УДК 004.056.53

О.В. Сєвєрінов[1], А.Г. Хрєнов[1], А.О. Поляков[2]

[1] *Харківський університет Повітряних Сил імені Івана Кожедуба, Харків*
[2] *Харківський національний економічний університет імені С. Кузнеця, Харків*

АНАЛІЗ СУЧАСНИХ МЕТОДІВ АТАК НА АВТОМАТИЗОВАНІ СИСТЕМИ УПРАВЛІННЯ ВІЙСЬКАМИ ТА ІНФОРМАЦІЙНІ МЕРЕЖІ

У даній статті розглянуто методи реалізації сучасних атак на автоматизовані системи управління військами та інформаційні мережі. Проведено аналіз існуючих методів атак та на основі їх аналізу виявлено найбільш небезпечні типи атак.

Ключові слова: *автоматизовані системи управління військами, інформаційні мережі, захист інформаційних систем та мереж, види атак.*

Вступ

У сучасній високотехнологічній війні перемагає той, хто володіє інформацією, спроможний швидко виявити противника, провести ефективну оцінку обстановки та першим завдати удару. Це означає, що перевага в здобутті інформації та ефективності управління військами здатна забезпечити перемогу навіть над противником, який має значну перевагу.

Для цього провідні армії світу ефективно використовують сучасні автоматизовані системи управління військами та зброєю. Військові теоретики детально досліджують питання «інформаційного домінування», які підкріплені практичними дослідженнями [1].

На даний час в Україні також активно ведеться робота по створенню сучасні автоматизовані системи управління. Одними з основних в таких системах є питання захисту інформації та протидії атакам противника.

Сучасні методи реалізації атак на інформаційні системи надають можливість зловмисникам отримати доступ до конфіденційної інформації та нанести значних збитків.

Тому необхідно приділяти значну увагу безпеці у кіберпросторі під час експлуатації таких інформаційних та автоматизованих систем. При цьому однією із задач є аналіз можливих сучасних методів атак за допомогою яких зловмисник може отримати доступ до системи та скоїти свій задум.

Метою статті є проведення аналізу сучасних методів атак на автоматизовані системи управління військами та інформаційні мережі.

Класифікація сучасних методів атак

Інформаційні мережі та автоматизовані системи управління військами є предметом для атак з боку противника (хакерів) та шкідливого програмного забезпечення.

Методи за допомогою яких проводяться сучасні атаки можна поділити на три групи, а саме:

- «Віруси та черв'яки», коли шкідливе програмне забезпечення здатне додати свій код в інші програми або файли;
- «Трояни», що маскуються під нешкідливі, навіть корисні додатки, але наносять збитки інформаційній системі після інсталяції;
- «Мережеві атаки», спрямовані на вторгнення до інформаційної мережі з метою аналізу уразливостей та в подальшому нанесення удару по інформаційній системі.

Проведемо аналіз кожного з даних методів атак.

Віруси та черв'яки

Вірус – шкідлива програма, що здатна додати свій код в інші програми або файли [2].

Віруси досить швидко поширюються по інформаційній мережі та змінним носіям. У багатьох випадках мета вірусу – це ввести користувача в оману, щоб виконати шкідливі посилання, або завантажити шкідливі файли. У деяких випадках використовуються електронні поштові скриньки для ураження інформаційної системи.

1. Resident Virus.

Вірус, який живе в пам’яті цільового комп’ютера. Таким способом він активується кожного разу при включенні комп’ютера або виконанні певної дії.

2. Non-resident Virus.

За допомогою цього методу вірус активно шукає цілі для інфекції на локальній, змінній або мережевій локації. Цей тип вірусу не живе в пам’яті та існує при подальшому виявленні потенціальних цілей.

3. Boot sector Virus.

Вірус, що заражає завантажувальний сектор на жорсткому диску. Цей тип вірусів завантажується задовго до завантаження операційної системи на інфікованому комп'ютері та націлений на ураження файлової структури жорсткого диску.

4. Macro Virus.

Вірус, який написано на мові макросів, вбудований в Word, Excel, Outlook і інші документи. Він активується при відкритті інфікованого документу, через те, що за замовчуванням скрипти написані на мові макросів виконуються автоматично при відкритті документу.

5. File-infecting Virus.

Класична форма вірусу, коли інфікований файл, при виконанні інфікує інші файли в інформаційній системі.

6. Polymorphic Virus.

Цей тип вірусу є особливо важким для виявлення, через те, що після виконання використовує алгоритми шифрування та копіює себе у новий файл, тим самим підчищаючи сліди за собою.

7. Metamorphic Virus.

Вірус здатний змінювати свій код при кожному зараженні. Процес переписування призводить до різних заражень, але функціональність коду залишається незмінною.

8. Stealth Virus.

Вірус, який використовує різноманітні методи для запобігання виявленню, наприклад шляхом видаленням себе від заражених файлів та розміщення нової інфікованої копії в іншому місці.

9. Armored Virus.

Дуже складний тип вірусу, що використовує різні методи для захисту від антивірусного програмного забезпечення, дезорієнтує його, дає зрозуміти, що він розташований десь в іншому місці ніж є насправді.

10. Multipartite Virus.

Одночасно атакує завантажувальний запис жорсткого диску та файли, що виконуються. Тим самим при виявленні та видаленні може інфікувати інформаційну систему з завантажувального запису повторно.

11. Camouflage Virus.

Тип вірусу, який хибно повідомляє антивірусне програмне забезпечення та направляє його дію на ліцензійні програми.

Черв’як – вважається суб-класом вірусу та використовує уразливості операційної системи для поширення. Вони можуть поширюватися, дублюватися і розмножуватися, але на відміну від вірусів, черв’яки не вимагають прикріплення до файлу, або будь-якої виконуваної програми. Цей тип шкідливого програмного забезпечення можно класифікувати за типом поширення:

1. E-mail Worms.

Поширюються через електронну пошту, а саме через прикріплені файли у електронному листі.

2. Internet Worms.

Поширюються безпосередньо через мережу Інтернет, користуючись відкритими портами або уразливостями системи.

3. Network Worms.

Поширюються по відкритим, незахищеним інформаційним мережам.

4. Multivector Worms.

Мають два, або більше методів поширення.

До найбільш небезпечних атак можна віднести Boot sector Virus, Polymorphic Virus, Stealth Virus, Multipartite Virus.

Такі атаки можуть нанести значних збитків та витоку конфіденційної інформації, ці атаки маскуються та перешкоджають антивірусному програмному забезпеченню, що ускладнює процес виявлення та обеззараження інформаційної системи.

Трояни

Комп`ютерні трояни – це тип шкідливого програмного забезпечення, що маскується під корисний додаток або корисну програму, але насправді уражає цільову інформаційну систему після інсталяції [3].

Суттєвою різницею між вірусом та трояном є те, що троян не інсталюється самостійно, він вводить в оману користувача маскуючись під корисне програмне забезпечення. Троян може розповсюджуватися за допомогою електронної розсилки у вигляді посилання або прикріпленого файлу.

Розглянемо поширені типи троянів:

1. Remote Access Trojans (RAT) aka Backdoor.Trojan.

Цей тип трояна відкриває бекдор на інфікованій інформаційній системі, щоб дозволити зловмиснику отримати віддалений доступ або навіть повний контроль над системою.

2. Trojan-DDoS

Цей вид троянів встановлюється одночасно на велику кількість комп'ютерів з метою створення мережі зомбі (ботнет) машин, які будуть використані для реалізації DDoS атаки на конкретну цільову інформаційну мережу.

3. Trojan-Proxy.

Призначений для використання цільового коп'ютера як проксі-сервера, що дозволить виконати безліч операцій анонімно, навіть реалізувати подальшу атаку на мережу за допомогою ураженого комп'ютера.

4. Trojan-FTP.

Призначений для відкриття FTP портів, що дозволить отримати віддалений доступ до інфікованої системи та мережі в цілому, а також вікна для подальшого поширення різноманітних загроз.

5. Destructive Trojans.

Призначені для знищення або видалення даних на інфікованій інформаційній системі.

6. Security Software Disabler Trojans.

Цей вид троянів призначений для боротьби з антивірусним програмним забезпеченням шляхом зупинки програм безпеки, брандмауеру, IPS або відключенням процесів та служб.

7. Keylogger Trojans.

Троян, який призначений для зчитування та запам'ятовування інформації під час натискання клавіш на клавіатурі інфікованої системи та з подальшою передачею цієї інформації зловмиснику, що буде використана з метою викрадення таємних даних.

8. Trojan-PSW (Password Stealer).

Спеціально розроблений тип троянів, що використовується для крадіжки паролів на інфікованій інформаційній системі.

9. Trojan-Spy.

Призначений для шпигування за інформаційною системою, викрадення паролів, інформації про кредитні картки, секретної інформації, збирання скріншотів з коп'ютера та ведення інших шпигунських дій на ураженій системі.

10. Cryptolock Trojan (Trojan.Cryptolocker).

Новий тип троянів, що з'явився у 2013 році та призначений для шифрування та замикання окремих файлів на інфікованій системі.

Наслідки ураження інформаційної системи даним типом шкідливого програмного забезпечення можуть значно відрізнятися, від заміни робочого простору до відкриття бекдорів на інфікованому комп`ютері, що дозволить іншим вірусам уразити інформаційну систему або дозволить зловмиснику отримати віддалений доступ до комп'ютера, видалити важливі системні файли та форматувати жорсткий диск.

Мережеві атаки

У цьому випадку ми маємо справу з пасивним методом атаки, який застосовується для аналізу мережевого середовища, збору інформації щодо відкритих портів або інших вразливих місць інформаційної системи [4]. Залежно від процедур під час нападу або типу уразливості, мережеві атаки можуть бути класифіковані наступним чином:

1. Social Engineering.

Відноситься до психологічної маніпуляції людьми в інформаційній мережі. Мета полягає у несанкціонованому отриманні доступу до конфіденційної інформації, крадіжки даних, промислового шпигунства і переривання обслуговування.

2. Phishing attack.

Тип атак, що використовує соціальну інженерію для викрадення конфіденціальної інформації – найбільш поширена мета таких атак полягає у викраденні інформації щодо до кредитних карток жертви. Фішинг атака, як правило спочатку розповсюджують електронні листи, що ведуть користувачів на заражені сайти, які маскуються під банківські системи.

3. Social Phishing.

Мета такого типу атак полягає в отриманні конфіденційної інформації і отриманні доступу до особистих файлів. Засіб враження полягає у розповсюджені шкідливих посилань через мережу Інтернет та за допомогою обману переконання користувачів натиснути на такі посилання.

4. Spear Phishing Attack.

Тип атак, що орієнтований на конкретних осіб та на конкретні компанії. Мета такого типу атак полягає реалізації промислового шпигунства та крадіжки конфіденційної інформації.

5. Watering Hole Attack.

Найбільш складний тип атак, що базується на комплексному підході до ураження інформаційної системи конкретного користувача. Спочатку зловмисник вивчає звички потенційної жертви, збирає історію про відвідувані веб-сайти та обирає найбільш популярні портали, що мають вразливість у безпеці. Наступним кроком є інсталяція свого шкідливого коду або програми у такий веб-сайт.

6. Vishing (Voice Phishing or VoIP Phishing).

Тип атаки, що комбінує соціальну інженерію та телефонну систему. Зловмисник маскує номер телефону під реально існуючого абонента з адресної книги або під банківську установу та шляхом обману здобуває конфіденційну інформацію або банківські рахунки.

7. Port scanning.

Тип атаки де зловмисник сканує порти на цільовій інформаційній системі, щоб з'ясувати де знаходяться активні та відкриті порти з метою ураження системи шкідливими послугами, що пов'язані з конкретними портами.

8. Spoofing.

Тип атаки, що маскує зловмисника, програму або адрес під інший шляхом фальсифікації даних з метою несанкціонованого доступу до інформаційної системи.

9. Denial of Service Attack (DoS Attack) and Distributed Denial of Service Attack (DDoS Attack).

Атака пов'язана з призупиненням надання послуг або повною зупинкою інформаційної системи шляхом створення потужної активності фальсифікованих користувачів в системі та великої кількості запитів до бази даних, що призводить до завантаження відповідної інформаційної системи.

10. Ping of Death (PoD).

Атака, що базується на відправці спотвореного або шкідливого пінгу на цільову інформаційну систему з метою переповнення буферу.

11. Smurf Attack.

Атака яка повторює дії Ping of Death з маскуванням IP адреса зловмисника.

12. Bluesnarfing.

Атака, що дозволяє отримати доступ до інформації на пристрої за допомогою зв'язку Bluetooth. Будь-який пристрій з включеним режимом Bluetooth на «виявити» може бути схильним до такого типу атак.

Мережеві атаки не руйнують ресурси або дані. Активна фаза відбувається коли зловмисник застосовує комбінований метод і поєднує мережеву атаку з будь яким типом вище розглянутих атак.

Висновки

Трояни та мережеві атаки реалізуються через інформаційні мережі, опираючись на сучасні методи розповсюдження інформації при цьому користуючись знаннями соціальної інженерії. Ці методи реалізації атак на інформаційні системи не руйнують ресурси або дані, найбільш небезпечними їх можна вважати при використанні комбінованого методу, коли до ураженої цільової системи додають шкідливий вірус.

Віруси та черв`яки являються найбільш небезпечними методами реалізації атак зловмисника на інформаційні системи та мережі. Противники, які зможуть реалізувати цей тип атаки спроможні отримати інформацію, знищити дані та файли на цільовому робочому місці оператора, нанести пошкодження комплектуючим інформаційної мережі або системи та отримати повний доступ до керування окремим робочим місцем оператора.

На основі проведеного аналізу сучасних методів атаки на інформаційні системи та мережі можна виділити віруси та черв`яки, як найбільш небезпечні методи атак.

Серед яких Boot sector Virus, Polymorphic Virus, Stealth Virus, Multipartite Virus є особливо небезпечними методами атаки.

Такі атаки можуть нанести значних збитків та витоку конфіденційної інформації, ці атаки маскуються та перешкоджають антивірусному програмному забезпеченню, що ускладнює процес виявлення та обеззараження інформаційної системи.

Список літератури

1. Сайт http://nvo.ng.ru [Електронний ресурс]. – Режим доступу до матеріалу сайту: http://nvo.ng.ru/realty/2011-01-14/1_automate.html.

2. Сайт http://ru.wikipedia.org/ [Електронний ресурс]. – Режим доступу до матеріалу сайту: https://uk.wikipedia.org/wiki/Вірус.

3. Сайт http://ru.wikipedia.org/ [Електронний ресурс]. – Режим доступу до матеріалу сайту: https://uk.wikipedia.org/wiki/Троян.

4. Сайт http://ru.wikipedia.org/ [Електронний ресурс]. – Режим доступу до матеріалу сайту: https://uk.wikipedia.org/wiki/Мережеві_атаки.

Надійшла до редколегії 25.05.2015

Рецензент: д-р техн. наук, проф. І.В. Рубан, Харківський університет Повітряних Сил ім. І. Кожедуба, Харків.

АНАЛИЗ СОВРЕМЕННЫХ МЕТОДОВ АТАК НА АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ ВОЙСКАМИ И ИНФОРМАЦИОННЫЕ СЕТИ

А.В. Северинов, А.Г. Хренов, А.А. Поляков

Рассмотрены методы реализации современных атак на автоматизированные системы управления войсками и информационные сети. Проведен анализ существующих методов атак и на основе их анализа обнаружены наиболее опасные типы атак.

Ключевые слова: *автоматизированные системы управления войсками и информационные сети, защита информационных систем и сетей, виды атак.*

ANALYSIS OF MODERN METHODS OF ATTACKS ON INFORMATION SYSTEMS AND INFORMATION NETWORKS

O.V. Severinov, A.G. Khrienov, A.O. Polyakov[2]

This article deals with modern methods of implementing attacks on automated command and control and information networks. The analysis of existing methods of attacks and techniques based on the analysis revealed the most dangerous types of attacks.

Keywords: *automated control of troops and information network, protection of information systems and networks, the types of attacks.*