УДК 621.263

Вадим Вячеславович Віщун
Андрій Володимирович Омельянчук

ТЕХНОЛОГІЯ ВИЯВЛЕННЯ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ШЛЯХОМ АНАЛІЗУ ІНФОРМАЦІЇ З ВІДКРИТИХ ДЖЕРЕЛ

Постановка проблеми. Аналіз останніх досліджень і публікацій

Сучасне людство є свідком динамічних глобальних світових змін, стрімкого переходу від індустріального суспільства до інформаційного, перебігу символічних економік провідних країн до суперсимволічних. Такі об'єктивні зміни вимагають оновлення форм, умов та способів праці у всіх, без виключення, спектрах діяльності людини, від легкого виробництва та аграрної промисловості до програмно-комп'ютерного забезпечення і космічних досліджень всесвіту.

Змінюються умови та фактори збройної боротьби, виникають інноваційні способи застосування збройних сил. Головна економічна вимога сучасності до війська – це підтримання боєздатності та дотримання принципів оборонної достатності. В арміях провідних країн світу виникають нові способи добування розвідувальної інформації, інформаційної підтримки управлінських процесів та рішень.

Динамічний інформаційний розвиток сучасного суспільства створив об'єктивні чинники для виникнення умов, коли все більше інформації, яка необхідна для прийняття рішення, можливо знайти у відкритих джерелах кіберпростору (Інтернету) [1].

Актуальністю уваги авторів статті до кіберпростору є те, що 16 травня 2011 року уряд Сполучених Штатів Америки (далі – США) прийняв Міжнародну стратегію діяльності у кіберпросторі (U.S. International Strategy for Cyberspace), що підтверджує факти рішучих намірів щодо активної діяльності у зазначеному напрямі.

За різними оцінками, з відкритих джерел кіберпростору американські розвідувальні служби добувають від 35% до 95% розвідувальної інформації. Така діяльність отримала назву OSINT – Open Source INTelligence (далі – OSINT) – (відкриті джерела розвідки). При цьому доля витрат на OSINT в розвідувальному бюджеті США складає приблизно 1%.

Формулювання мети статті. Виклад основного матеріалу

Збір розвідувальної інформації в OSINT суттєво відрізняється від інших напрямів розвідувальної діяльності, насамперед агентурної розвідки. При роботі з агентурними методами головна проблема полягає у добуванні інформації з джерела, що не завжди схильне до співпраці. В OSINT головним питанням є пошук змістовних та надійних джерел серед величезної кількості різноманітної інформації кіберпростору [2].

Орієнтовна методика пошуку інформації у відкритих джерелах за поглядами OSINT представлена рис. 1.

Рис. 1. Орієнтовна методика пошуку інформації у відкритих джерелах

Сутність її полягає у наступному: щоб отримати необхідну інформацію стосовно проблеми необхідно згенерувати якомога більшу кількість питань, згрупувати питання за характерними ознаками, встановити залежності між групами та окремими питаннями, здійснити пошук інформації по кожному з питань, проаналізувати джерела інформації на об'єктивність, новизну, достовірність тощо, відібрати найкращі джерела, систематизувати та структурувати інформацію.

В результаті ми отримаємо повну характеристику проблеми, що досліджується. Результати застосування даного підходу значно відрізняються від традиційного пошуку інформації безпосередньо по проблемі, що досліджується [3].

Для пошуку інформації у відкритих джерелах, представлених в мережі Інтернет, використовуються різні пошукові системи. Це універсальні пошукові системи, такі як Google, Yandex, Yahoo, Ask та спеціалізовані (для пошуку мультимедійного контенту: фотографії, ілюстрації, малюнки, відео та аудіо файли тощо), такі як TinEye та Bing. Кожна з представлених пошукових систем має власні механізми та синтаксис запитів, що значно спрощує процес пошуку інформації, аналізу та відбору джерел. Слід зазначити, що наведена методика роботи за принципами OSINT вже активно використовується у бізнес колах провідних країн світу для пошуку та отримання законними шляхами інформації про партнерів та конкурентів. Така діяльність набуває особливої уваги при проведенні політичних та передвиборчих кампаній.

В європейських країнах систематично відбуваються різноманітні курси, конференції та семінари з питань роботи з відкритими джерелами, записатись на які та пройти навчання, за відповідну оплату, можуть усі бажаючи. Так наприклад, швейцарські дводенні курси для відповідного бізнес-персоналу на даний час коштують 640 швейцарських франків (приблизно 5,5 тисяч гривень) [4].

На даний час існують програмні продукти, які розроблені за даною технологією [5]:

Maltego. Інструментарій використовується для аналізу зв'язків між людьми в соціальних мережах Twitter і Facebook, групами, веб-сайтами, доменами, мережами, частинами інтернет-інфраструктури і т.п.

Creepy. Працює під Windows і Linux і призначена для аналізу геолокаційних даних про користувачів на основі інформації із соціальних мереж, у тому числі Twitter і Flickr. Складені кластери дають можливість припустити координати місця проживання й місця роботи користувача.

Spokeo. Агрегатор, який аналізує інформацію з безлічі джерел, у тому числі телефонних довідників, соціальних мереж, фотоальбомів, маркетингових опитувань, даних державному перепису населення і т.п. Збираються демографічні дані, соціальні профілі, проводиться оцінка фінансового стану та володіння нерухомістю.

CaseFile. Молодший брат Maltego. Програма призначена для аналізу даних, які збираються в оффлайні, а не з відкритих джерел. Такими інструментами користуються слідчі та приватні детективи.

Recorded Future. Аналітичний інструмент, якій допомагає виявити тенденції у великих масивах неструктурованої інформації, витягаючи необхідні факти з Інтернету. За допомогою пропріетарних алгоритмів цей сервіс становить графіки з візуалізацією трендів у минулому, сьогоденні та екстраполяцією на майбутнє.

OSINT Opsec. Програмний серверний модуль. Цей інструмент призначено для ефективного моніторингу декількох найбільш важливих сайтів в Інтернеті. Програма здійснює пошук по ключових словах у свіжих публікаціях Pastebin, Facebook, Reddit, Twitter, Stackexchange, аналізує дані по ключових словах у реальному часі й генерує повідомлення, якщо знайдений збіг по тому або іншому ключовому слову. Програму можна використовувати для пошуку свіжих даних певного типу, оперативного повідомлення про витік інформації, а також відстеження рейтингу брендів. Автор програми зазначає, що люди "зливають" величезну кількість даних у відкритий доступ, залишається тільки структурувати цю інформацію: "Тут можна знайти копії паспортів, усі серійні номери, дати народження, імена і так далі". В 2009 році один з американських конгресменів у твіттері повідомляв про свої переміщення по Багдаду, а також як у тому ж твіттері співробітники корпорацій публікують інсайди про плановані корпоративні угоди. Теоретично, відслідковувати всі новини за ключовими словами можна за допомогою Google Alerts, але цей сервіс працює надзвичайно повільно та має ряд обмежень. Інструмент OSINT Opsec скачує контент на свій сервер де, в подальшому, можна реалізовувати для аналізу будь-який функціонал.

Як бачимо, можливості програмних продуктів, які реалізують технологію OSINT, мають велику потужність. Застосування їх на практиці, дозволить попереджувати служби інформаційної безпеки, не тільки про здійснення інформаційно-психологічного впливу на соціальні об'єкти, а також про здійснення кібератак на інформаційні системи інфраструктури держави.

Для пошуку уразливостей програмних продуктів та характерних ознак кібератак можна використовувати блоги спеціального призначення, де проводиться обмін досвіду між користувачами про вирішення проблем, що виникають при експлуатації програмних продуктів.

До промислового програмного продукту, який використовує принцип OSINT-пошуку, є – хмаровий сервіс Kaspersky Security Network. Даний програмний продукт використовує технологію OSINT приховано, пропонуючи кожному користувачу Інтернету перевірити невідомі дотепер експлойти, для порівняння їх із даними бази існуючих кіберзагроз.

Використання даної технології, дозволило "Лабораторії Касперского", опублікувати 14 серпня 2012 року результати перших досліджень про виявлення особливого комп'ютерного вірусу "Red October" [5].

Було виявлено, що протягом останніх п'яти років (починаючи з 2007 року) у різних країнах світу хакери зробили серію атак проти дипломатичних відомств, державних структур і науково-дослідних організацій (рис. 2).

Рис. 2. Площа розповсюдження вірусу "Red October"

У подібні організації вірус впроваджувався через конкретного користувача за допомогою фішингової пошти. Троян використовував уразливості, наявні, наприклад, в Microsoft Office і продуктах Adobe. Атаки ретельно готувалися, і в кожному конкретному випадку модуль вірусу допрацьовувався вручну з урахуванням специфіки користувача, через який здійснювалося зараження.

Зловмисники здійснили десятки успішних атак, викрали терабайти даних і при цьому залишилися фактично непоміченими для більшості жертв. Вірус, що має не менш 30 різних модулів, одержав від "Лабораторії Касперского" умовну позначку Backdoor.Win32.Sputnik. Він викрадає документи з різними розширеннями – від простого txt до acid – це розширення належить секретному програмному забезпеченню для шифрування "Acid Cryptofiler", яке використовується в структурах Євросоюзу й НАТО.

Використання фахівцями з кіберзахисту OSINT-технології дало б можливість попередити здійснення кібератаки Stuxnet на інформаційні системи атомної галузі Ірану, які відбулися у 2010 році. Так, при здійснені пошуку інформації щодо виявлення нового програмного продукту, його реєстрації та відтворенні картини розповсюдження за методикою OSINT, можна відслідковувати можливість здійснення шкідливих дій із різними типами інформаційних системам. Самим складним в даній методиці є формування бази даних програмних продуктів, які виявляються в закритих інформаційних системах. Адміністратори з безпеки не зацікавлені в розповсюдженні інформації щодо фактів таких випадків. До виправлення такої ситуації необхідно використовувати засоби соціальної інженерії, для проведення аналізу спілкування на закритих форумах, де дані адміністратори можуть бути зареєстровані.

Висновки

Таким чином, кіберпростір постає перед світовими державами не тільки як інноваційне поле для здійснення економічних та військових операцій, а й для проведення заходів із розвідувальної діяльності, для виявлення загроз їх інформаційній безпеці.

Література

1. Тоффлер Э. Война и антивойна. – М.:АСТ Транзиткнига, 2005. – с 240. **2. Модель** OSINT. Open Source в мире разведки. Режим доступу – http://www.perevodika.ru. **3. Search** Strategies – за матеріалами дводенних курсів International Security Forum/30 May – 1 June 2011/Zurich. **4.** За матеріалами сайту компанії "I-intelligence". Режим доступу – http://www.i-intelligence.eu. **5. Инструменты** для анализа данных из открытых источников. Режим доступу – http://www.xakep.ru/post/ 59590/default.asp. **6. Хакеры** 5 лет крали информацию у белорусских организаций. Режим доступу – http://euroradio.fm/ru/report/hakery-5-let-krali-informaciyu-u-belorusskih-organizaciy.

Изложены результаты по исследованию использования методики OSINT (поиска из открытых источников информации), предложен порядок использования методики OSINT для предотвращения проведения кибератак на ключевые элементы информационных систем критической инфраструктуры.

Ключевые слова: информационная безопасность, разведдеятельность, кибератаки.

The results of the study on the usetion techniques OSINT, proposed the use OSINT techniques for prevention of cyberattacks on key elements of critical infrastructure information systems.

Key words: information security, intelligence activities, cyberattacks.