УДК004.056

Інна Стеценко, Дмитро Огородников

МОДЕЛЮВАННЯ СЦЕНАРІЮ КІБЕРАТАКИ НА ОСНОВІ АТАКИ «PETYA», «NOTPETYA»

У статті описаний сценарій кібератак на основі вірусів шифрувальників. За результатом аналізу сценарію можна класифікувати більшість кібератак на інформаційні системи.

Ключові слова: кібератака, інформаційні системи, комп'ютерний вірус, життєвий цикл, шифрувальник.

Рис.: 6. Табл.: 1. Бібл.: 6.

The article describes a cyberattack script based on encrypted viruses. As a result of the scenario, most cyberattacks can be classified into information systems.

Keywords:cyberattack, information systems, computer virus, life cycle, encryptor.

Fig.: 6. Tabl: 1.Bibl.: 6.

Актуальність теми дослідження. Повідомлення «Виявлено поширення банківського вірусу трояна», «На державних пристроях виявлена програма для кібер-шпигунства», «Виявлений вірус, який вже заразив п'ять мільйонів пристроїв», «Ботнет навчився перетворювати пристрої на проксі-сервери» стали звичайними новинами тижня. Від шкідливих програм потерпають все частіше державні та фінансові установи, а кібертероризм порівнюють зі зброєю масового знищення. Загрози, які несуть злочини в інформаційному просторі, є небезпечними для транспортних, енергетичних, виробничих систем. Розуміння процесів, які відбуваються при запуску шкідливого програмного забезпечення, є необхідним кроком для розробки систем інформаційного захисту. Тому дослідження кібератак з метою визначення шляхів їх поширення є актуальною задачею.

Постановка проблеми. Для реалізації своїх цілей кіберзлочинці використовують спеціальне програмне забезпечення. Для доступу до особистих інформаційних ресурсів жертви злочинці використовують комп'ютерні віруси, ботнети або мережеві хробаки, які здійснюють копіювання, модифікацію та знищення інформації. Основними цілями кібератак є:

– отримання доступу до державних і військових секретів, а також банківської та особистої інформації (наприклад, вірус Red October);

– нанесення збитків окремим фізичним елементам інформаційного середовища (наприклад, мережевий хробак і ботнет Mirai);

– крадіжка чи знищення інформації методами обходу систем захисту і впровадження стороннього програмного забезпечення (наприклад, вірус Wanna Cry);

– захоплення каналів розповсюдження інформації;

– створення перебоїв у мережах комунікацій.

Виявлення та протидія кіберзагрозам в сучасних інформаційних системах спираються на вже відомі атаки. Проте кіберзлочинці постійно вишукують нові інструменти та розробляють нові програми, яким не можуть протидіяти системи

інформаційного захисту. Систематизація та узагальнення інформації про шкідливі програми та способи їх використання в кібератаках є важливим ресурсом для розробки нових систем інформаційного захисту.

Аналіз останніх досліджень і публікацій. На сьогоднішній день існує достатньо багато наукових досліджень, що стосуються моделювання кібератак та їх сценаріїв. Моделювання DoS/DDoS/DRDoS атак з урахуванням структури мережі та вагових коефіцієнтів, які оцінюють рівень загрози атаки, розглянуто в роботі «Атаки на відмову в обслуговуванні комп'ютерних мереж»[4]. Результати моделювання пропонується враховувати під час проектування систем інформаційного захисту. В роботі «Impact Analysis of Faults and Attacks in Large-Scale Networks»[5] для аналізу безпеки на основі глобальних показників після існуючих ситуацій з ураженням використовують графи і дерева атак. Дослідження слабких місць, політик безпеки, конфігурацій, списків програмного і апаратного забезпечення, встановлених на кожній платформі, події і міри, які можна використати для запобігання, представлено в публікації Common Vulnerabilities and Exposures [6].

Виділення недосліджених частин загальної проблеми. У схемі не розглянуті проблеми, що описує життєвий цикл атак від спроби заподіяння шкоди успішному ураженню до маніпуляціям даних.

Постановка завдання. Для передбачення дій кібернападника необхідні методи, які можуть аналізувати його попередні дії та на їх основі визначати (з певною достовірністю) кінцеву ціль атаки та наступні його дії. Аналіз сценарію кібератаки поділяється на три етапи: 1) класифікація атаки; 2) визначення основних кроків атаки; 3) моделювання та аналіз результатів. За результатом аналізу сценарію можуть бути розроблені інструментальні засоби виявлення відомих атак вже на перших їх кроках.

Викладення основного матеріалу.Класифікацію атак можна здійснювати, конкретизуючи ознаку, за якою виконується класифікація. Виділимо такі ознаки: характер взаємодії, цілі взаємодії, умова початку здійснення атаки, наявність зворотного зв’язку з об’єктом атаки, розташування відносно об’єкту атаки.

За характером взаємодії розрізняють атаки пасивні та активні. При виконанні активних атак, порушник виконує активні дії, які пов’язані зі зміною потоків даних. При пасивних атаках шкідливий програмний код розміщується, наприклад, у просторі інтернету, і порушник сподівається, що жертва самостійно через неуважність (атаки методом фішингу) виконає запуск шкідливого коду.

За цілями взаємодії розрізняють атаки, які спрямовані на порушення конфіденційності, цілісності або працездатності інформації.

За умовою початку здійснення вирізняють атаки за запитом від жертви, безумовну атаку та атаку з урахуванням умов. Атаку за запитом від жертви можна вважати продовженням пасивної атаки. Після переходу на шкідливий ресурс відбувається «добровільний» запуск шкідливого програмного коду. Безумовною є атака без дослідження систем захисту жертви. Атака з урахуванням умов виконується на основі визначення коефіцієнту успішності проведення атаки.

За наявністю зворотного зв'язку з об'єктом атаки атаки можна поділити на атаки зі зворотнім зв'язком та однонаправлені атаки.

Одним із основних факторів атаки є місце розташування суб'єкту атаки, тому розрізняють зовнішню та внутрішню атаки. При внутрішній атаці порушник може знаходитися одразу в системі, наприклад, як співробітник компанії, або мати доступ до внутрішньої мережі від самого початку. При зовнішній, - порушнику потрібно спочатку оминути зовнішній захист.

Схема класифікації атак представлена на рисунку 1.

Рис. 1. Класифікація кібератак.

Атаки можна розділити на вісім класів за уразливими місцями операційної системи:

1) «соціальна інженерія» - атака, яка направлена на введення жертви в оману;

2) «запозичення прав» - атака, яка має на меті захоплення прав авторизованих користувачів;

3) «використання» - використання вразливостей програмного забезпечення чи операційної системи;

4) «відносна (оманлива) довіра» - використання довіри до мереж чи сайтів;

5) «атаки управлінням даними» - троянські програми, віруси, хробаки;

6) «інфраструктурна вразливість» - використання особливостей стандартів, специфікацій;

7) «відмова в обслуговуванні» - атака, яка направлена на перешкоджання використанню системи;

8) «чародійство» - невідома атака, яка ще не зафіксована або не розшифрована.

Характер кібератаки, у більшості випадків, можна визначити за класом атаки та її спрямованістю. Часто одна атака може бути відволіканням уваги від іншої атаки. Найбільш розповсюдженими атаками в мережі інтернет, а також найбільш простими та, водночас, найбільш ефективними серед усіх методів зараження пристроїв є атаки розповсюдження стороннього програмного забезпечення [3], які використовують, наприклад, для майнінгу криптовалюти, створення ботнета, інформаційного збирання (особистих та банківських даних, в тому числі, паролів).

Планування і реалізація кібератаки складається з кількох етапів. На етапі збору інформації (рис. 2) здійснюється втручання в мережу методами шкідливого коду або використанням навичок, які мають вузький профіль (використання певних мов програмування, вразливих місць специфікацій і стандартів). На наступному етапі відбувається ураження пристрою, який є ціллю кібератаки (рис. 3). Після вдалого враження пристрою відбувається етап маніпуляції з даними та виконання функцій розповсюдження атаки (рис. 4, таблиця 1).

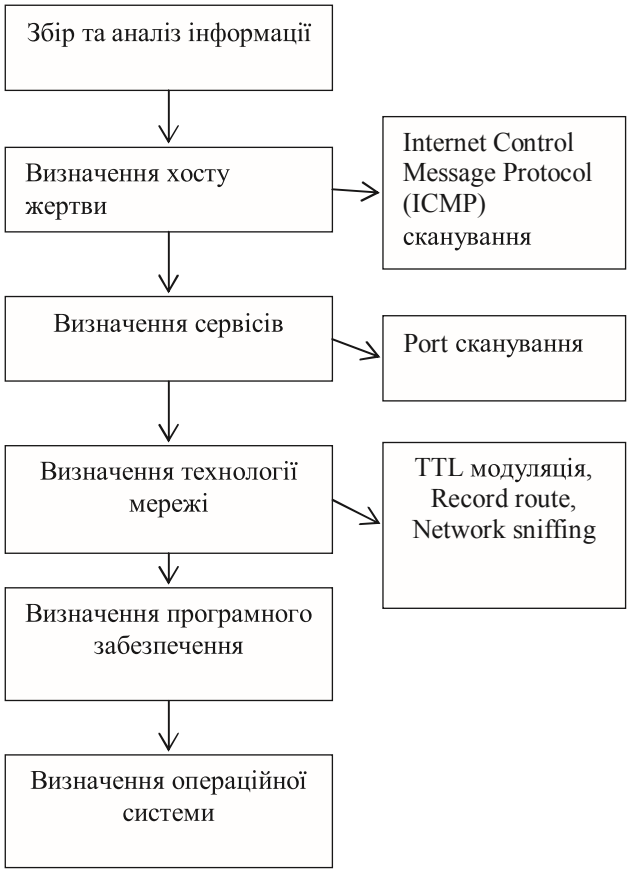

Рис. 2. Етап розвідки. Збір і аналіз інформації.

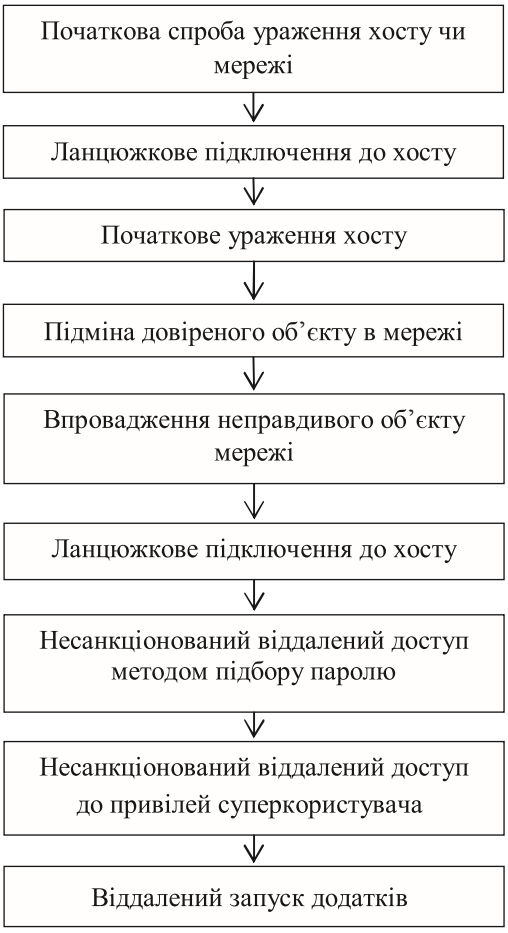

Рис. 3. Етап ураження пристрою чи мережі

Рис. 4. Етап розповсюдження атаки

Таблиця 1

Послідовність дій в ураженій системі

Функція	**Технологія і методи**
Видалення початкових слідів зламу	Самописні методи
Створення відкритого каналу з джерелом атаки	Дешифрування паролів. Встановлення захищеного прихованого каналу
Створення пріоритету процесів	Зараження системи, створення багатьох процесів у ОС
Несанкціоновані дії. Копіювання, видалення, змінення інформації	Використання шифрувальних технологій
Розповсюдження атаки	Дешифрування паролів, атаки через раніше встановлені/відкриті канали

Опис сценарію кібератаки «Petya», «NotPetya». Зразок вірусу має функцію крипто-шифрувальника [2]. Він шифрує файли з конкретним розширенням, потім перезаписує місце MBR (master boot record), очищує журнали (системний каталог), виконує перезавантаження системи. Після цього виводить повідомлення про умови дешифрування, в даному випадку, викуп.

Етап 1 «Зараження». Основним методом розповсюдження вірусу стали масові посилання, котрі розповсюджувались за допомогою електронної пошти [1]. Посилання атаки «фішингу»: користувач відкриває отриманий файл-вкладення на пошті, і виконується інфікування. Наступним кроком розповсюдження є локальний метод технології LAN, спрямований на ураження пристрою-сусіда.

Вірус отримує дані аутентифікації, використовуючи функцію CredEnumerate та допоміжне функціонування mimikatz. Далі вірус розповсюджується по мережі,

запускаючи функції admin $ (рис. 5) та PsExec.exe для віддаленого доступу до виконання команд, і функцію wmic.exe для доступу до інструментарію управління Windows [2]. Оскільки вказані функції доступні лише в сімействі операційних систем Windows, то на інших операційних системах запуск вірусу не результативний. Вірус також намагається отримати доступ до «SMB EternalBlue» і «EternalRomance», перевіряючи вразливі для зараження місця через TCP-порти.

```
wsprintfW(&Name, L"\\\\%s\\admin$", a1);
NetResource.dwScope = 0;
memset(&NetResource.dwType, 0, 0x1Cu);
NetResource.lpRemoteName = &Name;
NetResource.dwType = 1;
sub_10008B70((int)&v23);
wsprintfW(&FileName, L"\\\\%ws\\admin$\\%ws", a1, &v23);
while ( 1 )
{
  pszPath = 0;
  v11 = v4;
  v10 = WNetAddConnection2W(&NetResource, lpPassword, lpUserName, 0);
```

Рис. 5. Виклик функції ОС Windows admin $

При завантаженні вірус перевіряє наявність у системі файлу «C:\Windows\perfc». Якщо файл існує, то вірус завершує виконання (для зупинки зараження вже інфікованого пристрою). Вірус має також систему маскування. Комп'ютер сканується на активні процеси в операційній системі за хеш-кодуванням:

- 0x2E214B44 - «avp.exe» – it's Kaspersky AntiVirus - Kaspersky Internet Security;
- 0x6403527E - «ccSvcHst.exe» – Symantec Service Framework;
- 0x651B3005 - «NS.exe» – Norton Security.

При виконанні цих процесів вірус припиняє своє функціонування. Це виконується через загрозу програми бути ідентифікованою як вірус і видаленою з системи.

Етап 2 «Шифрування». Для шифрування вірус отримує випадкові дані через функцію CryptGenRandom, яка вважається криптографічною стійкою функцією.

Вірус записує у початок диску код-виклику функції, яка запускає ланцюжок шифрування лише після перезавантаження пристрою. Після перезавантаження функція шифрує MFT(головну файлову таблицю) системи, - це база даних, в якій зберігається інформація про вміст дискового розділу з файловою системою NTFS. Приблизний алгоритм шифрування MFT описується за процедурою:

- Зчитується сектор 0x20.
- Встановлюється позначення шифрування MFT.
- EncryptionKey копіюється у тимчасовий буфер.
- Поле з EncryptionKey записується нульовими байтами.
- Сектор 0x20 записується на диск.
- Зчитується сектор 0x21.
- Його вміст шифрується EncryptionKey + нулі.
- Змінений сектор 0x21 перезаписується на диск.

Коли всі файли зашифровані, пристрій знову перезавантажується і виконує текст вимоги викупу з полем для дешифрування. Шифрувальних шифрує файли з такими розширеннями [2]: .3ds .7z .accdb .ai .asp .aspx .avhd .back .bak .c .cfg .conf .cpp .cs .ctl .dbf .disk .djvu .doc .docx .dwg .eml .fdb .gz .h .hdd .kdbx .mail .mdb .msg .nrg .ora .ost .ova .ovf .pdf .php .pmf .ppt .pptx .pst .pvi .py .pyc .rar .rtf .sln .sql .tar .vbox .vbs .vcb .vdi .vfd .vmc .vmdk .vmsd .vmx .vsdx .vsv .work .xls .xlsx .xvd .zip.

Відповідний фрагмент коду представлений на рисунку 6.

```
if ( !(FindFileData.dwFileAttributes & 0x10) || FindFileData.dwFileAttributes & 0x400 )
{
  v5 = (struct _WIN32_FIND_DATAW *)PathFindExtensionW(FindFileData.cFileName);
  if ( (WCHAR *)v5 != &FindFileData.cFileName[wcslen(FindFileData.cFileName)] )
  {
    wsprintfW(&v10, L"%ws.", v5);
    if ( StrStrIW(
           L".3ds.7z.accdb.ai.asp.aspx.avhd.back.bak.c.cfg.conf.cpp.cs.ctl.dbf.disk.djvu.doc.docx.dwg.eml.fdb."
            "gz.h.hdd.kdbx.mail.mdb.msg.nrg.ora.ost.ova.ovf.pdf.php.pmf.ppt.pptx.pst.pvi.py.pyc.rar.rtf.sln.s"
            "ql.tar.vbox.vbs.vcb.vdi.vfd.vmc.vmdk.vmsd.vmx.vsdx.vsv.work.xls.xlsx.xvd.zip.",
           &v10) )
    {
      encrypt_file__sub_1000189A(&FileName, a3);
    }
  }
}
else if ( !StrStrIW(L"C:\\Windows;", &FileName) )
{
  encrypt_files_in_directory__sub_10001973(&FileName, a2 - 1, a3);
}
```

Рис. 6. Фрагмент коду віруса-шифрувальника Not-Petya
(вказано розширення файлів для шифрування)

Алгоритм шифрування схожий на алгоритм шифрувальника Salsa20, котрий виконує операції шифрування конкатенації 32-ти бітних чисел, побітову конкатенацію по модулю(XOR) і побітові зсуви, але був модифікований.

Ключ дешифрування повинен складатися з набору латинських символів і чисел розміром у 32 символи. Хеш-функція, наприклад, функція (SPONGENT), отримує на вхід деяку кількість байт і видає значення у розмірі 32 байта. Після цього алгоритм повторюється 128 разів і результат отримується як EncryptionKey.

Етап 3 «Розповсюдження». Розповсюдження вірусу виконується через виклик вірусом системних функцій «GetExtendedTcpTable», «GetIpNetTable», «NetServerEnum», «WNetEnumResource», «DhcpEnumSubnets», «DhcpEnumSubnetClients» для створення списку мережевих хостів.

Етап 4 «Видалення слідів». Після успішного шифрування вірус очищує системні журнали, викликавши команду WEVTUTIL, і перезавантажує пристрій. Перезавантаження виконується через виклик функцій «NtRaiseHardError», «InitiateSystemShutdownExW» та «ExitWindowsEx».

Висновки. В цілому, сценарій кібератаки складається з таких етапів:

- Атака на пристрій. Спроба стороннього програмного забезпечення отримати доступ до об’єкту атаки. У випадку успіху виконується наступний етап. У випадку невдачі, атака повторюється іншим методом або на інший пристрій.

- Зараження. Безперешкодний запуск шкідливого скрипта чи програми на пристрої. Ураження мережі та виконання команд для отримання прав суперкористувача.
- Приховування слідів зараження (залежить від типів атак). Приховування слідів ураження пристрою для успішного виконання шкідливого коду. Приховування коду від програм захисту/антивірусів.
- Виконання шкідливого коду (маніпуляція з даними). Запуск скрипта і виконання поставленої мети атаки. Шифрування даних, копіювання, видалення. Встановлення допоміжних каналів для розповсюдження зараження.
- Видалення слідів перебування (залежить від типів атак). Отримання результату від атаки, видалення логів та інформації з системних журналів, видалення підозрілих файлів.
- Розповсюдження (залежить від типів атак). Розповсюдження атаки у мережі через встановлені канали передачі. Створення ботнету. Розповсюдження спам-листів і повідомлень з посиланням на файл вірусу.

Виявлення шкідливих програм на комп'ютерному пристрої не дає можливості визначити кінцеву мету атакуючого. Моделі сценаріїв кібератак представляють не тільки вразливості інформаційної системи, які використовують кіберзлочинці, але й визначають послідовність дій, спрямовану на досягнення кінцевої мети. В подальшому моделі сценаріїв кібератак мають бути реалізовані з урахуванням перебігу часу, що надасть можливість оцінювати час розповсюдження кібератаки в розподіленій інформаційній системі.

Список використаних джерел

1. Огородников Д.В. Методи зовнішнього втручання у технології передачі даних Інтернет-речей // Інтернет речей: проблеми правового регулювання та впровадження : Матеріали науково-практичної конференції. 24 жовтня 2017 р., м. Київ. / Упоряд. : В. М.Фурашев, С. Ю. Петряєв. – Київ : Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського» Вид-во «Політехніка». 2017. - С. 101-105.

2. ISSP REPORT "PETYA" – "NOTPETYA" REVERSE ANALYSIS [Електронний ресурс] (2017) – Режим доступу: https://issp.ua/issp_system_images/Petya-NotPetya-Reverse-by-ISSP-Labs.pdf

3. THE WEB APPLICATION SECURITY CONSORTIUM THREAT CLASSIFICATION 01.01.2010 [Електронний ресурс] - Режим доступу: http://projects.webappsec.org/f/WASC-TC-v2_0.pdf

4. Карпінський М. П. Атаки на відмову в обслуговуванні комп'ютерних мереж / М. П. Карпінський, У. О. Яциковська, А. В. Балик, М. Александер // Вісник Національного університету "Львівська політехніка". Комп'ютерні системи та мережі. – 2014. – № 806. – С. 94-99.

5. Hariri S. Impact Analysis of Faults and Attacks in Large-Scale Networks / S. Hariri, G. Qu, T. Dharmagadda, M. Ramkishore, C.S. Raghavendra // IEEE Security and Privacy. - Vol. 1, 2003. - P. 49-54.

6. Common Vulnerabilities and Exposures (CVE) [Електронний ресурс] – Режим доступу: http://cve.mitre.org/.

ДОВІДКА ПРО АВТОРІВ

Стеценко Інна Вячеславівна – доктор технічних наук, професор кафедри автоматизованих систем обробки інформації і управління, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського».

Inna Stetsenko – professor, Departament of Automated Systems of Information Management and Management, National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”.

E-mail: i.stetsenko@kpi.ua

Огородников Дмитро Володимирович – студент, кафедра автоматизованих систем обробки інформації і управління, Національний технічний університет України «Київський політехнічнийінститут імені Ігоря Сікорського».

Dmytro Ohorodnykov – student, Department of Computer-Aided Management and Data Processing System, ASOIU,National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”.

E-mail:swarty16@gmail.com

Inna Stetsenko, Dmytro Ohorodnykov

MODELING SCENARIO OF CYBERATTACK BASED ON “PETYA”, “NOTPETYA” ATTACK

Target settings. Illegal actions aimed at violating the safety of an individual, a society or a state, methods used to relate material objects-obtaining unauthorized access, altering or breaking the integrity of information to gain an advantage in solving political economic or social problems are now defined as cyberterrorism. In consequence, the actual task to prevent attacks is to simulate the steps of actions that are performed at the attack.

Actual scientific researches and issues analysis. With the tendency of increasing the amount of information in the Internet network, the protection of information from unauthorized persons became a very topical issue. There are many articles that describe the specific attacks that vulnerabilities use, what they do with the information after a successful access to it, but the overall picture of the attack scenarios is not described.

Uninvestigated parts of general matters defining. There are no issues in the schema that describes the life cycle of attacks from attempted damage to successful lesion and data manipulation.

The research objective. The purpose of the study is to create a cyberattack script based on the popular Petya and NotPetya encryption viruses.

The statement of basic materials. The life cycle of the cyberattack's "Notpetya" was studied, on the basis of which a cyberattack script was created, by type of virus encryption-extortionists.

Conclusions. Was created the classification scheme of cyber attacks, attacks were divided into classes, simulated cyberattack life cycle, created cyberattack scene.

The script for cyberattacks consists of the following steps:

• Attack on the device. An attempt by third-party software to access an attack object. In case of success, the next stage is fulfilled. In the event of a failure, the attempt is repeated by another method or another device.

• Infection. Unhindered launch of a malicious script or program on your device. Defeat the network and execute commands to obtain superuser privileges.

• Hiding traces of infection (depending on the types of attacks). Hiding traces of device damage to successfully execute malicious code. Hiding code from security / antivirus software.

• Fulfilling the malicious code (manipulation with data). Run the script and execute the target attack target. Data encryption, copying, deletion. Installation of auxiliary channels for the spread of infection.

• Removing traces of stay. (depends on the types of attacks). Obtaining the result from an attack, deleting logs and information from system logs, removing suspicious files.

• Distribution. (depends on the types of attacks). Distribution of attack on the network through established channels of transmission. Create a botnet network. Distribution of spam emails and messages with a link to a virus file.

Detection of malware on a computer device does not provide an opportunity to determine the ultimate goal of the attacker. The models of cyberattack scenarios represent not only the vulnerabilities of the information system that use cybercriminals, but also determine the sequence of actions aimed at achieving the ultimate goal.

In the subsequent model scenario, cyberattacks should be implemented withtaking into account the current time, which will give an opportunity to estimate the time. Distribution of cyberattacks in distributed information system.

Keywords:cyberattack, information systems, computer virus, life cycle, encryptor.