УДК 004.056.5(043.2)

Пасько О.З.
Національний авіаційний університет, Київ

МЕТОДИ ЗАХОПЛЕННЯ БОТ-МЕРЕЖ

Вступ. Однією із форм ведення інформаційної війни є бот-мережі (ботнет). З їх появою кількість кіберзлочинів збільшилася в сотні разів, адже це не тільки кіберзброя, а й основа кіберкримінального бізнесу.

Постановка задачі. Ботнет представляє собою цілу армію інфікованих ботом комп'ютерів, що знаходяться під віддаленим контролем зловмисника. Вони паразитують на звичайних персональних комп'ютерах і серверах, в значній мірі являються самостійними (реплікація, відсутній зв'язок з іншими вузлами, виконання різного роду завдань для забезпечення життєдіяльності), але в кінцевому рахунку завжди підпорядковані тим, хто їх створив. Мета створення ботнет – здійснення атак, наприклад, DDoS, Flooding DoS, спамінг, крадіжка особистих даних та ін.

Для захоплення керування бот-мережею та її подальшої нейтралізації пропонується ряд рекомендацій:

- захопить або вивести із ладу C&C(Command&Control) – сервер для керування бот-мережею;
- DDoS на C&C;
- жалоби провайдеру, де знаходяться C&C;
- блокування IP-адрес;
- арешт власника ботнет;
- судовий позов.

Деякі з методів успішно вдалося застосувати. Так, ботнети Rustock і Coreflood були знищені саме таким чином. Проте дані засоби не зовсім підходять для нейтралізації ботнет на основі p2p-мереж, оскільки вони є децентралізовані. У цьому випадку використовують методи порушення p2p-механізмів та порушення обміну DNS/HTTP-командами.

Висновки. Сучасні суспільства представляють собою складні мережі, що складаються з людей, інформаційних систем та машин. Ті країни, які можуть швидко ідентифікувати і нейтралізувати критичні проблеми в комп'ютерних системах, отримують величезні переваги, оскільки виведення з ладу цих мереж відіграватиме вирішальну роль у функціонуванні країни.

Науковий керівник – І.І.Пархоменко, к.т.н., доц.