Далі методом афінних перетворень треба вирівняти лице так, щоб рот та очі були приблизно по центру.

3. Кодування лиця

Для реалізації цього кроку треба використати глибинне машинне навчання. Вхідні дані для навчання – 3 фото: 2 з них належать одній людині, та інше – іншій. На виході ми маємо отримати 128 вимірів кожного обличчя (карта лиця).

4. Пошук людини в базі

Цей крок найпростіший – за отриманою картою лиця треба знайти в базі відповідне ім'я людини. Тут можна використовувати будь-який алгоритм, який в певних умовах буде давати задовільні результати по швидкості пошуку.

Н. Швець
Науковий керівник – д. т. н., проф. Ромака В. А.

ДОСЛІДЖЕННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ШЛЯХОМ ПОРІВНЯННЯ ТЕХНІК МОНІТОРИНГУ ТА АНАЛІЗУ ІНФОРМАЦІЙНОЇ СИСТЕМИ

Інформаційний простір охоплює всі сфери діяльності сучасної людини, тому актуальною є безпека інформаційних ресурсів, яка потребує розвитку та вдосконалення. Сучасні загрози інформаційної безпеки виникають у різних формах та спрямованні на широкий спектр вразливостей. Запобігання загрозам та виявлення атак на систему є одним з найголовніших завдань для забезпечення цілісності, доступності та конфіденційності інформації.

Головним напрямком даної роботи є моніторинг інформаційної системи та реагування на порушення даних та кібер-атак, які стають більш поширеними. Для виявлення шкідливого програмного забезпечення та спроб компрометації пристроїв інформаційної системи використовують різні техніки моніторингу. Одним із ключових факторів успішного виявлення атаки та перешкоди реалізації конкретної загрози є вибір інструментарію.

В даній роботі представлено дослідження по аналізу вірусу за допомогою двох наборів інструментів. Це дозволить оцінити ефективність використання конкретних програм та технік. Критеріями ефективності є досягнення поставленої мети по виявленню та запобіганню загрози, затрачений час та складність використання.

Для проведення порівняння інструментарію проведено практичне застосування двох підходів на однаковому зразку шкідливого програмного забезпечення.

Обраний для аналізу вірус – Trojan.Kovter. Він належить до сімейства шкідливого програмного забезпечення, ціль вірусів такого типу – системи Windows.

Перший набір інструментів для аналізу вірусу це Process Explorer та RegJump. Аналіз проведено в режимі реального часу, здійснено дослідження поведінки вірусу та ресурсів до яких він здійснює спроби доступу.

В результаті дослідження Trojan.Kovter виявився вірусом, для реалізації мережевого шахрайства типу клікфрод. Основними методами зараження, які використовує даний вірус є метод файлового зараження та використання регістрів в під час етапу закріплення в системі.

Наступним етапом роботи є проведення дослідження даного вірусу за допомогою інструменту RedLine. Дана програма використовується в сучасному захисті інформації для моніторингу інформаційних систем. Основним фактором успішного використання даного інструменту є налаштування колектора для збору інформації відповідно до поставленого завдання та цілі виявлення.

Для проведення аналізу було заражена віртуальна машина вірусом Trojan.Kovter та зібрано всю доступну інформацію з цієї машини для подальшого аналізу. За допомогою RedLine проведено аналіз шкідливого програмного забезпечення і виявлено наслідки його дій в системі.

Третім етапом є порівняння двох наборів інструментів та підходів до виявлення та аналізу вірусу.

Критерій ефективності, який вказує на досягнення поставленої мети в обох випадках високий, оскільки при використанні двох технік було виявлено поведінку вірусу та ресурси системи, які він використовує в своїй діяльності.

Затрачений час на аналіз Trojan.Kovter за допомогою першого набору інструментів вдвічі менший за час аналізу системи за допомогою програми RedLine.

Але є низка переваг використання RedLine, основною перевагою є автоматичність та можливість проведення повторного аналізу зібраної інформації в будь-який час.

Зі сторони простоти використання обидві техніки є досить зрозумілими у використанні.

Результатом роботи є повний аналіз вірусу Trojan.Kovter. Зроблено висновки щодо ефективного застосування різних технік в залежності від типу шкідливого програмного забезпечення та конкретного завдання.