- установка екранів для веб-додатків;
- застосування стійких технік керування сесіями та завершення сесій після кожного запиту;
- відключення розподілу TCP-з'єднань на проміжних пристроях;
- активізація заборони на кешування всіх сторінок;
- використання технології SSL для захисту сайтів;
- повне усунення XSS-вразливостей;
- блокування запитів по протоколі HTTP/1.0 на рівні веб-сервера;
- фільтрація уведених користувачем даних з метою видалення послідовностей CRLF.

Одержано 27.10.2017

УДК 651. 34

Світлана Юріївна ГАВРИЛЕНКО,
кандидат технічних наук, доцент кафедри «Обчислювальна техніка та програмування» Національного технічного університету «Харківський політехнічний інститут»

Ілля Валентинович ШЕВЕРДІН,
аспірант кафедри «Обчислювальна техніка та програмування» Національного технічного університету «Харківський політехнічний інститут»

РОЗРОБКА ЕКСПЕРТНОЇ СИСТЕМИ ВИЯВЛЕННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НА БАЗІ АНАЛІЗУ ВІРУСУ PETYA

Найпомітнішою подією першого літнього місяця 2017 року на Україні стала епідемія вірусу-шифрувальника Trojan.Encoder.12544, що згадується в ЗМІ як Petya.A або mbr locker 256. Під удар «вірусу-вимагача» потрапили українські державні структури і приватні компанії: Кабінет Міністрів, «Ощадбанк», «Укренерго», «Нова пошта», аеропорт Бориспіль, Чорнобильська АЕС та інші організації. Ця шкідлива програма заразила комп'ютери безліч організацій і приватних осіб в 60 країнах світу.

В роботі проаналізовано даний вірус та описано етапи поширення, а саме встановлено наступні шляхи зараження:

1) шляхом експлуатації вразливості в SMB MS17-010 (аналогічно вірусу Wanna Cry);

2) шляхом спрямованої відправки шкідливого програмного забезпечення за електронною поштою;

3) шляхом використання вразливості для виконання шкідливого коду: CVE-2017-0199;

4) шляхом використання вразливості для поширення і зараження в EternalBlue.

Першим етапом є впровадження, воно здійснюється шляхом скачування шкідливого контенту з заражених веб-сайтів, через ботнет, через ігрові сервери або за рахунок використання вразливості різних компонентів системи, а саме:

- вразливості веб-браузерів (експлойти iframe, XSS);
- вразливості клієнтів електронної пошти;
- вразливості операційної системи.

Другий етап, це безпосередній запуск вірусу, що являє собою шифрування інформації. Як правило користувач запускає вірус сам, при цьому не здогадуючись про фатальну помилку, тому що вірус захований шляхом впровадження в стороннє програмне забезпечення або плагін для веб-браузера.

Розшифрувати файли, зашифровані вірусом шляхом підбору ключа неможливо, тому що вірус Petya використовує асиметричну криптографію RSA, тобто для кожного зараженого комп'ютера існує персональний ключ (private key) RSA. Для підбору ключа потрібно дуже великий обчислювальний потенціал, який в звичайних умовах неможливо відтворити.

Наступним етапом роботи вірусу Petya буде перезавантаження системи, в окремих випадках воно здійснюється автоматично, шляхом створення завдання на перезавантаження в системному планувальнику завдань. Після перезавантаження, на екран виводитися банер з вимогою перевести гроші за розшифрування, в якому пропонується перерахувати $300 шляхом використання піринговой платіжної системи Bitcoin. Використання даної платіжної системи дозволяє зловмисникам залишатися анонімними. Оплативши послугу, виводиться повідомлення про те, що необхідно надати ідентифікатор гаманця Bitcoin і згенерований ідентифікатор системи на електронну пошту вимагачів. Гарантії відновлення файлів немає, так як на той час, в більшості випадків, вже будуть заблоковані рахунки і поштовий ящики зловмисників. Так само немає доказів, що окремий подібний вірус створений тільки з метою вимагання. Подібні віруси також можуть створюватися з метою тільки шкідливого впливу, блокуючи роботу державних організацій.

Результатом аналізу вірусу у віртуальній операційній системі є збір системних звітів і подій та формування бази послі-

довності системних команд, котрі мають зловмисну дію. В якості команд будо виділено ключи реєстру, зміна MBR та зміни файлової системи, а саме створення файлів, шифрування та видалення. Отримано, що в заражених системах зазначені файли розташовуються в файловій системі в таких папках:

1) C: \ Windows \ perfc.dat;
2) % APPDATA% \ 10807.exe;
3) C: \ myguy.xls.hta.

Виявлено наступні шкідливі файли та їх хеш-суми:

1) файл myguy.xls, розмір 13893 байт,
SHA1: 736752744122A0B5EE4B95DDAD634DD225DC0F73
MD5:0487382A4DAF8EB9660F1C67E30F8B25;

2) файл BCA9D6.exe, розмір 275968 байт
SHA1: 9288FB8E96D419586FC8C595DD95353D48E8A060,
MD5: A1D5895F85751DFE67D19CCCB51B051A.

Отримана інформація дозволила побудувати антивірусний програмний додаток на базі нейронної мережі типу АРТ-1, що надалі дозволить виявляти модифікації даного вірусу.

Одержано 24.10.2017

УДК 004.056.53

Захар Георгійович ДЕМИДОВ,
науковий співробітник науково-дослідної лабораторії захисту інформації та кібербезпеки Харківського національного університету внутрішніх справ

ОСНОВНІ ВИДИ КІБЕРАТАК НА WEB-САЙТИ

Основне правило при створенні web-ресурсу - ніколи не довіряти даним, введеним користувачем. Про це знають багато web-програмістів, але не всі до кінця дотримуються цього, з думкою: "Що там на цьому сайті ламати, та кому це потрібно". Але найчастіше на таких сайтах і вчаться зламувати адмінку й бази даних. Винятки становлять сайти, зроблені на основі якогось сучасного фреймворку (Наприклад: LARAVEL, SYMFONY, YII 2.0), бо там система безпеки вже протестована досвідченими фахівцями в цьому напрямку [1].

У інтернет-мережі зараз маса інформації щодо різних видів хакерських атак на web-сайти, але давайте їх ще раз узагальнимо, пояснимо та визначимо способи боротьби та запобігання.