https://doi.org/10.31891/2307-5732-2023-317-1-300-309
УДК 004.93

ЛИСЕНКО Сергій
Хмельницький національний університет
https://orcid.org/0000-0001-7243-8747
АТАМАНЮК Ольга
Хмельницький національний університет
БОХОНЬКО Олександр
Хмельницький національний університет
https://orcid.org/0000-0002-7228-9195
ВОРОБЙОВ Володимир
Хмельницький національний університет
https://orcid.org/0000-0001-7738-1444

ДОСЛІДЖЕННЯ МЕТОДІВ ВИЯВЛЕННЯ КІБЕРЗАГРОЗ ТИПУ RANSOMWARE НА ОСНОВІ ЗАСТОСУВАННЯ HONEYPOT

В роботі представлено метод та програмно-технічний засіб виявлення кіберзагроз типу Ransomware на основі застосування Honeypot, які є концептуальними пастками, призначеними для блокування несанкціонованого доступу до даних. Honeypot, також відома як технологія виявлення вторгнень, тип технології безпеки, яка перевіряє пристрої для запобігання небажаним діям. У даній статті буде представлено огляд кібербезпек, кіберзагроз і системних методів. Ця стаття є результатом багатьох досліджень, і, оцінюючи honeypots, дослідники виявили, що це важливий інструмент безпеки, який може обмежити системні атаки та надати аналітикам уявлення про походження і поведінку даних кіберзагроз.

Ключові слова: шкідливе програмне забезпечення, кіберзагроза, програми-вимагачі, кібербезпека, кіберпростір.

LYSENKO Sergii, ATAMANIUK Olga, BOKHONKO Oleksandr,VOROBIYOV Volodymyr
Khmelnytskyi National University

METHOD FOR DETECTION OF RANSOMWARE CYBER THREATS BASED ON HONEYPOT: STATE-OF-ART

The work presents the research of the methods for detecting cyber threats such as Ransomware based on the use of Honeypot. Today, lack of awareness allows attacks to bypass basic security mechanisms, security vulnerabilities in the IT systems of small and large corporations are increasingly being used to cause business failures. The cyberattackscontinue to expand rapidly as cybercriminals constantly bypass the security tools developed and implemented by organizations. The purpose of attacks is increasingly data that is critical to both individuals and organizations. Attackers use capabilitiesthat can help them seize control of valuable data to demand a ransom from the data owner. Ransomware is a form of malware that infects a computer or multiple computers over a network by encrypting files and folders, making them unusable. The users are then asked to make a ransom. Ransomware is not a new threat, but its use is growing rapidly and causing large financial losses in the world. This is a serious challenge for cybersecurity analysts because typical ransomware is not detected by antivirus software due to its polymorphic nature. There was a sudden surge in extremely dangerous ransomware attacks that harmed most companies and individuals. Ransomware poses a great threat and must be fought at a global level. There is a lack of comprehensive analysis to cover the security issues of individual users and corporations. Ransomware avoidance methods are the most effective and require special attention as the reduction and recovery of ransomware becomes increasingly difficult. The task arises to investigate the effectiveness of known methods in order to assess and identify their advantages and disadvantages, which will allow in the future to develop and implement new effective methods and means of combating Ransomware-type SPZ based on the use of Honeypot. The study shows that because malware is automated and targets any location arbitrarily, placing the bait anywhere to detect activity is an improvement over the lack of monitoring at all. Experimental studies indicate a high reliability of the proposed methods, in particular the reliability of the detection of cyber threats of the Ransomware type, but the insufficient adaptability of these methods in the evolution of the malware.

Keywords: ransomware, honeypot, malware, cyber threat, cyber security.

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

Сьогодні недостатня обізнаність дозволяють атакам обходити базові механізми безпеки, уразливі місця безпеки в IT-системах малих і великих корпорацій все частіше використовуються, щоб викликати збої в бізнесі. Кібератаки продовжує швидко розширюватися, оскільки кіберзлочинці постійно обходять засоби безпеки, розроблені та впроваджені організаціями. Метою атак все частіше стають дані, які є критично важливими як для окремих осіб, так і для організацій. Зловмисники використовують можливості, які можуть допомогти їм захопити контроль над цінними даними, щоб вимагати викуп від власника даних [1].

Програмне забезпечення-вимагач – це форма шкідливого програмного забезпечення, яке заражає комп'ютер або кілька комп'ютерів через мережу, шифруючи файли та папки, роблячи їх непридатними для використання. Потім користувачам пропонується внести викуп. Програмне забезпечення-вимагач не є новою загрозою, але його використання стрімко зростає та спричиняє великі фінансові втрати в світі. Це серйозний виклик для аналітиків кібербезпеки, оскільки типове програмне забезпечення-вимагач не виявляється антивірусним програмним забезпеченням через його поліморфну природу.

51% організацій у всьому світі у 2021 році постраждали від високотехнологічних атак програм-вимагачів. Ці атаки використовували розширені командні та контрольні сервери, що ускладнювало їх зворотне проектування [2].

Netwalker — одна з найновіших і небезпечних програм-вимагачів. Його популярність полягає в методі розповсюдження, використовуючи фішингові електронні листи, пов'язані з COVID-19, таким чином спонукаючи жертву завантажити вкладені файли, що призводить до виконання портативних двійкових файлів і зараження системи. У лютому 2021 року було випущено останню версію програм-вимагачів Zeoticus 2.0. Zeoticus 2.0 може виконуватися повністю в автономному режимі, не вимагаючи жодного сервера керування. Щоб отримати платіж за викуп, Zeoticus використовує надійно захищені та зашифровані поштові облікові записи Proton, щоб уникнути відстеження [3].

Відбувся раптовий сплеск надзвичайно небезпечних атак програм-вимагачів, які завдали шкоди більшості компаній і окремих осіб. Програми-вимагачі становлять велику загрозу і з ними потрібно боротися на глобальному рівні. Бракує комплексного аналізу, який би охоплював питання безпеки окремих користувачів і корпорацій.

Методи уникнення програм-вимагачів є найефективнішими та потребують спеціальної уваги, оскільки зменшення та відновлення програм-вимагачів стає дедалі складнішим.

Постає задача дослідити ефективність відомих методів з метою здійснення оцінки та виявлення їх переваг та недоліків, що дозволить в майбутньому розробляти та імплементувати нові ефективні методи та засоби боротьби з ЗПЗ типу Ransomware на основі застосування Honeypot.

Тому метою роботи є дослідження методів виявлення ЗПЗ типу Ransomware на основі застосування Honeypot з метою надання певних мір безпеки шляхом розроблення методу.

Поняття ЗПЗ типу Ransomware на основі застосування Honeypot

ЗПЗ типу Ransomware вважаються одним із найнебезпечніших варіантів шкідливих програм. Це насамперед тому, що для підвищення привілеїв навіть не потрібна активна взаємодія користувача. Навіть використання стандартних інструментів і технологій не змогло стримати програм-вимагачів. Щойно програмне забезпечення-вимагач заражає пристрій, жертва немає можливості отримати доступ до файлів. Через те, що викуп сплачується за допомогою криптовалюти, немає способу відстеження виконавців атак програм-вимагачів. Рисунок 1 ілюструє фінансову шкоду, завдану програмами-вимагачами у 2021 році порівняно з її попередниками [4].

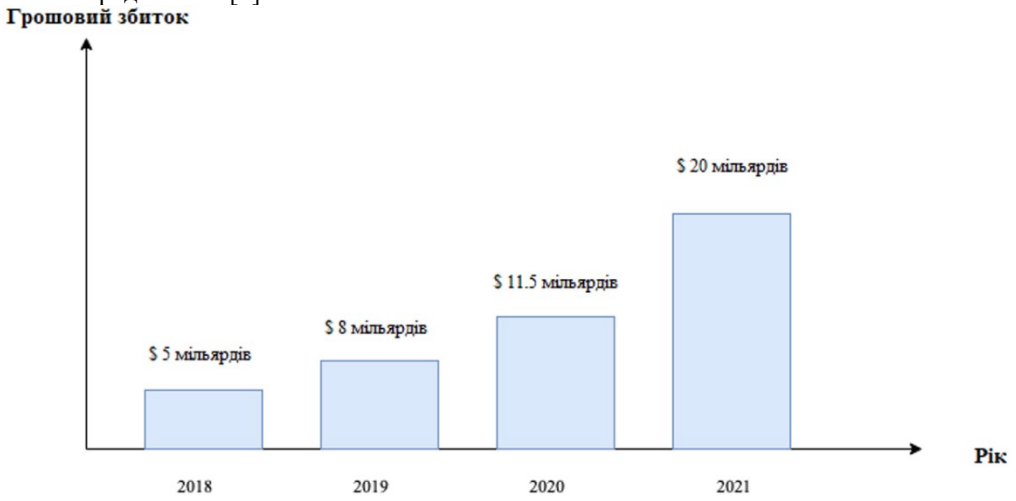

Рис. 1. Збитки програм-вимагачів за останні роки

1.1. Поширення ЗПЗ типу Ransomware на основі застосування Honeypot

Поширюється програма-вимагач насамперед через відсутність кібергігієни на індивідуальному рівні. Кібергігієна стосується всіх аспектів онлайн-безпеки, включаючи поведінку веб-переглядача, доступність і постійне оновлення антивірусного програмного забезпечення, встановлення стороннього програмного забезпечення та обізнаність користувачів. Необхідно дотримуватися кібергігієни, щоб уникнути програм-вимагачів та інших зловмисних програм. Незважаючи на вдосконалення стандартів безпеки та протоколів, родинам програм-вимагачів вдалося проникнути в системи захисту організацій, урядів та окремих користувачів [5]. Деякі з основних джерел програм-вимагачів включають:

- Додатки електронної пошти

Вкладення електронної пошти зазвичай містять документи у форматі Portable Document Format (PDF), голосові повідомлення, зображення тощо. Програми-вимагачі використовують методи, завдяки яким електронний лист виглядає так, ніби його надіслав надійний відправник.

- Знімний носій

Багато хто не вважає знімний носій порталом для програм-вимагачів. Однак було проведене опитування, яке показало, що люди справді зацікавлені тим, що може бути у випадкових накопичувачах універсальної шини (USB), які лежать у громадському місці.

- Шкідлива реклама

Шкідлива реклама — це організоване зараження рекламної інфраструктури, яку вебсайти використовують для показу онлайн-реклами. Шкідлива реклама виявилася ще одним популярним методом зараження систем програмами-вимагачами.

- Соціальні мережі та SMS

Цей тип розповсюдження програм-вимагачів підпадає під категорію соціальної інженерії, де жертву спонукають перейти за посиланням. Зловмисники використовують техніку скорочення Uniform Resource Locator (URL), щоб додати незрозумілості вихідному посиланню. Користувачів із поганою кібергігієною переходять за цими посиланнями. Іноді користувачі також отримують SMS-повідомлення, які зображують терміновість і змушують їх натискати ці посилання.

- Програми-вимагачі як послуга

Подібно до інших хостингових служб у Dark Web, які пропонують анонімність, Ransomware-as-a-Service (RaaS) з'явився як послуга виключно для зловмисників із недостатніми навичками програмування, щоб легко поширювати програми-вимагачі.

2.3. Типи програм-вимагачів

Існує в основному два поширених типи програм-вимагачів, відомих як Crypto Ransomware і Locker Ransomware.

2.3.1. Крипто-вимагач

Crypto Ransomware використовує алгоритми шифрування для шифрування даних жертв за допомогою двох підходів. У випадку симетричного алгоритму існує лише один ключ, який використовується як для шифрування, так і для дешифрування. Другий алгоритм, який є більш поширеним, — це асиметричний алгоритм, за допомогою якого дані шифруються за допомогою відкритого ключа, і жертва може отримати свої дані назад лише тоді, коли вона заплатить за ключ дешифрування. Протягом багатьох років зловмисники ускладнювали роботу реверсивних інженерів, які намагалися розшифрувати дані без сплати викупу. Тепер зловмисники використовують комбінацію симетричних і асиметричних алгоритмів, щоб зробити процес дешифрування більш складним. Дані жертви шифруються за допомогою симетричного алгоритму завдяки його швидкості. Потім використаний ключ шифрується за допомогою відкритого ключа, яким володіє зловмисник.

2.3.2. Locker Ransomware

Як видно з назви, Locker Ransomware блокує пристрій замість шифрування файлів і папок. Після зараження пристрій жертви не може отримати доступ. Цей тип програм-вимагачів є менш ефективним, ніж Crypto Ransomware, оскільки доступ до даних усе ще можна отримати, перемістивши пристрій зберігання на інший комп'ютер.

2.4. Операція Ransomware

Різні фази роботи програми-вимагача (показано на рисунку 2) докладно описано нижче:

2.4.1. Поширення програми-вимагача на пристрій жертви

Перший етап – поширення програми-вимагача на пристрій жертви. Є кілька джерел, через які програми-вимагачі знаходять вектор інфекції. На цьому етапі стратегія зловмисника полягає в тому, щоб отримати завантажене програмне забезпечення-вимагач на комп'ютер жертви. Ця стадія значною мірою залежить від діяльності жертви та загальної кібергігієни. Якщо потенційна жертва є кіберобізнаною, тоді дуже ймовірно, що програма-вимагач не зможе заразити систему [6].

2.4.2. Шифрування/Блокування

Після зараження програма-вимагач починає виконувати запрограмовану послідовність дій залежно від свого типу. Властивістю останніх програм-вимагачів є те, що вони зв'язуються з центральним сервером керування (C2C), завдяки чому процес автоматизації для зловмисника стає простим. Сервер C2C також діє як репозиторій, через який різні жертви можуть завантажити свої ключі розшифровки після здійснення платежу. Після першого етапу криптографічні ключі генеруються або на персональному комп'ютері (ПК) жертви, або на сервері C2C. Потім зловмисник блокує файли та папки або може відразу змінити головний завантажувальний запис, щоб жертва не змогла отримати доступ до свого пристрою.

2.4.3. Викуп даних

Під час третього етапу на екрані починає відображатися повідомлення, яке вимагає від жертви суму викупу, щоб вона могла повернути доступ до своєї системи. Зловмисник надає біткойн-адресу для виплати викупу. Це збільшує труднощі для правоохоронних органів відстежити платіж зловмиснику.

2.4.4. Результат функціонування ЗПЗ типу Ransomware

Після третього етапу користувач може заплатити суму викупу. На цьому етапі є три результати. Якщо жертва вирішить заплатити викуп, їй буде надано ключ розшифровки, щоб розблокувати доступ до своїх пристроїв. Інший результат може виникнути, коли жертва має певні технічні навички або може скористатися допомогою реверсивних інженерів, щоб скасувати операції програм-вимагачів і повернути файли. Третій результат виникає в ситуації, коли жертва не може заплатити викуп. Це призводить до незворотного пошкодження та повної втрати даних.

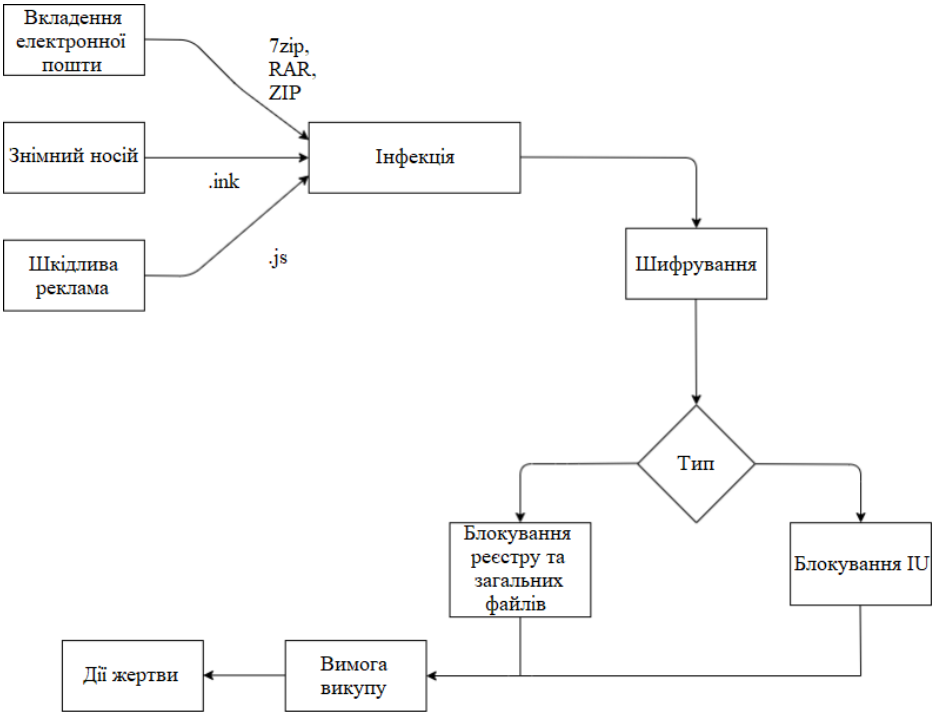

Рис. 2. Типова послідовність операцій програми-вимагача

2.5. Роль криптовалют

На початку появи програм-вимагачів зловмисники вимагали гроші у формі прямого банківського депозиту або через агентства з переказу грошей. З моменту появи криптовалют кількість атак програм-вимагачів різко зросла. Це пов'язано з тим, що криптовалюти вводять концепцію анонімності. Криптовалюти сприяють створенню програмного забезпечення-вимагача, яке замість розгортання методу прямої оплати один-на-один використовує платіжний шлюз третьої сторони, щоб мінімізувати ризик виявлення. Зазвичай, коли криптовалюта налаштована як спосіб оплати, зловмисник пасивно спостерігає за блокчейном, який дозволяє криптовалютам перевіряти, чи була сплачена сума викупу чи ні. Після здійснення платежу процес надсилання ключа розшифровки жертві може бути розпочато за допомогою автоматизації. Це застосовує теорію анонімності та неможливості відстеження [7].

Дослідження методів виявлення Ransomware на основі застосування Honeypot

1.2. Методи виявлення

Різні методи виявлення програм-вимагачів були запропоновані як дослідниками, так і експертами з промислової безпеки. Ці методи здебільшого працюють за допомогою статичного або динамічного аналізу. Статичний аналіз виконується шляхом перевірки коду без фактичного запуску виконуваного файлу. Динамічний аналіз виконується після запуску ймовірного програмного забезпечення-вимагача. Під час його виконання дії та системні виклики, здійснені підозрілим файлом, записуються, і на основі цієї інформації створюється остаточний звіт [8].

1.2.1. Статичний аналіз

В [9] представлено метод, який використовуватиме статичний аналіз як підхід до виявлення програм-вимагачів. Метод містив інфраструктуру, яка спочатку сконструювала PE-файл, а потім застосувала динамічну компоновану бібліотеку (DLL) і вилучення викликів функцій до PE-файлу. Автори проаналізували 43 зразки програм-вимагачів, використовуючи різні параметри. У даному методі вдалося відрізнити програми-вимагачі від звичайних програм за допомогою графіка косинусної подібності на основі інструкцій зі складання. Незважаючи на те, що даний метод новий, він не може виявити найновіші сімейства програм-вимагачів, які використовують методи ухилення від сигнатур.

В [10] було розроблено метод GreatEatlon для виявлення програм-вимагачів Android. GreatEatlon використовував чотири етапи, щоб визначити наявність програм-вимагачів на пристрої Android. Перший етап полягав у відстеженні потоків коду виконуваного файлу, підозрюваного як програмне забезпечення-вимагач. GreatEatlon зміг легко визначити шлях програм-вимагачів, який використовується для аналізу потоків коду програм Android. Потім GreatEatlon пройшов виконуваний файл через другий етап, на якому перевірялися API DeviceAdmin, коли виконуваному файлу було дозволено запуститися. Якщо виконуваний файл неправильно використав API для підвищення своїх привілеїв, він буде позначений як шкідливий. На останніх двох етапах застосовувалися методи статичного та ручного аналізу, щоб остаточно визначити поведінку підозрюваного виконуваного файлу.

В [11] запропонувано метод зі зворотнім проектуванням на WannaCry Ransomware, щоб зрозуміти, як працює шкідливий двійковий файл. Методом аналізу, який використовували автори, був статичний аналіз. IDA Pro використовувався для зворотного проектування, щоб зрозуміти внутрішню роботу програми-вимагача. PE-файл, який спочатку використовувався для першого етапу роботи програми-вимагача, на наступних етапах конвертувався в інші формати. По-перше, файл PE доставляється через експлойт Eternal Blue, який потім використовує API Windows для вбудовування. На наступному етапі дві служби, mssecsvc.exe і tasksche.exe, відповідають за подальше розповсюдження шляхом зміни налаштувань середовища. Третій етап відповідає за загальне шифрування даних жертви, де taskche.exe завантажує .dll шифрування в пам'ять пристрою. Останній етап підтримується серверами C2C для відстеження платежів і перебігу зараження.

1.2.2. Динамічний аналіз

В [12] подано метод, що включає машинне навчання та динамічний аналіз коду. EldeRan перевірив зразки додатків за набором параметрів, які могли б визначити, чи є зразок програмним забезпеченням-вимагачем під час фази зараження. EldeRan успішно проаналізував виклики Windows API, операції з ключами реєстру, операції з файлами та каталогами, видалені файли та вбудовані рядки. Далі відбувався вибір функцій, які могли б відрізнити програмне забезпечення-вимагач від звичайного програмного забезпечення за критеріями взаємної інформації і класифікація. Загалом EldeRan досяг високого рівня успіху у виявленні нових сімейств програм-вимагачів.

Автори [13] вперше подали метод, що виявляв вплив програм-вимагачів на клінічне середовище. Автори розробили метод на основі машинного навчання, яка могла виявляти наявність програми-вимагача ще до того, як вона почала поширюватися. Метод виявляє зміни в мережевому трафіку під час запуску програми-вимагача. Потім ці шаблони передає до імовірнісного контрольованого класифікатора програм-вимагачів, щоб нарешті виділити складні характеристики зразка. Запропонований метод мав чотири основні компоненти. Перший модуль відстежує моделі трафіку, отримані в результаті живої вибірки. Наступний модуль потребує нагляду людини для генерації відповідного набору даних, який буде передано в алгоритми машинного навчання для виявлення та класифікації програм-вимагачів. Третій модуль ідентифікує аномальні моделі та позначав їх. Останній модуль зосереджений на методах зменшення за допомогою моделей машинного навчання на основі правил.

В [14] запропоновано метод зворотного проектування WannaCry Ransomware за допомогою динамічного режиму аналізу. У цьому випадку зразок WannaCry був запущений в системі, і його взаємодія з процесами, файловою системою, реєстром і мережевою активністю була записана. Автори використовували інструмент для запису підпису зразка. WannaCry, будучи багатоступеневою програмою-вимагачем, використовує процес для завантаження файлу tasksche.exe, який у свою чергу запускає різні процеси.

В [15] розроблено метод під назвою REDFISH, який стверджував, що виявляє наявність програм-вимагачів в організаційних налаштуваннях раніше за всіх фреймворків за допомогою аналізу мережевого трафіку. Для перевірки свого алгоритму автори використали близько 19 сімей програм-вимагачів. Цей метод розроблено для боротьби з програмами-вимагачами, створеними для шифрування файлів і папок на спільних мережевих дисках у Network Attached Storage. Після ретельної оцінки всіх середовищ, у яких можуть зберігатися програми-вимагачі, автори з'ясували, що існування SMB у мережі вказує на можливе середовище, де можуть перебувати програми-вимагачі. Вони використали пристрій перевірки мережевого трафіку, щоб проаналізувати поведінку вхідного та вихідного трафіку. Вони проаналізували використання команд на основі SMB, щоб знайти аномалії в трафіку. Автори провели кілька тестів алгоритму та повідомили, що REDFISH може виявити програми-вимагачі протягом 20 секунд.

В [16] подано метод раннього виявлення з новою функцією вилучення шаблону. Їхній метод зміг підготувати автоматизований аналітичний звіт. У звіті вдалося представити найбільш унікальні моделі та шляхи поведінки різних сімей програм-вимагачів. За результатами експериментів семи сімейств програм-вимагачів автори змогли з'ясувати ефективність кожного з алгоритмів, що використовуються для виділення патернів. Метод, розроблений авторами, можна використовувати на середніх і великих підприємствах, оскільки він може легко обробляти великі дані і виявляти програмне забезпечення-вимагач перед іншими стандартними галузевими рішеннями.

В [17] подано метод під назвою DeepAMD, що використовував набір даних для вилучення функцій. Очищені дані, отримані в результаті вилучення функцій, аналізувалися як статично, так і динамічно, щоб визначити програму. DeepAMD виявився ефективним підходом для раннього виявлення найдосконаліших сімейств програм-вимагачів. Це пов'язано з високою швидкістю перевірки DeepAMD за допомогою останнього та оновленого набору даних про зловмисне програмне забезпечення Android.

В [18] розроблено метод, який зміг виявити Crypto Ransomware, яке є найпоширенішим типом Ransomware. Він може виявляти майже всі ланцюжки крипто-вимагачів на стадії їх попереднього шифрування. Спочатку він перевіряє підозрілий двійковий файл шляхом порівняння контрольної суми, а потім, за допомогою алгоритму, який контролює попереднє шифрування API. Єдиним обмеженням є висока залежність від Windows API. Отже, якщо метод розгорнуто як єдиний механізм виявлення, він може не виявити останні сімейства.

В [19] представлено метод раннього виявлення Crypto Ransomware, але за допомогою іншого підходу. Модель використовувала два модулі виявлення, один для аналізу поведінки, а другий для оцінки

аномалій. Злиття обох результатів тоді дасть правильне рішення про те, чи є двійковий файл шкідливим. Завдяки результатам, показаним у роботі, модель показала надзвичайно хороші результати у виявленні ланцюгів програм-вимагачів. Даний метод можна використовувати для інших екосистем через надзвичайно низький рівень помилкових позитивних результатів.

Рисунок 4 ілюструє основні методи аналізу для виявлення програм із їхніми підтипами.

Рис. 4. Таксономія методів виявлення програм-вимагачів

Методи виявлення програм-вимагачів стали більш ефективними у боротьбі з великими атаками програм-вимагачів. Незважаючи на прогрес у техніках виявлення, найновіші сімейства програм-вимагачів продовжують уникати їх, оскільки ці методи не розроблені для захисту всіх ланцюгів програм-вимагачів одночасно. Рішення для виявлення створюються здебільшого для виявлення окремого ланцюга або одного типу програм-вимагачів, тому загальних рішень не існує, оскільки їх надзвичайно складно розробити.

4.3. Методи зменшення негативних наслідків впливу ЗПЗ типу Ransomware

З моменту появи програм-вимагачів кіберзахисники намагаються розробити передові рішення безпеки, які б протистояли різним напрямкам програм-вимагачів. З іншого боку, розробники програм-вимагачів використовували нові вразливості, використовуючи недостатню поінформованість переважної більшості населення про кібербезпеки. Тому було запропоновано кілька методів, які можуть забезпечити ефективне видалення програм-вимагачів і відновлення пристроїв.

В [20] представлено метод, який використовує програмно визначену мережу для протидії програмам-вимагачам. Техніка використовувала динамічний чорний список серверів C&C під час виконання зразка. Без C&C сервера заражена машина не може отримати доступ до відкритого ключа, який використовуватиметься для її шифрування. Однак цей метод не міг ідентифікувати сервери, які раніше не використовувалися як сервери C&C. Техніка чорного списку працювала зі списком доступних проксі-серверів. Впровадження такої системи стало можливим завдяки двом додаткам на основі SDN, SDN1 і SDN2. SDN1 оцінив відповіді DNS від вхідного трафіку та перевірив, чи домен уже присутній у базі даних незаконних проксі-серверів. SDN2 розширив функціональні можливості SDN1, переконфігурувавши всю мережеву інфраструктуру для блокування активності програм-вимагачів. SDN2 використовував протокол OpenFlow для блокування трафіку, пов’язаного зі зловмисним зразком.

В [21] використано метод зворотного проектування, щоб виявити фактичну роботу, за якою йдуть різні версії програм-вимагачів. Підхід, якого дотримувалися автори складався з двох модулів. Перший модуль використовував зворотне проектування, щоб знайти функції для видалення та відновлення даних у вихідному коді шкідливого ПЗ. За допомогою першого модуля автори змогли визначити різні властивості програм-вимагачів. Другий модуль використовував ізольоване програмне середовище для аналізу поведінки програм-вимагачів. За допомогою другого модуля були зібрані різні особливості поведінки вибірки. Потім автори перейшли до обговорення методів приховування файлів, які використовували зловмисники. Вони виявили, що зловмисники не використовують безпечні методи видалення файлів, які унеможливлюють відновлення файлів. У своєму експерименті вони змогли відновити дані через слабку методологію видалення, яку використовує програма-вимагач.

В [22] Байкара та ін. розробив метод за допомогою програми під назвою Safe Zone, у якій в одному файлі зберігаються всі файли користувача шляхом їх стиснення. Файл, створений авторами, був відомий як safezone.safe і зберігався в режимі безперервного запису, щоб інші джерела не могли його змінити. Програма використовувала систему журналювання під назвою File Watcher, яка реєструвала всі події в безпечній зоні, а також відстежувала зміни, зроблені в батьківських папках файлів, доданих до безпечної зони. Програма

мала ще одну функцію, яка перевіряла цілісність у safezone.safe. У разі атаки програм-вимагачів жертви можуть безпечно повернутися до останньої резервної копії, збереженої в безпечній зоні і відновити систему до попереднього стану.

В [23] Акбанов та ін. використали метод для захисту від програм-вимагачів WannaCry у мережі. У своєму методі автори обмежили поширення програми-вимагача лише на одному пристрої. Спочатку весь зловмисний трафік надсилається до контролера, який потім аналізує всі пакети та порівнює зловмисні пакети з базою даних чорного списку. Потім він перевіряє наявність індикаторів WannaCry. TCP-порт 445 контролюється контролером, і щойно надходить будь-який трафік із цього порту або TCP-порту 139, він обмежується контролером, щоб програми-вимагачі не могли поширюватися далі від зараженого хоста. Однак він не може виявити нові версії WannaCry, які використовують розширені експлойти через механізми ухилення, які вони розгортають.

В [24] Софос розробили метод зменшення кінцевих точок під назвою Intercept X, який стверджує, що усуває сімейства APT нульового дня. Intercept X використовує аналіз поведінки, щоб запобігти модифікації сімей програм-вимагачів у реєстрах. Рівень успіху X становить 99,7% у виявленні та зменшені за допомогою лише однієї помилкової тривоги в реальному тестуванні.

На рисунках 5-8 показані результати аналізу підходів до виявлення ЗПЗ типу Ransomware на основі застосування Honeypot F-score значення.

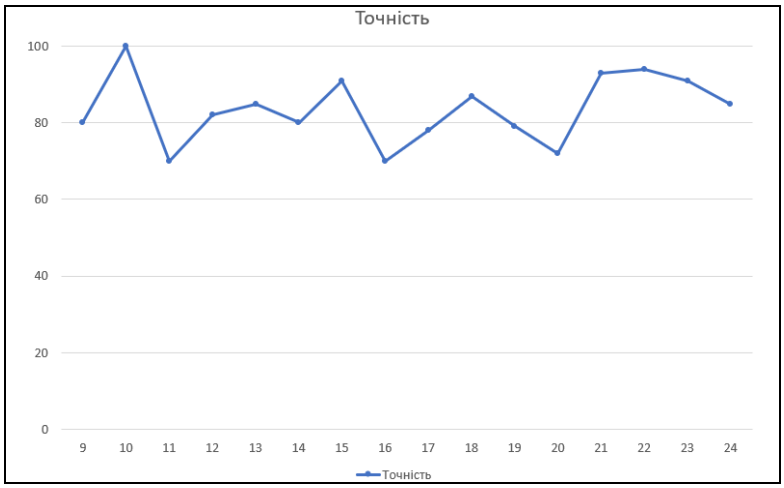

Рис. 5. Результати проаналізованих підходів до виявлення ЗПЗ типу Ransomware на основі застосування Honeypot з точки зору точності

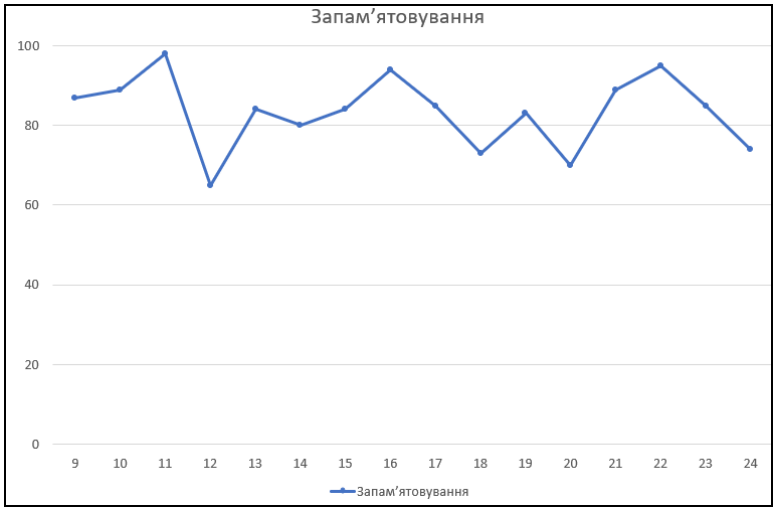

Рис. 6. Результати проаналізованих підходів до виявлення ЗПЗ типу Ransomware на основі застосування Honeypot з точки зору запам’ятовування

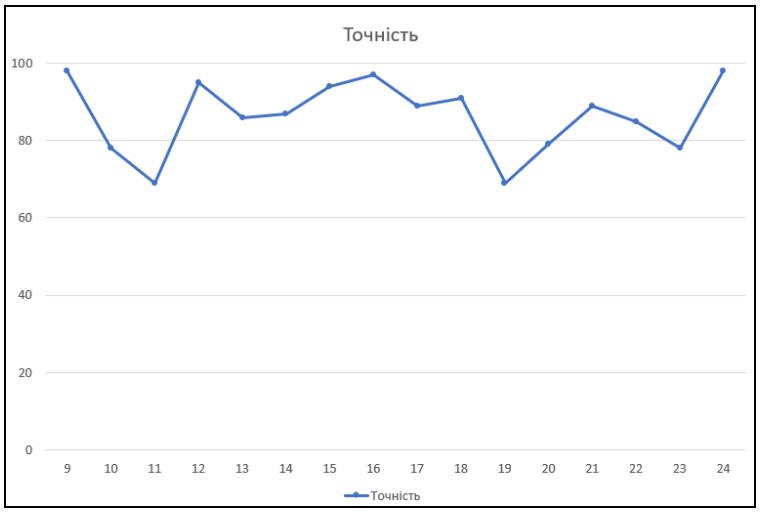

Рис. 7. Результати проаналізованих підходів до виявлення ЗПЗ типу Ransomware на основі застосування Honeypot з точки зору точності

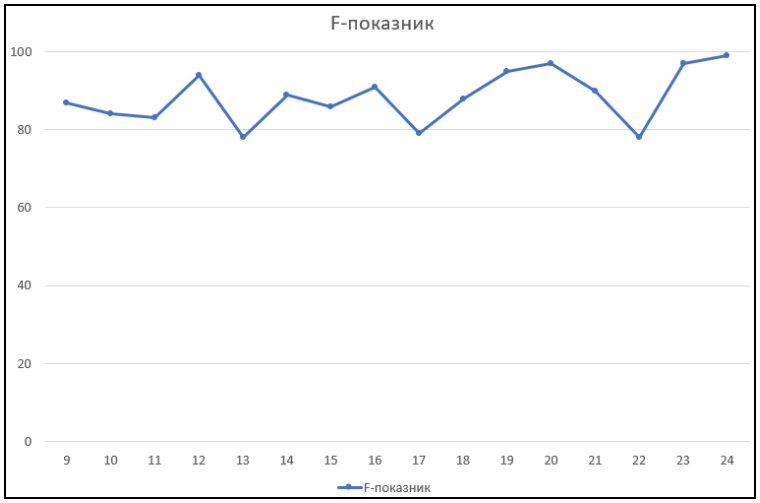

Рис. 8. Результати проаналізованих підходів до виявлення ЗПЗ типу Ransomware на основі застосування Honeypot з точки зору F-показника

Результати продемонстрували, що метод Зімба та ін. досягає найкращих результатів для виявлення атак Ransomware. Завдяки своєму методу вони змогли відновити дані через слабку методологію видалення, яку використовує програма-вимагач. У зразках, проаналізованих авторами, майже всі зразки видалили тіньові копі, але завдяки своєчасному офлайн-резервному копію цих копій вдалося відновити пристрій користувача. Навіть у тих випадках, коли програми-вимагачі змогли уникнути пісочниці, автори змогли відновити дані, використовуючи методологію генерації пар відкритих ключів на пристрої жертви. Дані дослідження продемонстрували високу достовірність виявлення ЗПЗ типу Ransomware на основі застосування Honeypot запропонованим методом до 99%.

Таким чином, існує велика кількість методів та засобів виявлення ЗПЗ типу Ransomware на основі застосування Honeypot, однак основним їх недоліком, як показав аналіз, є їх недостатня адаптивність щодо їх еволюції та недостатня достовірність виявлення, що зумовлює необхідність розроблення нових методів виявлення.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі

У роботі досліджено методи виявлення кіберзагроз типу Ransomware на основі застосування Honeypot. Дослідження показує, що оскільки зловмисне програмне забезпечення є автоматизованим і націлюється на будь-яке місце довільно, розміщення приманки будь-де для виявлення активності є покращенням у порівнянні з відсутністю моніторингу взагалі. Експериментальні дослідження свідчать про високу достовірність запропонованих методів, зокрема достовірність виявлення кіберзагрози типу Ransomware, однак недостатню адаптивність вказаних методів при еволюції ЗРЗ.

Література

1. Nihad A. Hassan. Ransomware Revealed. 2019. Pp. 12-20.

2. Mark Dunkerley, Matt Tumbarello. Mastering Windows Security and Hardening: Secure and protect your Windows environment from cyber threats using zero-trust security principles, 2nd Edition. 2022. Pp. 124-132.

3. What is Netwalker Ransomware? Attack Methods & Protection Tips, 2022. URL: https://www.upguard.com/blog/what-is-netwalker-ransomware. – 15.09.2022р. (дата звернення: 15.09.2022).

4. Cybercrime To Cost The World $10.5 Trillion Annually By 2025, 2022. URL: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021. – 18.09.2022р. (дата звернення: 18.09.2022).

5. Chee Keong NG, Lei Pan, Yang Xiang. Honeypot Frameworks and Their Applications: A New Framework (SpringerBriefs on Cyber Security Systems and Networks) 1st ed. 2018 Edition. 2018. Pp. 48-61.

6. Allan Liska. Ransomware: Understand. Prevent. Recover. 2021. Pp. 238-261.

7. Antony Lewis. The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology that Powers Them (Cryptography, Derivatives Investments, Futures Trading, Digital Assets, NFT). 2018. Pp. 123-129.

8. Scott Augenbaum. The Secret to Cybersecurity: A Simple Plan to Protect Your Family and Business from Cybercrime Hardcover. 2019. Pp. 78-96.

9. Subedi, K.P.; Budhathoki, D.R.; Dasgupta, D. Forensic analysis of ransomware families using static and dynamic analysis. In Proceedings of the 2018 IEEE Security and Privacy Workshops (SPW), San Francisco, CA, USA, 24 May 2018; pp. 181-185.

10. Zheng, C.; Dellarocca, N.; Andronio, N.; Zanero, S.; Maggi, F. Greateatlon: Fast, static detection of mobile ransomware. In Proceedings of the International Conference on Security and Privacy in Communication Systems, Guangzhou, China, 2016; Springer: Berlin/Heidelberg, Germany, 2016; pp. 619-634.

11. Hsiao, S.C.; Kao, D.Y. The static analysis of WannaCry ransomware. In Proceedings of the 2018 20th International Conference on Advanced Communication Technology (ICACT), Chuncheon, Korea, 2018; Pp. 157-161.

12. Sgandurra, D.; Muñoz-González, L.; Mohsen, R.; Lupu, E.C. Automated dynamic analysis of ransomware: Benefits, limitations and use for detection. arXiv 2016, arXiv:1609.03020.

13. Fernandez Maimo, L.; Huertas Celdran, A.; Perales Gomez, A.L.; Garcia Clemente, F.J.; Weimer, J.; Lee, I. Intelligent and dynamic ransomware spread detection and mitigation in integrated clinical environments. Sensors 2019, 19, 1114. [CrossRef]

14. Kao, D.Y.; Hsiao, S.C. The dynamic analysis of WannaCry ransomware. In Proceedings of the 2018 20th International Conference on Advanced Communication Technology (ICACT), Chuncheon, Korea, 2018; pp. 160-166.

15. Morato, D.; Berrueta, E.; Magaña, E.; Izal, M. Ransomware early detection by the analysis of file sharing traffic. J. Netw. Comput. Appl. 2018, 124, 13-32. [CrossRef]

16. Chen, Q.; Islam, S.R.; Haswell, H.; Bridges, R.A. Automated ransomware behavior analysis: Pattern extraction and early detection. In Proceedings of the International Conference on Science of Cyber Security,Nanjing, China, 9–11 August 2019; Springer: Berlin/Heidelberg, Germany, 2019; pp. 199–214.

17. Imtiaz, S.I.; ur Rehman, S.; Javed, A.R.; Jalil, Z.; Liu, X.; Alnumay, W.S. DeepAMD: Detection and identification of Android malware using high-efficient Deep Artificial Neural Network. Future Gener. Comput. Syst. 2021, 115, 846-856. [CrossRef]

18. Kok, S.; Abdullah, A.; Jhanjhi, N. Early detection of crypto-ransomware using pre-encryption detection algorithm. J. King Saud-Univ.-Comput. Inf. Sci. 2020, 1–16, Early Access. [CrossRef]

19. Al-rimy, B.A.S.; Maarof, M.A.; Prasetyo, Y.A.; Shaid, S.Z.M.; Ariffin, A.F.M. Zero-day aware decision fusion-based model for crypto-ransomware early detection. Int. J. Integr. Eng. 2018, 10, 82–88. [CrossRef]

20. Cabaj, K.; Mazurczyk, W. Using software-defined networking for ransomware mitigation: the case of cryptowall. IEEE Netw. 2016, 30, 13-20. [CrossRef]

21. Zimba, A.; Wang, Z.; Simukonda, L. Towards data resilience: The analytical case of crypto-ransomware data recovery techniques. Int. J. Inf. Technol. Comput. Sci. 2018, 10, 41-51. [CrossRef]Sustainability 2022, 14, 8 24 of 24

22. Baykara, M.; Sekin, B. A novel approach to ransomware: Designing a safe zone system. In Proceedings of the 2018 6th International Symposium on Digital Forensic and Security (ISDFS), Antalya, Turkey, 21-25 March 2018. Pp. 1–5.

23. Akbanov, M.; Vassilakis, V.G.; Logothetis, M.D. Ransomware detection and mitigation using software-defined networking: The case of WannaCry. Comput. Electr. Eng. 2019, 76, 111-121. [CrossRef]

24. Sophos. Endpoint Security Buyers Guide. Available online: https://www.enterpriseav.com/datasheets/endpointbuyersguide.pdf (дата звернення 20.09.2022).

References

1. Nihad A. Hassan. Ransomware Revealed. 2019. Pp. 12-20.

2. Mark Dunkerley, Matt Tumbarello. Mastering Windows Security and Hardening: Secure and protect your Windows environment from cyber threats using zero-trust security principles, 2nd Edition. 2022. Pp. 124-132.

3. What is Netwalker Ransomware? Attack Methods & Protection Tips, 2022. URL: https://www.upguard.com/blog/what-is-netwalker-ransomware. – 15.09.2022p. (application date: 15.09.2022).

4. Cybercrime To Cost The World $10.5 Trillion Annually By 2025, 2022. URL: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021. – 18.09.2022p. (application date: 18.09.2022).
5. Chee Keong NG, Lei Pan, Yang Xiang. Honeypot Frameworks and Their Applications: A New Framework (SpringerBriefs on Cyber Security Systems and Networks) 1st ed. 2018 Edition. 2018. Pp. 48-61.
6. Allan Liska. Ransomware: Understand. Prevent. Recover. 2021. Pp. 238-261.
7. Antony Lewis. The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology that Powers Them (Cryptography, Derivatives Investments, Futures Trading, Digital Assets, NFT). 2018. Pp. 123-129.
8. Scott Augenbaum. The Secret to Cybersecurity: A Simple Plan to Protect Your Family and Business from Cybercrime Hardcover. 2019. Pp. 78-96.
9. Subedi, K.P.; Budhathoki, D.R.; Dasgupta, D. Forensic analysis of ransomware families using static and dynamic analysis. In Proceedings of the 2018 IEEE Security and Privacy Workshops (SPW), San Francisco, CA, USA, 24 May 2018; pp. 181-185.
10. Zheng, C.; Dellarocca, N.; Andronio, N.; Zanero, S.; Maggi, F. Greateatlon: Fast, static detection of mobile ransomware. In Proceedings of the International Conference on Security and Privacy in Communication Systems, Guangzhou, China, 2016; Springer: Berlin/Heidelberg, Germany, 2016; pp. 619-634.
11. Hsiao, S.C.; Kao, D.Y. The static analysis of WannaCry ransomware. In Proceedings of the 2018 20th International Conference on Advanced Communication Technology (ICACT), Chuncheon, Korea, 2018; Pp. 157-161.
12. Sgandurra, D.; Muñoz-González, L.; Mohsen, R.; Lupu, E.C. Automated dynamic analysis of ransomware: Benefits, limitations and use for detection. arXiv 2016, arXiv:1609.03020.
13. Fernandez Maimo, L.; Huertas Celdran, A.; Perales Gomez, A.L.; Garcia Clemente, F.J.; Weimer, J.; Lee, I. Intelligent and dynamic ransomware spread detection and mitigation in integrated clinical environments. Sensors 2019, 19, 1114. [CrossRef]
14. Kao, D.Y.; Hsiao, S.C. The dynamic analysis of WannaCry ransomware. In Proceedings of the 2018 20th International Conference on Advanced Communication Technology (ICACT), Chuncheon, Korea, 2018; pp. 160-166.
15. Morato, D.; Berrueta, E.; Magaña, E.; Izal, M. Ransomware early detection by the analysis of file sharing traffic. J. Netw. Comput. Appl. 2018, 124, 13-32. [CrossRef]
16. Chen, Q.; Islam, S.R.; Haswell, H.; Bridges, R.A. Automated ransomware behavior analysis: Pattern extraction and early detection. In Proceedings of the International Conference on Science of Cyber Security,Nanjing, China, 9–11 August 2019; Springer: Berlin/Heidelberg, Germany, 2019; pp. 199–214.
17. Imtiaz, S.I.; ur Rehman, S.; Javed, A.R.; Jalil, Z.; Liu, X.; Alnumay, W.S. DeepAMD: Detection and identification of Android malware using high-efficient Deep Artificial Neural Network. Future Gener. Comput. Syst. 2021, 115, 846-856. [CrossRef]
18. Kok, S.; Abdullah, A.; Jhanjhi, N. Early detection of crypto-ransomware using pre-encryption detection algorithm. J. King Saud-Univ.-Comput. Inf. Sci. 2020, 1–16, Early Access. [CrossRef]
19. Al-rimy, B.A.S.; Maarof, M.A.; Prasetyo, Y.A.; Shaid, S.Z.M.; Ariffin, A.F.M. Zero-day aware decision fusion-based model for crypto-ransomware early detection. Int. J. Integr. Eng. 2018, 10, 82–88. [CrossRef]
20. Cabaj, K.; Mazurczyk, W. Using software-defined networking for ransomware mitigation: the case of cryptowall. IEEE Netw. 2016, 30, 13-20. [CrossRef]
21. Zimba, A.; Wang, Z.; Simukonda, L. Towards data resilience: The analytical case of crypto-ransomware data recovery techniques. Int. J. Inf. Technol. Comput. Sci. 2018, 10, 41-51. [CrossRef]Sustainability 2022, 14, 8 24 of 24
22. Baykara, M.; Sekin, B. A novel approach to ransomware: Designing a safe zone system. In Proceedings of the 2018 6th International Symposium on Digital Forensic and Security (ISDFS), Antalya, Turkey, 21-25 March 2018. Pp. 1–5.
23. Akbanov, M.; Vassilakis, V.G.; Logothetis, M.D. Ransomware detection and mitigation using software-defined networking: The case of WannaCry. Comput. Electr. Eng. 2019, 76, 111-121. [CrossRef]
24. Sophos. Endpoint Security Buyers Guide. Available online: https://www.enterpriseav.com/datasheets/endpointbuyersguide.pdf (application date: 20.09.2022).