УДК 004.7:004.56.53
Я. Кінах
(Тернопільський національний технічний університет імені Івана Пулюя)

ВИКОРИСТАННЯ КРИПТОГРАФІЧНИХ ЗАСОБІВ ДЛЯ ПРОГРАМНОЇ НЕЙТРАЛІЗАЦІЇ АГРЕСИВНОГО ТРАФІКУ

Задача керування інформаційними ризиками в умовах глобалізації набула особливої гостроти в Україні. Це зумовлено ескалацією інформаційних конфліктів в комп'ютерних мережах, що реалізуються інформаційними війнами, кібератаками, гіперактивними користувачами мереж. Сучасні системи безпеки не справляються із задачею контролю інформаційних потоків, оскільки не аналізують ризики, що виникають в трафіках комп'ютерних мереж, та не досліджують першоджерела пакетів, їхні шляхи, а лише констатують наявність атаки та частковий захист від потенційний зловмисників [1] (Рис. 1).

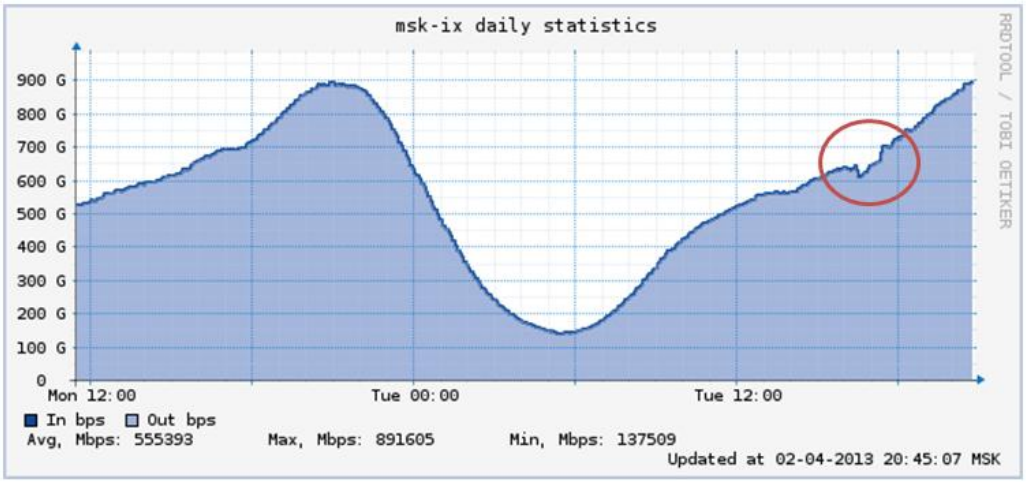

Рис. 1. Типовий вплив кібератаки на трафік комп'ютерної мережі

Для розв'яку цієї задачі доцільно скористатися імовірнісними методами маркування пакетів із використанням алгоритмів цифрового підпису з використанням криптографічного методу RSA [3], це дозволить на практиці ефективно знаходити бот-мережі та складати їхні карти, що реалізують кібератаки. Така методологія також використовуються для виявлення нових версій комп'ютерних вірусів, які проходять випробування на користувачах відкритих систем типу VirusTotal [2]. Тому довільні зміни в програмному коді і його бінарній компіляції є малоймовірними. Виявлення нових версій програм та даних за допомогою RSA підпису дозволяє легальне оновлення та зміну сигнатури програмного коду, аналізувати нові варіанти і повідомляти про нові бот-вузли, що працюють проти цільової аудиторії користувачів.

Істинність цифрового підпису забезпечить джерелу та приймачу інформаційного потоку безпеку [4], нейтралізує агресивне інформаційне середовище та дозволить достеменно визначати ризики комп'ютерних мереж з подальшим їхнім керуванням.

1. http://www.msk-ix.ru/network/traffic.html
2. http://www.emc.com/collateral/white-papers/h12756-wp-shell-crew.pdf
3. *Rivest R. L.*, *Shamir A.*, *Adleman L.* A method for obtaining digital signatures and public-key cryptosystems // *Communications of the ACM*. — New York, NY, USA: ACM, 1978. — Т. 21. — № 2, Feb. 1978. — С. 120—126. — ISSN 0001-0782. — DOI:10.1.1.40.5588
4. *Ян С.* Криптоанализ RSA. — Ижевск: РХД, 2011. — 312 с.