Автоматизация процессов моделирования поведения судов в море и обнаружения структурированных аномалий являются актуальными задачами улучшения морской ситуационной осведомленности.

Кроме того, специальное программное обеспечение для выявления “аномалий” и обеспечения целостности и конфиденциальности сетевой информации, полученной из активов совместного использования разнообразных датчиков, становится ключевым инструментом для борьбы с киберпреступностью в морской сфере.

Шкідливе програмне забезпечення як знаряддя кіберзлочинності

Лефтеров Л.В.
Начальник другого відділу
УІТП в Південному регіоні Департаменту
Кіберполіції НП України

Влітку 2017 року електроні системи та мережі українських державних підприємств, банківських установ, приватних організацій та медіа-компаній припинили свою діяльність у результаті цілеспрямованих масштабних кібератак. В результаті цих атак була тимчасово заблокована діяльність сукупності об’єктів критичної інфраструктури держави, робота яких безпосередньо пов'язана з технологічними процесами або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення. Виведення з ладу або порушення функціонування таких структур може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду або становити загрозу для життя і здоров'я людей.

Зазначені кібер-інциденти, які відбулись на національному рівні, а також інші фактори, що несуть в собі загрозу інформаційної безпеки населення України, стали передумовами прийняття Закону України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017. Незважаючи на той факт, що Закон набере чинність лише у травні 2018 року, більшість підприємств та установ (незалежно від форми власності) вже активно вивчають показники, що використовуються для виявлення та реагування на кіберзагрози.

Вчинені атаки на українські системи стали можливі завдяки роботі шкідливого програмного забезпеченні (комп’ютерного вірусу типу Ransomware). Саме вірусне програмне забезпечення є основними знаряддям кіберзлочинності.

Шкідливе програмне забезпечення (далі ШПЗ) має багато різновидів, які виконують ту або іншу дію пов’язаною з незаконним отриманням інформації або блокування роботи електронно обчислювальної машини.

Так прийнято виділяти такі види шкідливих програм та компьютерних вірусів:

- Троянська програма. Основна особливість троянських програм – це замаскований збір конфіденційної інформації і передача третій стороні. До неї відносять реквізити банківських карт, паролі для платіжних систем, паспортні дані та інші відомості.
- Бекдор (Backdoor). Мета Backdoor - приховане управління комп'ютером, аж до можливості його перезавантаження, зміни мережевих підключень і доступу до реєстру системи.
- Дроппер (Dropper) - це програма що здійснює інсталяцію та встановлення шкідливого ПЗ на жорсткий диск видаленого комп'ютера. Додатковим видом вказаного ПЗ можна визначить – Downloader, який спрямовано на оновлення та завантаження додаткових комп’ютерних вірусів.
- Мережевих хробак (Worm) - різновид шкідливого ПЗ, який має властивість самостійно розповсюджуватись у мережах локального та глобального типів.
- Експлойт - це комп'ютерна програма або частина коду, яка шукає уразливі місця в програмному забезпеченні і в разі знаходження таких, отримує контроль над системою або порушує її роботу.
- Руткіт - програма або набір програм для приховування слідів присутності зловмисника або шкідливої програми в системі.

Комп’ютерні віруси розповсюджуються, копіюючи своє тіло і забезпечуючи його подальше виконання: впроваджуючи себе у виконавчий код інших програм, замінюючи собою інші програми, прописуючись в автозапуск через реєстр або інше.

Крім того слід зазаначити, що ШПЗ – є програмою, яка створена мовою програмування (асемблер, високорівнева мова програмування, скриптова мова) тому у коді однієї програми можуть

міститись як один вид ШПЗ так і функції одразу декількох вірусів. Також вказані шкідливі програмами мають змогу функціонувати комплексно, крок за кроком по черзі виконуючи окремі завдання установлені кіберзлочинцями.

Розповсюдження ШПЗ – здійснюється різними способами. Вірусом або його носієм можуть бути не тільки програми, що містять машинний код, а й будь-яка інформація, яка містить автоматично виконувані команди, - наприклад, пакетні файли і документи Microsoft Word і Excel, що містять макроси. Крім того, для проникнення на комп'ютер вірус може використовувати уразливості в популярному програмному забезпеченні (наприклад, Adobe Flash, Internet Explorer, Outlook), для чого розповсюджувачі впроваджують його в звичайні дані (картинки, тексти і т. д.) разом з експлойтом, що використовує вразливість.

Найпоширенішим способом розповсюдження комп'ютерних вірусів є пересилання шляхом електронно-комунікаційних додатків, електронної пошти, коротких повідомлень соціальних мереж, тощо. Нерідко з метою пересилки ШПЗ зловмисники використовують соціальну інженерію і підроблені сторінки популярних сайтів (а також кіберсквоттинг - реєстрація доменних імен, що містять торговельну марку, що належить іншій особі з метою їх подальшого перепродажу або несумлінного використання).

Відповідальність щодо захисту від шкідливого ПЗ, насамперед, лежить на самому користувачі. Для того щоб мінімізувати зараження персонального комп'ютера слід користуватися загальновідомими заходами захисту, а саме:

- своєчасне оновлення пакетів безпеки операційної системи компьютера
- уникнення змін системних файлів і встановлення програм з невідомих джерел;
- встановлення антивірусного програмного забезпечення
- створення резервних копій всіх важливих документів і файлів.

Література:

1. Закон України «Про інформацію» (Відомості Верховної Ради України (ВВР), 1992, N 48);
2. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 (Набрання чинності, відбудеться 09.05.2018);
3. The Petya ransomware is starting to look like a cyberattack in disguise / Russell Brandom [Електронний ресурс] // Vox Media. – 2017. – Режим доступу до ресурсу: https://www.theverge.com/2017/6/28/15888632/ petya-goldeneye-ransomware-cyberattack-ukraine-russia;
4. Defining Malware: FAQ / Robert Moir [Електронний ресурс] // Microsoft Corporation. - 2003 - Режим доступу до ресурсу: https://technet.microsoft.com/en-us/library/dd632948.aspx;
5. Типи шкідливих програм: від Trojan до Rootkit [Електронний ресурс] // Zillya. – 2015. – Режим доступу до ресурсу: http://zillya.ua/tipi-shkidlivikh-program-vid-trojan-do-rootkit.

Інформаційно-аналітичне забезпечення оперативно-розшукової діяльності Департаменту боротьби зі злочинами, пов'язаними з торгівлею людьми Національної поліції України

Мельнікова О.О.
викладач кафедри кібербезпеки та інформаційного забезпечення
Одеського державного університету внутрішніх справ

Проблеми інформаційно-аналітичного забезпечення оперативно-розшукової діяльності постійно розглядаються провідними українськими науковцями в контексті практичного удосконалення важливих напрямів протидії злочинності засобами ОРД. Вагомий внесок у розробку відповідних питань внесли К.В. Антонов, М. Бандурка, Б. І. Бараненко, Г.М. Бірюков, І.О. Воронов, В.Я. Горбачевський, В.О. Глушков, О.Ф. Долженков, В.П. Захаров, І.П. Козаченко, М.В. Корнієнко, В.А. Некрасов, Д.Й. Нікіфорчук, В.Л. Ортинський, М.А. Погорецький, Б.Г. Розовський, Е.В. Рижков, І.В. Сервецький, О.П. Снігерьов, В.Є. Тарасенко, М.Л. Шелухін, І.Р. Шинкаренко І.Ф. Хараберюш га багато інших науковців.

Розробка нових наукових підходів до модернізації засобів, методів та форм ОРД можлива лише з урахуванням активних процесів інформатизації суспільства, розвиток якого в умовах сьогодення визначається інтенсивністю інформаційних потоків. У сучасному світі основні матеріальні, енергетичні та організаційні ресурси актуалізуються саме з допомогою інформаційних можливостей і, таким чином, мають матеріально-енерго-інформаційний характер. їх цінність визначається перш за все цінністю