УДК 044.056.53

АНАЛІЗ ФАКТОРІВ КІБЕРЗЛОЧИНСТВА

Горошко Т.С., Масальська О.О.
Державний ВНЗ «Національний гірничий університет», http://bit.nmu.org.ua/,
E-mail: tatyanagoroshko@mail.ru

У статті аналізується кіберзлочинство на прикладі життєвого циклу шкідливого програмного забезпечення. Продемонстровані найбільш розповсюджені загрози інформації й обчислювальній техніці звичайних громадян та напрямки атаки шахраїв, а також обґрунтована неефективність існуючої боротьби з ними.

Ключові слова – небезпечне програмне забезпечення, кіберзлочинство.

ВСТУП

Незважаючи на прийняте законодавство по боротьбі з кіберзлочинністю, її склад досі чітко не описаний, як і не має загальновизнанного визначення поняття «комп'ютерна злочинність». Це обумовлено безперервним ростом можливостей технічних засобів, програмного забезпечення, засобів телекомунікацій, так і кримінальних хитрувань самих кіберзлочинців з розвитком науково-технічного прогресу і відсталістю правових норм протидії.

Кіберзлочинність можна визначити як незаконні дії, які здійснюються людьми, які використовують інформаційні технології для злочинних цілей. Серед основних видів кіберзлочинності виділяють поширення шкідливих програм, злом паролів, крадіжку номерів кредитних карт та інших банківських реквізитів, а також поширення протиправної інформації (наклепу, порнографічних матеріалів) через мережу Інтернет.

ТЕРМІНИ ТА ВИЗНАЧЕННЯ

Загроза – це потенційна можливість події, яка чинить небажаний вплив. Загроза реалізується через вразливість – слабке місце у системі захисту інформації.

У даній роботі основні загрози, що надходять з кіберпростору, а також можливі напрямки їх атак будуть розглянуті на прикладі одного з яскравих прикладів кіберзлочинності – шкідливого програмного забезпечення.

Програми з потенційно небезпечними наслідками (далі – шкідливі програми – ШП) – це окремі програми (набори інструкцій), які мають спроможність виконувати будь-яку непусту множину наступних функцій:

- приховування ознак своєї присутності в програмно-апаратному середовищі мережі;
- здатність до самодублювання, асоціювання себе з іншими програмами і (або) перенесення своїх регламентів в інші ділянки оперативної або зовнішньої пам'яті;
- руйнування (спотворення) кодів програм в оперативній пам'яті;
- збереження фрагментів інформації з оперативної пам'яті в деякій ділянці зовнішньої пам'яті прямого доступу (локальної або віддаленої);
- спотворення довільним чином, блокування і (або) підміна масивів інформації, що виводиться у зовнішню пам'ять або в канал зв'язку, утворених в результаті роботи прикладних програм, або масивів даних, що уже знаходяться у зовнішній пам'яті;
- придушення інформаційного обміну в телекомунікаційних мережах, фальсифікування інформації в каналах управління;
- нейтралізація роботи тестових програм і систем захисту інформаційних ресурсів.

ШЛЯХИ РОЗПОВСЮДЖЕННЯ ШП

Аналіз ринку – перша стадія життєвого циклу ШП. Він дає змогу зрозуміти, як важко буде знайти в популярних програмних продуктах вразливості, чи будуть вони цінні, чи буде вигідною покупка вразливостей у розробників або тестерів цього програмного продукту з метою використання або перепродажу.

Аналіз програмного забезпечення – другий етап життєвого циклу. На ньому проводиться детальний аналіз програмного або апаратного продукту, вибраного на першому етапі.

Розробка ШП – на даній стадії через знайдена вразливість (або кілька вразливостей) реалізується кінцевий, шкідливий продукт.

Поширення – останній етап, коли ШП інфікують пристрій, на який воно націлено. Є багато шляхів поширення шкідливих програм, у цій роботі виділимо ті, що найчастіше зустрічаються.

1. Програмна пастка представляє програмну закладку, яка використовує помилки або неоднозначність у програмному забезпеченні. Ця категорія є вразливістю сама по собі, а також може служити методом для поширення шкідливих програм, наприклад, браузером. Цей тип вразливості не новий, але він буде актуальним завжди.

2. Троянські програми – програмні закладки, які мають законний доступ до системи, проте виконують також і приховані (неоголошені) функції, тобто шкідливі програми маскуються під корисні.

3. Фішинг – спроба видати шкідливий сайт за сайт великої та відомої компанії, якій користувач довіряє. Сайт пропонує ввести свої логін та пароль, навіть дані кредитних карток, потім видає помилку і просить спробувати пізніше.

4. Спам – анонімні масові розсилки електронної пошти, найчастіше використовується для реклами товарів і послуг. Спамери наживаються на тих, хто відповідає на повідомлення. Крім того, спам слугує і для поширення шкідливих програм. Зараз поштові служби блокують більшість спам-повідомлень.

5. Бот-мережа – це мережа комп'ютерів, заражених шкідливою програмою, яка дозволяє кіберзлочинцям віддалено керувати зараженими машинами. За допомогою бот-мережі можна організувати

розповсюдження спаму, проведення DDoS-атак та розподільних обчислень.

6. Мобільні пристрої – бурхливий розвиток мобільних технологій, значне збільшення їх обчислювальних можливостей і швидкості доступу до мережі Інтернет не могли залишитися непоміченими для зловмисників. ШП для мобільних пристроїв часто крадуть персональні дані власників, відправляють дорогі повідомлення, дзвонять за кордон. Не виключені і стандартні сценарії, як відправлення спаму чи фішинг.

5. Соціальні мережі – цей спосіб стає все менш ефективним, оскільки розробники соціальних мереж покращують захист користувачів. Але і досі ШП використовують довірливість людей. Сценарії збігаються з попереднім випадком, тільки платформою для відправки повідомлень виступає клієнт обміну миттєвими повідомленнями.

6. Локальні мережі – один з найстаріших способів, але досі ефективний, що доводить недавня епідемія вірусу Conficker/Kido. Цей метод схожий на програмну пастку, але він використовує вразливості в операційних системах, мережевих протоколах, пристроях и службах.

7. Мобільні пристрої збереження інформації – усі носії від дискет до флеш-накопичувачів. Найчастіше ШП використовують автозапуск, багато хто відмовляється від цієї функції заради безпеки. Стає на заваді цьому шляху також поширення «хмарних» технологій.

ШЛЯХИ ОТРИМАННЯ МАТЕРІАЛЬНОЇ ВИГОДИ

Використовують ШП найчастіше для одержання прибутку, тобто вразливості «монетизуються» різними способами.

Зловмисник може продати вкрадену інформацію або здати в оренду обчислювальні ресурси бот-мережі. Даний тип монетизації потребує досить багато зусиль, оскільки потрібно координувати роботу великої кількості інфікованої техніки, залишаючись при цьому непоміченим.

Методи боротьби з бот-мережами на даний час неефективні, як тільки вдається припинити функціонування однієї бот-мережі, зловмисник заміняє втрачені ресурси резервними. Спіймати зловмисників майже неможливо, вони часто приховуються за довгим ланцюжком проксі-серверів. Тому потрібно приділяти значно більше уваги дослідженню кримінальних структур, що стоять за подібними порушеннями, і створити такі умови, щоб їх послуги не були потрібними.

Інший шлях – розповсюдження спаму. З цим, напевно, стикався кожен. Окрім пропозицій покупки товарів, а також фішинга, користувач може отримати і інші шахрайські повідомлення, наприклад, «нігерійські» кошти, які виманюють гроші, обіцяючи ще більше грошей.

Злодій може продати персональні дані та іншу конфіденційну інформацію – дані кредитних карт, регістраційні дані соціальних мереж, історію відвідування веб-сайтів, інформацію з пам’яті комп’ютера «жертви».

Часто зловмисники виводять зі строю обладнання і вимагають гроші за повернення працеспроможності.

ШЛЯХИ ЛЕГАЛІЗАЦІЇ

Мало заробити гроші – їх потрібно «відмити», тобто легалізувати так, щоб злочин не був виявлений. Виділяють кілька способів.

Дроп – зловмисник витрачає кошти в онлайн-магазинах, передаючи їх посередникам («дропам»), які потім повертають товар безпосередньо зловмиснику. Так не розкривається фізична адреса, навіть місто, у якому проживає зловмисник.

Оффшор – старий метод, який використовують і «класичні» злочинці. Потрібно провести суму грошей через декілька банківських рахунків так, щоб це не можна було його відстежити. Рахунки, навіть цілі банки, що беруть участь у подібних операціях, звичайно існують короткий проміжок часу, а потім безслідно зникають.

Електронні гроші – нематеріальний характер і складність відстеження операцій сприяє різним фальсифікаціям. Легко розвернути і ліквідувати.

Азартні ігри в мережі Інтернет – метод схожий на попередній, транзакції та джерело грошей дуже важко відстежити.

ВИСНОВКИ

Для боротьби з кіберзлочинством доцільно:

- вдосконалити законодавство, усунути в ньому неточності, розбіжності;
- вжити заходи по зниженню рівня хуліганської і кримінальної активності в мережі Інтернет. Можливості контролю цієї активності значно обмежено правом людей на недоторканість приватного життя;
- розробити систему з попередження шахрайств в мережі Інтернет, проведення сертифікації сайтів компаній, які проводять розрахунки між продавцем та покупцем за допомогою електронного зв’язку;
- створити сайт, що висвітлюватиме протидію вітчизняних правоохоронних органів кіберзлочинності. Цікавим прикладом слугує портал Cyber-crimes.ru, де публікуються реально розслідувані кримінальні справи.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Карпов Н., Вертузаев М. К вопросу о борьбе с компьютерными преступлениями в Украине // Закон и жизнь. – 2004. – № 7.

2. Ястребов Д.А. Институт уголовной ответственности в сфере комп. информации // Гос. и право. – 2005. – № 1.

3. Конахович Г.Ф., Климчук В.П., Паук С.М., Потапов В.Г. Защита информации в телекоммуникационных сетях. — К.: МК-Пресс, 2005.