УДК 004.92

А.О. Нічепорук, к.т.н., А.А. Нічепорук, Ю.О. Нічепорук, Казанцев А.Д.

МОДЕЛЬ ПРОЦЕСУ ПОБУДОВИ ПІДГРАФІВ ФРАГМЕНТІВ БОТ-МЕРЕЖ НА ОСНОВІ АНАЛІЗУ МЕРЕЖЕВОГО ТРАФІКУ

Виявлення бот-мереж є однією із головних проблем в галузі кібербезпеки. Сучасні методи в першу чергу спрямовані на виявлення бот-мереж та попередження їх поширення [1]. Проте при виявленні таких загроз розробники досить часто нехтують умовою наявності декількох бот-мереж, що інфікували одну локальну мережу [2]. Це значно знижує ефективність залучених методів по виявленню бот-мереж в локальній мережі. Тому актуальною є задача формалізації процесу побудови підграфів фрагментів бот-мереж на основі аналізу мережевого трафіку.

Подамо модель процесу побудови підграфів фрагментів ботнет на основі аналізу мережевого трафіку у вигляді кортежу:

$$M_{proc} = \langle L, \omega, \gamma, \kappa, Q, G, C \rangle, \tag{1}$$

де L – локальна мережа; κ – функція, яка здійснює відстеження шкідливої активності хостів, що є частиною бот мережі; ω – функція відображення хостів, що проявляють шкідливу активність у зважений повнозв'язний граф; γ – функція виділення фрагментів бот мережі; Q – множина шкідливих активностей, що проявляються на хостах, інфікованих бот мережею; G – зважений повнозв'язний граф; C – множина бот мереж.

Тоді функцію, яка здійснює відстеження шкідливої активності хостів, що є частиною бот мережі задамо наступним чином:

$$\kappa : Att \times h'_C \to Q, \forall h'_C \in Q, \tag{2}$$

де Att – множина атрибутів для ідентифікації шкідливої активності на хосту h'_C, що інфікований бот мережею C.

Визначимо функцію відображення хостів, що проявляють шкідливу активність у зважений повнозв'язний граф:

$$\omega : h'_C \to G, \forall v_i \in h'_C, \forall h'_C \in Q, \tag{3}$$

де G – зважений повнозв'язний граф:

$$G = (V, E, w), \tag{4}$$

де V – набір вузлів, причому кожен інфікований хост – вузол, а E – набір ребер, w – ваги ребер.

Представимо функцію виділення фрагментів бот мережі:

$$\gamma : G \to \{G_1, G_2, ..., G_n\}, G_i \subseteq G, \forall G_i = \sum w(g_i) \to min \tag{5}$$

де вага кожного ребра, що з'єднує дві вершини визначається з правила Байєса:

$$w(g_i, g_j) = p(C_{i,j}^{(t)} \mid G_i^{(t)} = g_i, G_j^{(t)} = g_j) = \frac{p(G_i^{(t)} = g_i, G_j^{(t)} = g_j \mid C_{i,j}^{(t)}) p(C_{i,j}^{(t-1)})}{p(G_i^{(t)} = g_i, G_j^{(t)} = g_j)}. \tag{6}$$

В кожний дискретний момент часу оновлюватимемо попереднє значення імовірності $p(C_{i,j}^{t-1})$ між кожною парою вузлів до останнього значення $p(C_{i,j}^{t})$ використовуючи правило Баєса. Оновлена вага ребра між двома вузлами залежить від попередньої ваги ребра $p(C_{i,j}^{t-1})$, тобто ймовірності побачити групу активностей $G_i^{(t)}$ та $G_j^{(t)}$ з урахуванням значення $C_{i,j}$, і загальної ймовірності побачити пару дій $p(G_i^{(t)}, G_j^{(t)})$.

Висновки. Таким чином, запропонована модель процесу дозволяє здійснити формалізоване представлення побудови підграфів фрагментів ботнет на основі аналізу мережевого трафіку та залежить, в першу чергу, від тимчасових взаємозв'язків шкідливих дій між комп'ютерами в мережі і не залежить від архітектур бот-мереж і засобів, які використовуються для їхнього керування.

Література

1. Kapre A. Behaviour based botnet detection with traffic analysis and flow interavals using PSO and SVM / A. Kapre, B. Padmavathi // International Conference on Intelligent Computing and Control Systems: Proceedings (Madurai, India, 15-16 June 2017). Madurai, 2017. P. 718–722.
2. Jaikumar P. A graph-theoretic framework for isolating botnets in a network / P. Jaikumar, A.C. Kak // Security and Communication Networks. – 2012. – Vol. 5. – No. 6. – Pp. 2605–2623.