МОДЕЛІ І МЕТОДИ RANSOMWARE АТАК В КІБЕРПРОСТОРІ

Федюшин О.І., Ковальчук Д.Ю.
Харківський національний університет радіоелектроніки, Харків, Україна

В роботі розглянуті моделі і методи Ransomware атак в кіберпросторі.

Об'єктом дослідження є процес розпізнавання діяльності Ransomware атак в кіберпросторі.

Предмет дослідження – моделі і методи реалізації Ransomware атак.

Ransomware – це зловмисне програмне забезпечення, призначене для заборони доступу користувача або організації до файлів на їх комп'ютері. Шифруючи ці файли та вимагаючи викупу за ключ дешифрування, кібератаки ставлять організації в положення, коли сплата викупу є найпростішим і найдешевшим способом відновити доступ до своїх файлів[1,2]. Деякі варіанти атак додали додаткові функції, такі як крадіжка даних, щоб заохочувати жертв програм-вимагачів платити викуп. Програми-вимагачі швидко стали найпоширенішим і найпомітнішим типом шкідливих програм.

Щоб захиститись від зараження програмами-вимагачами, рекомендується зберігати пильність та використовувати програми безпеки. У жертв програм-здирників є три варіанти дій після зараження: можна заплатити викуп, спробувати видалити шкідливу програму або перезавантажити пристрій. Вектори атак, що використовуються троянами-здирниками, включають, в основному, протокол віддаленого робочого столу, фішингові повідомлення електронної пошти та вразливість програмного забезпечення [3].

В роботі розглянуті такі сімейства програм-вимагачів, а саме: Ryuk, Maze, REvil (Sodinokibi), Lockbit, DearCry, Lapsus$. Загалом вони відносять до типів вірус Locker та крипто-вимагач. Головна ідея вірусу Locker- це блокування робочого стола та покриття його банером з вимогою викупу. Крипто-вимагач – шифрує файли та змінює їх розширення, для розшифрування потрібно заплатити викуп. Сучасні варіанти програм-вимагачів зазвичай викрадають конфіденційні дані компанії перед їх шифруванням. В дослідженні проаналізовані основні вектори атак та способи їх детектування, розроблений фреймворк для класифікації та оцінки наслідків їх злочинної діяльності.

Список літератури

1. Liska A. Ransomware. Defending Against Digital Extortion / A. Liska, T. Gallo., 2017. – 174 с.

2. A. Hassan N. Ransomware Revealed / Nihad A. Hassan., 2019. – 229 с.

3.A. Grimes R. Ransomware. Protection Playbook / Roger A. Grimes., 2022. – 323 с.