційної системи (далі – ОС) пристрою, показує на екрані рекламні повідомлення, які заважають роботі користувача.

Але шкода від такого РПЗ може бути набагато більшою від банальної нав'язливої реклами. Зокрема, для підвищення своєї ефективності більшість РПЗ збирають дані про користувача для відображення рекламних повідомлень, які найбільш підходять йому, і ці дані можуть бути використані не тільки із цією метою. Крім того, РПЗ можуть містити функціонал шкідливого програмного забезпечення: розповсюджуватися подібно до комп'ютерних вірусів, модифікувати інші додатки за допомогою вставки спеціальних скриптів, перенаправляти користувача на шкідливі веб-сайти та небезпечні сторінки через різні посилання, наражаючи на ризик зараження комп'ютерними вірусами тощо [1].

Частка РПЗ серед іншого шкідливого програмного забезпечення доволі велика, на що звертають увагу провідні спеціалісти у галузі захисту інформації [2].

Як видно, шкідливе РПЗ містить загрози для інформаційної безпеки користувачів сучасних інформаційних технологій, отже актуальним є його виявлення та захист від нього.

Модифікацій такого шкідливого РПЗ існує безліч: від найпростіших, що видаляються в кілька кліків за допомогою вбудованих функцій операційної системи, до найнебезпечніших, які дуже складно видалити. Вони підстерігають користувачів завжди і всюди: від комп'ютерів під операційними системами Windows чи Mac OS, до мобільних телефонів і практично всіх типів браузерів.

Залежно від способу проникнення в систему поділяють кілька типів РПЗ. Перший потрапляє до системи у процесі скачування та встановлення безкоштовних або умовно безкоштовних програм. Деякі недобросовісні розробники безкоштовних програм використовують рекламне програмне забезпечення для фінансування розробки та дистрибуції своїх продуктів, вживлюючи в інсталятори своїх програм спеціальні модулі, які містять саме таке шкідливе РПЗ. Воно активується після розпакування та інтегрується в систему.

Другий розповсюджується через інфіковані веб-ресурси. При відвідуванні зараженої сторінки автоматично виконується спеціальний алгоритм, який здійснює несанкціоноване завантаження та встановлення РПЗ поза дозволом і інформуванням користувача. Користувач і сам може допомогти завантаженню, здійснивши натискання на кнопку (посилання) у додатковому вікні або фіктивному повідомленні про помилку.

В обох випадках рекламний модуль може бути завантажений і встановлений шкідливим агентом, що вже присутній в системі, наприклад, «троянським конем» - завантажувачем.

Також можна умовно поділити шкідливе РПЗ за способом реалізації: в одному випадку вони виконані, як самостійні програми, що запускаються зі стартом системи, в іншому – виконані у вигляді модуля, що впроваджується в існуючі процеси, найчастіше в браузер. Найчастіше модулі шкідливого РПЗ відразу дають про себе знати, наприклад, через певний проміжок часу, відкриваючи одну і ту ж сторінку браузера (електронне казино, сайти еротичного змісту), тим самим даючи зрозуміти, що система заражена. Але деякі різновиди пересічний користувач може навіть не помітити, бо вони активізуються тільки на певних сторінках, які користувач відвідує частіше за все. Сучасний користувач настільки звик до реклами та різних спливаючих вікон при перегляді тих чи інших сайтів, що часом йому важко розрізнити з чим він має справу, із шкідливим РПЗ або звичайним показом реклами на сайті.

Відомими випадками використання РПЗ із шкідливою метою є наступні.

Adware Generic Summary – завантажує в браузери потенційно небезпечні рекламні оголошення, панелі інструментів, відстежує історію відвідування сайтів, змінює налаштування стартової сторінки, замість довірених пошукових систем встановлює посилання на рекламні та вірусні веб-ресурси.

Adware.Win32.Look2me.ab – уповільнює функціонування ОС, виводить додаткові вікна з нав'язливою рекламою у браузері. Ретельно маскує свої елементи в папці System32: після кожного старту системи змінює їх назви (sMfrcdlg.dll, lvlm0931e.dll, azam0931e.dll, noxpnt.dll). Реєструє у реєстрі розширення Winlogon та Explorer. Захищає файли рекламного модуля: встановлюючи атрибути «тільки читання» та «системний».

Adware.SwiftBrowse.Win32 – підміняє результати пошуку, перенаправляє користувача на завантаження шкідливих програм. Цей метод використовується як для завантаження нових версій Adware.SwiftBrowse, так і для завантаження інших шкідливих програм [3].

З метою дотримання інформаційної безпеки кожен користувач повинен знати типові ознаки, за якими можна виявити, що на пристрої встановлено шкідливе РПЗ:

– домашня сторінка браузера змінилася без дозволу користувача;

– рекламні оголошення показуються там, де їх не повинно бути;

– веб-сторінки, які часто відвідує користувач, часто відображаються по-різному;

– посилання веб-сайтів пересилають користувача на непередбачені сторінки;

– веб-браузер працює надто повільно та (або) часто виникають збої;

– без дозволу користувача з'явилися нові панелі, додаткові модулі або розширення;

– почали автоматично встановлюватися програми, дозвіл на що користувач свідомо не давав;

– спостерігаються стрибки споживання ресурсів пристрою.

Щоб запобігти, або хоча б знизити, ймовірність завантаження шкідливого РПЗ на пристрій, користувачам необхідно виявляти обережність при роботі з будь-якими сайтами, що підозріло виглядають. Для цього необхідно дотримуватися певних рекомендацій:

– під час перегляду сайтів не натискати на будь-які рекламні оголошення, банери або сповіщення;

– слідкувати за тим, щоб на всіх пристроях було оновлено операційну систему, тому що неоновлені системи більш вразливі: шкідливі програми можуть використовувати вразливості у їх безпеці;

– увімкнути параметри безпеки в ОС, що захищають від завантаження РПЗ;

– налаштувати браузер для блокування спливаючих вікон;

– бути обережним під час завантаження безкоштовних або умовно безкоштовних програм, зокрема, уважно перевіряти, яке програмне забезпечення може бути встановлено разом із основною програмою, і чи не надає користувач свою згоду на його встановлення;

– завантажувати програми тільки з надійних перевірених сайтів, яким довіряє користувач;

– перевіряти антивірусом кожен файл, що завантажується тощо.

Таким чином, можна зробити певні висновки. По-перше, існує нормальне і шкідливе РПЗ, головна відмінність другого від першого, що воно може встановлюватися або вчиняти певні дії із комп'ютерним пристроєм поза згодою і увагою власника, а також не має простого механізму припинення своєї діяльності і видалення з пристрою. По-друге, розрізняють класифікацій шкідливого РПЗ, з який найбільш значимими для протидії йому є: в залежності від способу проникнення на пристрій та за способом реалізації. По-третє, часто користувачі самі стають ініціаторами (винуватцями) проникнення до системи шкідливого РПЗ, що вимагає від них дотримання певних правил безпеки при роботі із мережевими ресурсами, що повинне стати основою для протидії шкідливому РПЗ.

Список літератури

1. Pieter Arntz. Adware vs. ad fraud // Alwarebytes: Cyberprotection for every one. - URL: https://www.malwarebytes.com/blog/news/2017/03/adware-vs-ad-fraud (дата звернення: 15.05.2023).

2. Вірусні загрози 2015: під знаком adware // Zillya! Антивирус: офіц. сайт. - URL: https://zillya.ua/index.php?q=virusni-zagrozi-2015-pid-znakom-adware (дата звернення: 15.05.2023).

3. Семейство Adware. SwiftBrowse.Win32 // Zillya! Антивирус: офіц. сайт. - URL: https://zillya.ua/index.php?q=ru/semeistvo-adware-swiftbrowsewin32 (дата звернення: 15.05.2023).