УДК 004.056.57
Зайко Т.А.[1], Сокол Р.В.[2]
[1] канд. техн. наук, доц. НУ «Запорізька Політехніка»
[2]студ. гр. КНТ-128 НУ «Запорізька Політехніка»

ЗАХИСТ ВІД ПРОГРАМ-ВИМАГАЧІВ

У часи повної автоматизації систем, як банківських, так і державних, окрім ергономічності та автономності, важливо приділяти не меншу увагу і до питань безпеки й надійності цих самих систем, бо через це дуже збільшився процент програм-вимагачів та шахраїв.

Згідно зі статистикою ресурсу Purplesec шкода завдана програмами-вимагачами росте дуже швидко, протягом часу. Якщо у 2018 році збитки від такого ПЗ були близько 8 мільйонів доларів, то у 2020 році ця цифра збільшилась вже до 20 мільйонів доларів на рік.

Програма-вимагач – це шкідливе програмне забезпечення, яке шифрує важливі файли на вашому ПК, щоб зробити їх недоступними, і погрожує опублікувати або видалити їх, якщо не буде виплачена певна грошова сума (викуп). Але навіть після виплати викупу немає ніяких гарантій, що ви зможете відновити свої файли або знов отримати доступ до вашого комп'ютера [1].

Найчастіше таке ПЗ потрапляє на комп’ютер користувача через e-mail. Зазвичай він починається з класичного фішингового електронного листа, який служить приманкою для завантаження зараженого файлу. У більшості випадків зараження програмою-вимагачем відбувається через відкриття прикріпленого PDF, DOC або XLS файлу. Відображення розширень файлів за замовчуванням деактивовано в більшості поштових клієнтів, тому

користувач, як правило, не може розпізнати формат файлу, на перший погляд [2].

Також популярним способом потрапляння програм-вимагачів на девайси є завантаження зараженого файлу з мережі інтернет або встановлення неліцензійного програмного забезпечення, що насправді являє собою вірус.

Відкриття шкідливого файлу, є безповоротним моментом, бо після цього проводиться установка на відповідну систему програми-вимагача. Як тільки активується програма-вимагач, починається фактична шкода: розпочинається процес шифрування. Окремі файли в одній системі або навіть декількох системах в межах мережі локальної можуть бути зашифровані. Відтепер користувач більше не має доступу до певних файлів або до всього свого комп'ютера. Він повністю втратив свої права адміністратора. Контроль знаходиться в руках хакера.

Як тільки все зашифровано, на екрані жертви з'являється повідомлення. Тут хакер вимагає викуп, щоб повернути користувачу доступ до файлів. Після чого зловмисникам залишається лише чекати, поки жертва заплатить викуп.

Для захисту від програм-вимагачів необхідно розробляти план кібербезпеки від шкідливих програм. Оскільки таке ПЗ дуже важко виявити та боротися з ними, для боротьби з ним слід використовувати різні механізми захисту. Найважливіший захист - це навчання та сенсибілізація працівників [3]. Але, звісно, вивчення проблеми є актуальним не лише для працівників компаній та і для пересічних користувачів ПК та мережі інтернет, бо обізнаність дозволяє утримувати проблему від себе як можна далі.

Якщо ж комп'ютер був вражений програмою-вимагачем, то найпростішим рішенням буде резервна копія вашої системи. Таким чином можна завантажити стару версію без зараження. Це зменшує втрату даних якомога менше. Резервне копіювання можна зробити вручну або автоматично. Хмарне рішення для компаній стане чудовою можливістю для резервного копіювання даних[2].

На мою думку, найкращим захистом від програм-вимагачів – є комплексний підхід до цієї проблеми, а саме: використовувати антивіруси, що мають функції відстеження таких програм, вивчати та бути у курсі того, які програми вимагачі існують та що вони собою уявляють і у разі отримання підозрілих листів поводитися логічно та раціонально, не піддаючись на хитрощі шахраїв. Також не малу частину захисту від такого роду ПЗ буде раціональне використання інтернет-ресурсів, які ви відвідуєте та дуже ретельна фільтрація ресурсів з яких будуть завантажені будь-які файли.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. AVAST “Защита от программ-вымогателей: часто задаваемые вопросы [Электрон. ресурс]. – Режим доступа : https://support.avast.com/ru-ua/article/Antivirus-Ransomware-Shield-FAQ/

2. ESET “Програми-вимагачі”. [Електрон. ресурс]. – Режим доступу : https://www.eset.com/ua-ru/support/information/entsiklopediya-ugroz/programma-vymogatel/

3. Hornetsecurity “Ransomware” [Electronic resource]. – Access mode : https://www.hornetsecurity.com/en/knowledge-base/ransomware/