Міністерство освіти і науки України

«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій

Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
завідувач кафедри кібербезпеки
та захисту інформації
_____ Н.В. Лукова-Чуйко
« » червня 2021р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

дипломної роботи
бакалавра
(назва освітнього рівня)

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)

спеціальність 125 Кібербезпека
(код і назва спеціальності)

освітня програма Кібербезпека
(назва освітньої програми)

на тему: «Технології захисту від атак ransomware»

Виконавець: студентка IV курсу, групи КБ-41

_____ **Андрейчук Ольга Валентинівна**
(підпис) (прізвище ім'я по-батькові)

	Прізвище, ініціали	**Підпис**
Керівник	Браіловський М.М.	

Нормоконтроль	Даков С.Ю.	

Київ 2021

Міністерство освіти і науки України
«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій

Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідувач кафедри кібербезпеки
та захисту інформації
_____ Н.В. Лукова-Чуйко
«10» жовтня 2020 р.

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньої програми)

Студентці **КБ-41** (група) **Андрейчук Ользі Валентинівні** (прізвище ім'я по-батькові)

Тема дипломної роботи Технології захисту від атак ransomware

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема дипломної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №2 від 08.10.2020 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Механізм роботи атак ransomware, таксономія шкідливого забезпечення.

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Необхідно ознайомитися з теорією атак з метою викупу та їх таксономією, типовою поведінкою на кожному етапі ланцюга нападу, проаналізувати можливі механізми захисту на кожній фазі attack chain, представити удосконалену методику захисту проти програм-шантажистів, що базуються на чотирьох етапах обрати та оптимальний метод захисту на етапі виявлення.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Вдосконалення технологій захисту проти атак ransomware та вибір оптимальної методики захисту на етапі виявлення.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання:12 жовтня 2020 року

Завдання видав	_____	М.М. Браіловський
	(підпис)	(ініціали, прізвище)
Завдання прийняла до виконання	_____	О. В. Андрейчук
	(підпис)	(ініціали, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	25.01.2021 – 3.02.2021	*виконано*
2	Аналіз літератури	5.02.2021 – 20.02.2021	*виконано*
3	Ransomware, історія виникнення	21.02.2021 – 22.02.2021	*виконано*
4	Дослідження таксономії ransomware	26.02.2021 – 7.03.2021	*виконано*
5	Аналіз ланцюга нападу атак з метою викупу	15.03.2021 – 2.04.2021	*виконано*
6	Дослідження задіяних у формуванні атаки технологій та механізмів захисту на кожному етапі attack chain	6.04.2020 – 26.04.2021	*виконано*
7	Представлення удосконаленої методики захисту проти програм-шантажистів, що базуються на чотирьох етапах та обрання оптимального методу захисту на етапі виявлення.	30.04.2021 – 15.05.2021	*виконано*
8	Оформлення пояснювальної записки	17.05.2021 – 28.05.2021	*виконано*
9	Підготовка до захисту дипломної роботи	30.05.2021 – 08.06.2021	*виконано*

Завдання видав	_____	М.М. Браіловський
	(підпис)	(ініціали, прізвище)
Завдання прийняв до виконання	_____	О. В. Андрейчук
	(підпис)	(ініціали, прізвище)

Термін подання дипломної роботи до ЕК 08 червня 2021 року

РЕФЕРАТ

Дипломна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, додатків, має 60 сторінок основного тексту, одну таблицю та 9 рисунків. Список використаних джерел містить 74 найменування та займає 7 сторінок.

Метою даної роботи є створення експериментальної бази для наукових досліджень та побудова ефективної захисної стратегії проти атак типу ransomware.

У роботі проаналізована існуюча література щодо атак з метою викупу , виконаний аналіз документів, порівняння, вивчення та узагальнення вітчизняної та зарубіжної практики з теми ransomware, розроблено рекомендації з вибору методу виявлення атак ransomware.

Представлена удосконалена методика захисту від атак з метою викупу, що базується на чотирьох основних етапах, може використовуватися працівниками корпоративних мереж для побудови ефективної системи захисту від ransomware.

Ключові слова: ransomware, викуп, технології захисту, біткоїн, honeypot.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

AES	–	Advanced Encryption Standard
ECC	–	Elliptic Curve Cryptography
RaaS	–	Ransomware as a service
DGA	–	Domain generation algorithms
IoT	–	Internet-of-Things
NLP	–	Natural Language Processing
NTFS	–	New Technology File System
MBR	–	Master Boot Record
CNN	–	Convolutional Neural Network
RNN	–	Recurrent Neural Network
SCADA	–	Supervisory Control And Data Acquisition
IED	–	Improvised Explosive Device
SIM	–	Security information management
SIEM	–	Security information and event management
FSRM	–	File Server Resource Manager
ПЗ	–	Програмне забезпечення
UBA	–	User Behavior Analitycs

ЗМІСТ

ВСТУП

Актуальність. Згідно з нещодавно опублікованими даними дослідників в області кібербезпеки, в 2020 році кількість атак з метою отримання викупу (або *ransomware*) зросло в сім разів, а власне технології їх здійснення стають все більш небезпечними, так як кіберзлочинці прагнуть зашифрувати якомога більшу частину корпоративної мережі з метою вимагання біткоїнів в обмін на відновлення важливих (конфіденційних) даних. В результаті однієї такої атаки підприємства втрачають сотні тисяч або навіть мільйони доларів. Стабільно зростаючий список компаній, які стали жертвами подібних атак, повідомляє, що інші витрати, пов'язані з атакою, – обладнання, втрачені можливості збуту, незадоволені клієнти, кошти на зменшення наслідків атаки та відновлення, зіпсована репутація компанії, штрафи за невиконання договірних зобов'язань перед клієнтами – роблять зазначену хакерами вартість викупу тривіальною. За даними фірми Emsisoft, що займається питаннями з кібербезпеки, на початку 2020 року межа між атаками з метою отримання викупу і витоком даних продовжує розмиватися, і ряд успішних «операторів викупу» (Maze, Sodinokibi, DoppelPaymer, Nemty, Nefilim, CLOP і Sekhmet) створюють власні веб-сайти, на яких публікують вкрадені дані неплатоспроможних жертв.

На сьогоднішній день відомі три основні види ransomware: scareware – програми-вимагачі, що заважають роботі з інтернет-браузерами, перекриваючи основне вікно рекламним банером або залякуючи користувачів фальшивими протизаконними діями, ціль злочинців – вимагання коштів за розблокування; screen locker (є найпоширенішим в зв'язку з простотою написання подібних програм) – працює методом блокування доступу до операційної системи жертви, роблячи роботу з комп'ютером повністю або частково неможливою, класичним прикладом даного виду шкідливих програм є WinLocker; encrypting ransomware – програма-шантажист піддає файли жертви криптографічному перетворенню і

вимагає заплатити за надання ключа розшифрування або спеціальної утиліти-декриптора.

Таким чином, знаходження оптимальних методів захисту проти атак типу ransomware є актуальною задачею.

Метою дипломної роботи «Технології захисту проти атак ransomware» є створення експериментальної бази для наукових досліджень та побудова ефективної захисної стратегії проти атак типу ransomware.

Для досягнення зазначеної мети дипломної роботи поставлені окремі завдання:

– провести аналітичний огляд атак з метою отримання викупу;

– дослідити таксономію атак ransomware;

– проаналізувати ransomware attack chain та розглянути кожний етап перебування програм-вимагачів у системі;

– дослідити задіяні технології в формуванні загроз типу ransomware;

– запропонувати технології захисту на кожному етапі визначеного attack chain;

– обрати ефективний метод виявлення з технологією honeypot;

– зробити висновки щодо запровадження технологій захисту від ransomware.

Об’єктом дослідження дипломної роботи є процес аналізу атак ransomware та традиційних механізмів захисту.

Предметом дослідження дипломної роботи є розробка методів захисту проти програм-шантажистів, що базуються на чотирьох етапах, а також налаштування технології honeypot на етапі виявлення ransomware.

У процесі виконання та збору необхідної інформації для дипломної роботи було використано наступні методи:

– аналіз;

– системний підхід;

– історичний метод;

– синтез.

Практична цінність кваліфікаційної роботи полягає в наступному:

– вдосконалення технологій захисту проти атак ransomware;

– представлення чотирьох-етапного комплексу захисту від атак ransomware;

– представлення методів виявлення з технологією honeypot.

Отже, запровадження ефективних технологій захисту від програм-шантажистів є важливим рішенням для безпеки персональних даних, збереження коштів підприємствами та усунення негативних наслідків перебування ransomware в корпоративних мережах.

РОЗДІЛ 1
ПОНЯТТЯ RANSOMWARE. ТАКСОНОМІЯ АТАК RANSOMWARE. RANSOMWARE ATTACK CHAIN

1.1 Поняття ransomware. Історія виникнення атак з метою отримання викупу

Ransomware – одна з найнебезпечніших кіберзагроз, з якими мають справу як приватні особи, так і організації. За даними Kaspersky Lab ICS CERT 2017 рік був важким з точки зору руйнівних атак. Однією з головних глобальних загроз для користувачів стало ransomware. Компанія Verizon Enterprise назвала ransomware найпоширенішим видом шкідливого ПЗ в 2018 році в звіті Data Breach Investigations Report (DBIR).

Ransomware – це шкідливе ПЗ, яке вимагає викуп, беручи в заручники ресурси користувачів. Це вимагання можливе через страх жертви втратити цифрові активи або позбутися доступу до них. Концепція ransomware або шкідливих програм, заснованих на вимаганні, була вперше офіційно представлена доктором Джозефом Поппом в 1989 році з випуском "AIDS Information Trojan" [10]. Троян AIDS поширювався через заражені дискети з фальшивою обкладинкою "PC Cyborg Corporation" серед жертв. Він атакував користувачів, шифруючи і спотворюючи імена їх файлів і вимагаючи заплатити 189 доларів США за відновлення файлів. Модус операнди AIDS полягав в заміні файлу AUTOEXEC.BAT шкідливими інструкціями, в результаті чого машина жертви ставала непридатною для використання при 90-му завантаженні системи. Незважаючи на те, що троян AIDS використовував складні техніки, він мав кілька недоліків. Одним з недоліків було те, що цей троян використовував симетричну криптографію і вбудовував ключ в саму шкідливу програму.

Після цього Адам Янг і Моті Юнг [11] запропонували ідею використання асиметричної криптографії (а ще краще – гібридної) для вірусів з високим

виживанням. На сайті автори використовували шифрування з відкритим ключем в криптовірусологічних атаках і продемонстрували, що воно необхідне для таких загроз. Вірус One-Half, вірус LZR, троян AIDS Info і вірус KOH – це зразки шкідливих програм, які були досліджені в їх науковій роботі. В даний час цей метод застосовується до криптографічних викупних програм.

Протягом наступних 10 років з'являлося лише кілька варіантів, але справжня загроза викупу – тільки в 2004 році, коли GpCode використовував слабке RSA-шифрування для отримання винагороди за особисті файли.

У 2007 році WinLock став передвісником появи нового типу програм-викупів, які замість шифрування файлів блокували робочий стіл. WinLock захоплював екран жертви і показував порнографічні зображення. Потім він вимагав оплати через платне SMS-повідомлення, щоб видалити їх.

Незважаючи на тривалий період затримки, ransomware знову з'явилися, а їх інтенсивність і різноманітність досягли піку за останні кілька років. З 2012 року шахрайські програми-викупи і їх бізнес-модель знову стали процвітати. CryptoLocker, про який повідомлялося в 2013 році, був різновидом криптографічного ransomware, який став першопрохідцем у прибутковій індустрії криптографічного ransomware. Він заразив понад 250 000 систем менш ніж за чотири місяці, а його дохід досяг більше 3 мільйонів доларів. З появою ransomware as-a-service (RaaS) і систем платежів, які не можна вислідкувати, ця торгівля на підпільному ринку стала більш серйозною. Поява RaaS надало можливість розробки і вдосконалення нових варіантів ransomware кожному кіберзлочинцю, що навіть не володіє необхідними навичками.

У грудні 2017 року з'явився імітатор під назвою Locker. Його викуп становив 150 доларів, оплата проводилася за допомогою Perfect Money або номерів віртуальної карти QIWI Visa Virtual Card. Пізніше в грудні був випущений CryptoLocker 2.0. Він був написаний іншою мовою, ніж CryptoLocker, і тому, ймовірно, випущений іншими зловмисниками. Протягом 2013 року, за оцінками Symantec, кількість атак зросла з 100 000 в січні до 600 000 на грудні. Вони також підрахували, що три відсотки заражених користувачів заплатили викуп. З вересня

2013 року по травень 2014 року, за оцінками, понад 500 000 жертв були заражені. У червні Operation Tovar, коаліція правоохоронних органів, виробників систем безпеки і вчених, знищила сервери поширення CryptoLocker. Два постачальника, FireEye і Fox-IT, знайшли базу даних ключів розшифровки всіх жертв CryptoLocker і випустили сервіс, що дозволяє безкоштовно розшифровувати дані всім жертвам. У лютому знайшла своє місце програма CryptoDefense. Це була досить слабка частина ransomware, але все ж в перший місяць вона заробила 34 000 доларів. У квітні була випущена поліпшена версія під назвою CryptoWall. Вона використовувала уразливість Java і поширювалася через шкідливу рекламу. Ця версія принесла більше $ 1 000 000 викупу.

У січні 2016 року з’явилась програма-вимагач, що використовує тільки JavaScript. Використання JavaScript дозволяє атакувати безліч платформ, включаючи Linus і MacOS X. У лютому здирницькі ПЗ заразили тисячі сайтів WordPress. WordPress – це популярна платформа для ведення блогів.

Apple довелося випустити оновлення, щоб заблокувати здирницькі програми KeRanger. Вважається, що KeRanger – це перша атака ransomware, спрямована на комп'ютери Apple. Після встановлення KeRanger активується протягом трьох днів і призначений для шифрування більше 300 типів файлів. У лютому в Австралії і Росії було виявлено шкідливе ПЗ під назвою Xbot, націлене на пристрої Android. Воно не тільки шифрує файли, але і намагається вкрасти дані онлайн-банкінгу. У липні в програму Locky ransomware був доданий механізм захисту від збоїв, який починає шифрувати файли, навіть якщо програма не може запросити унікальний ключ шифрування з серверів зловмисників через те, що цільовий комп'ютер знаходиться в автономному режимі або блокує зв'язок. За оцінками ФБР, за перші три місяці 2016 року дохід від ransomware склав $ 209 000 000.

Три найбільш поширені версії на 2017 рік – CryptoWall, CTB-Locker і TorrentLocker. CryptoWall – це поліпшена версія CryptoDefense. Вона шифрує файли не тільки на зараженому комп'ютері, але і на всіх підключених до нього зовнішніх накопичувачах або дисках загального доступу. CTB-Locker – це скорочення від curve-Tor-Bitcoin. І CryptoWall, і CTB-Locker мають партнерські програми продажів.

TorrentLocker збирає адреси електронної пошти, коли заражає комп'ютер, щоб розсилати спам іншим користувачам.

Спалах таких атак, як WannaCry, Petya і NotPetya, отримав велику популярність і увагу в 2017 році. Відповідно до звітів, середня сума, запитувана в якості викупу, зазвичай становить від 300 до 700 доларів США для приватних осіб і від 10 000 до 17 000 доларів США для підприємств. Ransomware вражає не тільки сервери і персональні комп'ютери, але і всі обчислювальні системи, включаючи смартфони, IoT-пристрої, ICS / SCADA і багато інших, як показано на рис. 1. Тому боротьба з ним є однією з вимог безпеки будь-якої організації.

Виявлення сімейств ransomware залишається складним завданням через еволюцію технологій і постійного вдосконалення використовуваних методів, які відіграють важливу роль.

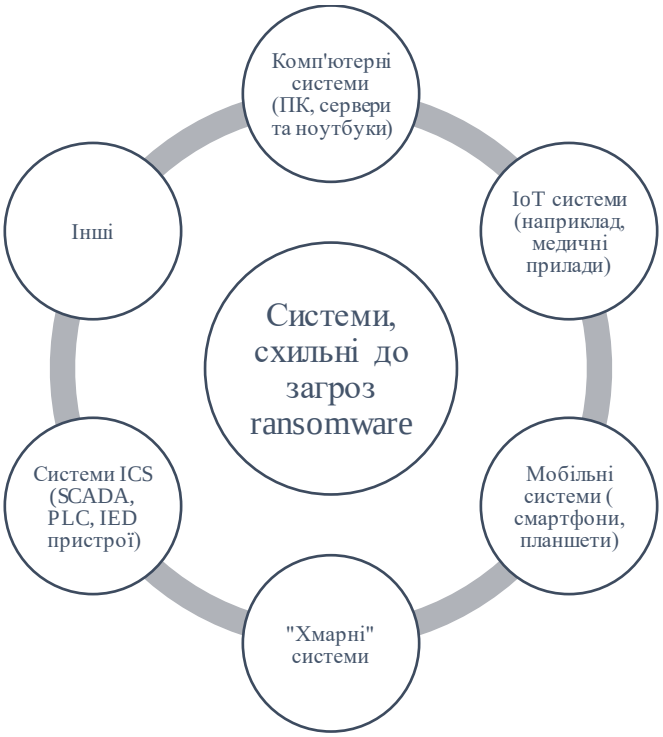

Рис. 1.1 Цілі атак ransomware

Отже, самостійне уявлення про задіяні компоненти може бути ефективним при розробці рішень для захисту від атак ransomware і обходу нових їх різновидів.

1.2 Таксономія атак ransomware

З постійним розвитком і ускладненням сімейств ransomware дослідники безпеки почали вводити ряд таксономій, щоб полегшити розуміння атак ransomware і реалізувати відповідні контрзаходи з мінімальними втратами цифрових активів. Кібератаки можна класифікувати декількома способами, щоб краще зрозуміти їх функціональність і рівень загрози. Луо і Ляо [49] класифікували ransomware в залежності від ступеня загрози. Вони відрізнили здирницькі програми від справжніх. Потім, відповідно до запропонованого ними методу, реальні ransomware були розділені на прості атаки і шифрування з різною довжиною ключа.

Таксономія, запропонована Ахмадіаном [51], просто класифікувала здирницькі програми на некриптографічні і криптографічні, та не розглядала всі атаки, засновані на вимаганні. Аль-Рімі та інші [15] класифікували ransomware з трьох точок зору, а саме: серйозності, платформи і цілі. Цей підхід, заснований на ступенях серйозності, розділяє загрозу на програми-залякування та шкідливі програми-вимагачі. Надалі вони поділяють їх на програми-блокувальники та крипто-рандомні програми. Баджпаі розглядає таксономію здирницьких програм з точки зору управління ключами.

З огляду на популярність здирницьких атак та великого поширення нових видів, відсутність всеосяжної класифікації, що охоплює всі здирницькі атаки, все ще відчувається. Нижче наведена ієрархічна та послідовна таксономія ransomware, яка охоплює всі загрози, засновані на залякуванні, на рисунку 2. У загальному випадку під шкідливим ПЗ розуміється будь-який шкідливий код, який використовується злочинцем для реалізації злих намірів в системі без дозволу і відома її власника [19, 52]. Ransomware – це різновид шкідливих програм, який може потрапити в підкатегорію scareware. Однак в деяких відкритих джерелах інформації scareware розглядається як різновид ransomware. На думку багатьох дослідників, більш доречно відносити ransomware до підкатегорії scareware-атак, оскільки вони використовують метод залякування людей в своїх незаконних і прибуткових цілях.

Scareware – це форма шкідливих програм, яка, лякаючи людей уявними чи реальними загрозами, змушують їх робити спеціальні дії. Як правило, всі атаки scareware можна назвати погрозами, заснованими на вимаганні. У цьому ж сенсі програми для залякування поділяються на три категорії, які будуть описані нижче.

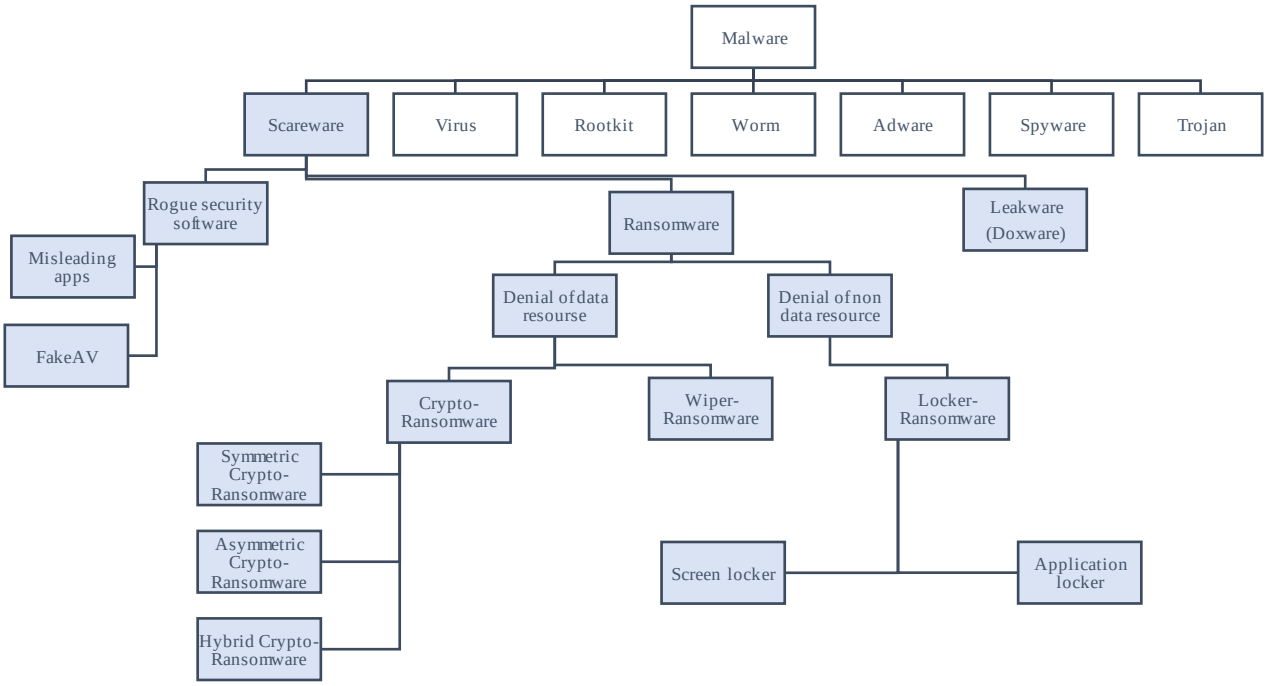

Рис. 1.2 Таксономія атак ransomware

1.2.1. Rogue security software або несумлінне програмне забезпечення безпеки

Це шахрайське програмне забезпечення безпеки є однією з найвідоміших і найпоширеніших програм-залякувачів. Воно є оманливою програмою, яка видає себе за анти-шпигунське ПЗ або легітимну системну утиліту, але насправді сама є шкідливим ПЗ. Така програма робить вигляд, що вона виявила потенційні шкідливі елементи або незаконний вміст на комп'ютері жертви. Основна відмінність шахрайської утиліти від класичного ransomware полягає в тому, що шахрайські програми, як правило, не закривають доступ до ресурсів і не пошкоджують пристрій жертви. Найчастіше вони з'являються у вигляді проблемної програми, що працює у фоновому режимі, та постійно повідомляють користувачів про фальшиві сигнали безпеки, переконуючи їх придбати пропоноване рішення безпеки. Підроблений

антивірус (FakeAV) є одним з найпоширеніших шахрайських програм, які були капіталізовані до сих пір. FakeAV повідомляє користувачам, що в їх системі знаходиться шкідливий код, і стверджує, що вони просто зобов'язані придбати його програмне забезпечення. Але насправді, рішення, запропоноване групою, що стоїть за FakeAV, робить не більше ніж видалення самої шкідливої програми. У більшості випадків метою шахрайського додатку є отримання грошей від жертв або почати більш серйозну атаку.

1.2.2 Ransomware

Поява ransomware призвело до кардинальних змін в індустрії програм-залякувань. Цей клас шкідливих програм, взявши в заручники ресурси користувача і вимагаючи викуп за їх звільнення у вигляді сплати грошей, покупки програмного забезпечення або виконання спеціального завдання, став прибутковою бізнес-моделлю серед інших атак. Ключовою особливістю, що відрізняє ransomware від інших типів scareware, є конфіскація пристрої жертви або цінних даних і позбавлення користувача доступу до них. Залежно від захопленого ресурсу, ransomware поділяється на два класи: відмова в доступі до ресурсу даних і відмова в доступі до ресурсу, що не пов'язано з даними.

Відмова в доступі до ресурсів даних (DoDR). Найцінніший актив в комп'ютерній системі – це дані. Цей клас ransomware блокує доступ до ресурсів даних (файлів) і вимагає від жертв заплатити викуп, якщо вони хочуть повернути доступ до даних. Crypto-ransomware є найбільш поширеним з цієї категорії. Хоча криптографія відома як чисто захисна технологія від несанкціонованого доступу, crypto-ransomware використовує цю техніку в наступальних цілях для шифрування важливих даних і вимагає викуп за обмін ключа шифрування. Можна сказати, що троян AIDS Info є першим виявленим і задокументованим crypto-ransomware або криптографічною атакою з метою викупу. Ця атака не була настільки успішною, оскільки ключ дешифрування можна було витягти з коду трояна. Звідси виникла ідея використання асиметричного ключа і гібридних методів. Таким чином, в

залежності від механізму шифрування, crypto-ransomware можна розділити на три групи: симетричні, асиметричні і гібридні.

У симетричних криптопрограмах один і той же ключ використовується як для шифрування, так і для дешифрування. Одним з ключових переваг цього підходу є швидкість його роботи, що призводить до підвищення ефективності атак ransomware. Однак невмілий спосіб управління ключем викриває його. В асиметричних криптопрограмах для шифрування і дешифрування використовуються різні ключі. Використання асиметричної криптосистеми (також відомої як шифрування з відкритим ключем) дозволяє використовувати сильнішу форму криптовірусних атак. При цьому використовується закритий ключ, який відомий тільки власнику шкідливої програми. Після шифрування даних за допомогою відкритого ключа жертвам потрібен закритий ключ, щоб розшифрувати і повернути свої файли. До переваг цього криптографічного методу можна віднести стійкість і практично незламність. Основним недоліком цього підходу є його повільність, що є проблемою при кібератаці.

Гібридний механізм об'єднує симетричну і асиметричну криптографію, щоб отримати найкраще з обох методів. У гібридній стратегії асиметрична криптографія використовується для надійного шифрування сеансового ключа, який є симетричним шифром, використовуваним вимагачами для шифрування даних [11, 50]. Наприклад, TorrentLocker є зразком, який використовує алгоритми RSA і AES. Випадково згенерований ключ AES шифрується RSA. Як інший приклад можна привести варіант Gpcode, який шифрує дані за допомогою унікального секретного ключа AES-256 і повторно шифрує цей ключ 1024-бітовим відкритим ключем RSA [22,23]. CTB-Locker (Curve-Tor-Bitcoin-Locker) також віднесений до класу гібридних крипто-рандомних програм, що використовують комбінацію AES і криптографію Elliptic Curve Cryptography (ECC). Крім алгоритму криптографії, зловмисники можуть використовувати як стандартні (наприклад, CryptoAPI, що надається платформою Windows), так і власні криптосистеми під час атак.

Хоча crypto-ransomware – найпопулярніший та досить успішний клас відмови в доступі до ресурсів даних, він не єдиний. Шкідливі програми, які позбавляють

користувачів доступу до ресурсів до тих пір, поки вони не заплатять або не виконають будь-яку дію, вважаються ransomware. Wiper – це ще одна категорія здирницьких програм DoDR. Незважаючи на те, що wiper можна віднести до окремої групи шкідливих програм, метою яких є знищення критично важливих файлів, він зустрічається в декількох атаках, заснованих на вимаганні. Отже, ця атака визначена як підмножина DoDR ransomware. Звичайний wiper спрямований скоріше на знищення, ніж на отримання фінансової вигоди. Shamoon і StoneDrill – сумнозвісні сімейства, що відносяться до класичних програм типу wiper-ransomware [9, 30]. В основному, більшість wiper-ransomware мають можливість модифікувати і перезаписувати головний завантажувальний запис (MBR), який відповідає за завантаження операційної системи, своїм шкідливим кодом, щоб зробити систему марною, видаливши ресурс даних. Хоча ця функціональність може існувати і в інших родинах ransomware. Існує безліч методик знищення даних, що дозволяють зробити їх непридатними для використання. У разі crypto-ransomware для цього застосовується несанкціоноване шифрування даних. Але в категорії Wiper використовується або несанкціонована заміна даних, або їх шифрування (зрозуміло, без ключа розшифрування). Клас Wiper вимагає менших зусиль. Незважаючи на визначену структуру wiper-ransomware, деякі атаки crypto-ransomware можуть випадково потрапити в цю категорію через помилки в їх реалізації. WannaCry є прикладом атак на знищення даних в 2017 році. Вона використовувала комбінацію AES і RSA для шифрування файлів і генерувала унікальну адресу гаманця Bitcoin для кожної жертви. Однак через помилки цей код виконувався некоректно. Противники не могли визначити, хто з жертв заплатив. Згодом у жертв не було ніяких шансів відновити доступ до своїх файлів [13]. Крім WannaCry, Petya, PetWrap, NotPetya, AnonPop, Ordinypt і MBR-ONI з'явилися руйнівні атаки, які можна віднести до класу wiper-ransomware в запропонованій таксономії. Наприклад, Ordinypt – це різновид wiper-ransomware, який замінює вміст файлів випадковими даними і вимагає викуп у розмірі 0,12 біткоїнів.

Відмова в доступі до ресурсів, що не містять даних (DoNR). Друга категорія ransomware позбавляє жертву доступу до пристрою або системних утиліт, але

залишає дані користувача недоторканими. На перший погляд дані можуть здатися недоступними, але головна відмінність від попередньої групи (тобто DoDR) полягає в тому, що дані не будуть підроблені або знищені.

Таким чином, це робить DoNR менш ефективним у вимаганні викупу у жертв у порівнянні з його аналогом. Найвідомішим і, можливо, єдиним ідентифікованим класом, що належить до DoNR, є locker-ransomware, який використовує механізми блокування проти жертв. Оскільки атаки locker-ransomware, подібно нелегальному захисному ПЗ, не несуть смертельної загрози для пристроїв і не знищують дані, вони повинні використовувати методи соціальної інженерії, щоб переконати і змусити жертв заплатити викуп. IoT-пристрої, особливо в сфері охорони здоров'я і надзвичайних ситуацій, є привабливими цілями для цього типу атак. Категорія locker-ransomware більше націлена на мобільні, IoT і ICS пристрої, ніж на комп'ютерні системи або хмарні сховища, в яких зберігаються цінні дані. Залежно від заблокованих ресурсів, що не відносяться до даних, атаки

Locker-ransomware діляться на підкласи. Ці ресурси можуть включати в себе операційну систему, додатки, сервіси, призначені для користувача інтерфейси і багато інших програм. Наприклад, Trojan.Ransomlock.G [46] блокує екран користувача і відображає повноекранну записку з викупом, яка займає весь робочий стіл. Крім того, перший варіант DeriaLock був тільки блокувальником екрану і вимагав оплати. Lockdroid і його варіанти націлені на платформи Android і використовують ряд психологічних прийомів, щоб переконати жертву заплатити викуп. Reveton – ще один зразок Locker Ransomware, який блокує екран і залишає файли недоторканими. Він також відключає диспетчер задач і видає себе за повідомлення від правоохоронних органів, які помітили незаконну діяльність на машині жертви. Деякі інші різновиди locker-ransomware блокують браузер. Більшість блокувальників браузера є клієнтськими кросплатформами(як наприклад, Browlock).

1.2.3 Програми-вимагачі (Doxware)

Загрози, засновані на вимаганні, досягли нового рівня небезпеки. Ще одна категорія програм-залякувань, – це програми-витоки (також відомі як Doxware). Це нова еволюція цифрового захоплення і кібершантажа. Слово "doxing" означає публікацію конфіденційної і особистої інформації в Інтернеті. Doxware використовує механізми програм-шпигунів і викрадачів інформації, а в деяких випадках поєднує їх з методологіями ransomware, такими як криптографія або блокування. Замість того, щоб позбавити користувача доступу до ресурсів (в основному до приватних і цінних даних), Leakware робить їх видимими для всіх, якщо жертва не заплатить викуп.

Вперше ця концепція була формально сформульована Адамом Янгом, який представив у 2003 році криптовірус з новою функцією [21]. «Теорія ігор» була задіяна як невід'ємна частина самої атаки, яка була запущена на хост. Вона використовувалася для аналізу ефективності запропонованої атаки. З 2017 року загроза стала більш небезпечною. В цілому, Leakware небезпечніше всіх різновидів ransomware, оскільки стратегії резервного копіювання не можуть пом'якшити збитки. Що робить Leakware гірше і наполегливіше інших атак, заснованих на вимаганні, так це те, що навіть якщо жертва заплатить викуп, їй все одно може загрожувати небезпека, оскільки копія даних знаходиться в руках злочинців. Судячи з усього, Charger (з назвою додатка EnergyRescue) – це додаток для економії заряду батареї для платформ Android. Воно викрадає SMS-повідомлення та список контактів користувача, а також блокує пристрій. Потім воно шантажує жертву, погрожуючи продати її особисту інформацію на чорному ринку.

1.3 Ланцюг нападу ransomware

Атаки ransomware і їх види ростуть з неймовірною швидкістю. Їх здатність вражати окремих користувачів та організації, невеликий ризик і витрати для зловмисників, відсутність необхідності шукати покупця на вкрадені дані,

можливість розгортання на численних пристроях і, таким чином, накладення більших викупів, зробили ransomware цікавим інструментом з точки зору противників. Щоб ефективно боротися з такою кіберзагрозою, необхідно розуміти етапи атаки. Поділ процесу атаки дозволяє дослідникам і фахівцям з безпеки мати загальний договір, в рамках якого вони можуть донести свої ідеї та обговорити проблему виявлення та припинення загрози на кожному етапі атаки.

Атака ransomware починається в той момент, коли шкідливе корисне навантаження доставляється через один із векторів зараження на комп'ютер жертви. Успішна атака ransomware після отримання контролю над пристроєм забороняє користувачам доступ до нього або зберігаються на ньому даними. Превентивні дії в основному включають шифрування і блокування. Наступним кроком є залишення записки з викупом та інформування користувача про те, що його ресурси стали недоступними. Щоб вижити в кіберсвіті, кампанії по боротьбі з вимаганням повинні взяти на себе зобов'язання звільняти заручників (наприклад, розшифрувавши ресурси даних або розблокувавши ресурси, що не належать до даних) після отримання викупу. Відповідно, доречно навести цикл атаки, який охоплює всі види ransomware, незалежно від методології, використовуваної для захоплення ресурсу. На рис. 1.3 показаний кожен з етапів атаки.

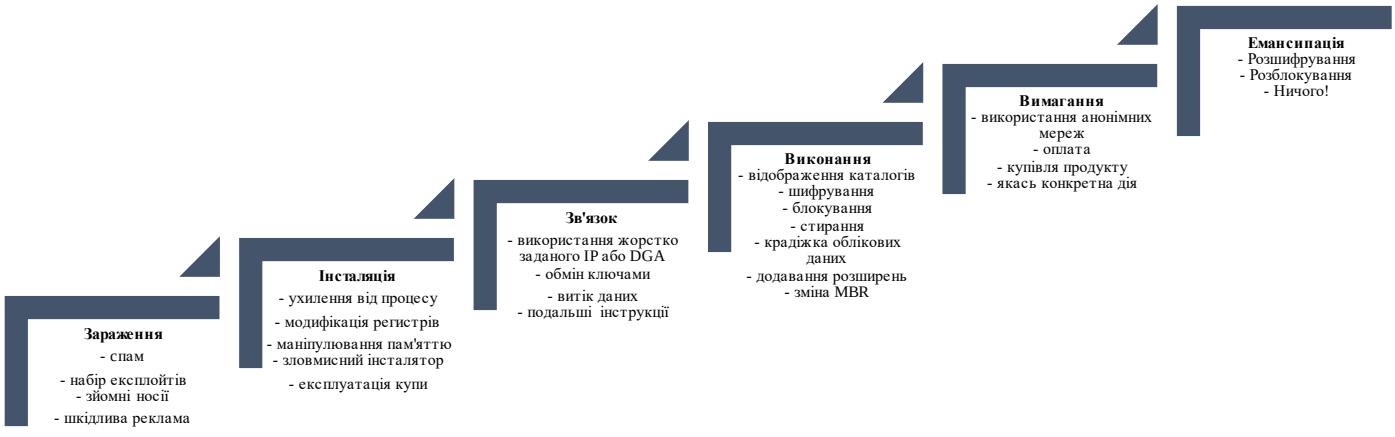

Рис. 1.3 Запропонований attack chain для всіх типів ransomware

У таблиці 1, що знаходиться у додатку А, представлені індикатори, виведені з деяких інших зразків програм з метою викупу (включаючи crypto та wiper-ransomware) на кожному етапі ланцюга нападу ransomware.

1.3.1 Етап зараження

Всі атаки ransomware починаються з моменту доставки шкідливого коду жертві. Це завдання вирішується за допомогою векторів зараження на першому етапі ланцюжка атак – етапі зараження. Хоча існує безліч векторів зараження, в атаках ransomware в основному використовуються фішингові спам-листи та набори експлойтів. Спам містить або шкідливі вкладення (наприклад, документ Microsoft Office, що містить макрос, PDF-файл з JavaScript), або посилання на зламаний веб-сайт. Перший вектор вимагає взаємодії з користувачем для натискання і завантаження шкідливого навантаження, в той час як другий – ні. Незважаючи на те, що набори експлойтів за своєю природою є набором експлойтів "нульового дня", противники вважають за краще поширювати ransomware за допомогою фішингових листів і методів соціальної інженерії. У разі мобільного ransomware одним з найбільш поширених векторів зараження є завантаження шкідливої програми з ненадійних сайтів або з магазинів додатків, які не мають необхідного контролю безпеки. Charger [33] і Lockdroid є зразками цієї групи.

Перша відома програма-вимагач, троян AIDS, використовувала заражені дискети для доставки шкідливого ПЗ жертвам. З розширенням ботнетів і їх процвітанням в розсилці величезної кількості спаму електронною поштою, швидкість прийняття спаму була збільшена для поширення шкідливого ПЗ серед якомога більшого числа користувачів. CryptoLocker використовував ботнет Gameover ZeuS для поширення через спам серед багатьох своїх жертв. Аналогічно, CryptoWall, Cerber, Jaff і Locky – інші успішні програми-вимагачі, які поширюються через спам.

Проте, в поширенні ransomware помітний слід декількох наборів експлойтів. Відповідно до звітів, Angler, Neutrino, Magnitude, Nuclear і RIG - це набори експлойтів, які використовувалися в якості методів доставки в деяких родинах ransomware, таких як CryptXXX, CryptoWall, Cerber і Locky [31].

Хоча більшість варіантів ransomware поширюються через зазначені вектори зараження, є види, які діють за принципом «саморозповсюдження». З цієї причини

очікується поява нової епохи "крипточерв'яків" в атаках кібервимагачів. Ця концепція більш очевидна, оскільки спам-кампанії стають все менш ефективними. WannaCry є більш шкідливим, ніж інші поширені ransomware, завдяки властивості «саморозповсюдження», яка дозволяє йому використовувати критичні уразливості на етапі зараження [14]. До появи WannaCry подібну поведінку демонстрував ZCryptor, який використовував червоподібний вектор зараження на платформі Windows [31].

1.3.2 Етап інсталяції

«Корисне навантаження» найчастіше завантажується через дропери. Після доставки шкідливого коду на машину жертви за допомогою вищезазначених векторів, ransomware переходить в фазу встановлення. На цьому етапі ransomware має встановити себе в системі та отримати контроль над пристроєм, не привертаючи уваги програм безпеки. Для цього ransomware використовує різні техніки. Одним з методів, який тяжко розпізнати засобам захисту на основі сигнатур, є впровадження коду.

Process Hollowing – це техніка впровадження коду, яка використовується шкідливими програмами, щоб приховати себе. Наприклад, TorrentLocker використовував цю техніку для впровадження шкідливого коду в легітимний процес Windows. В якості прихованого процесу він використовує explorer.exe. Аналогічно, CryptoWall і GlobeImposter – інші зразки, які використовують Process Hollowing для здійснення своєї діяльності з, здавалося б, легального процесу. Process Doppelgänging – це нова і дуже підступна техніка міжпроцесного впровадження. Ця техніка дещо схожа на process hollowing і допомагає обійти більшість сучасних систем безпеки. Process Doppelgänging використовує переваги транзакції NTFS для маскування завантаження виконуваного файлу. Він вважається безфайловою атакою, оскільки шкідливий код не зберігається на диску.

SynAck – перша родина здирницьких програм, яка застосувала технологію Process Doppelgänginging, яка дозволяє уникнути сканування файлів в режимі

реального часу [53]. Ще один оманливий метод обходу антивірусних рішень під час установки – заховати шкідливе ПЗ в пакеті програми установки. Останнім часом спостерігається хвиля нових шкідливих інсталяторів Nullsoft Scriptable Install System (NSIS), що використовуються в кампаніях ransomware. Вони намагаються виглядати якомога більш «нормальними» з включенням нешкідливих компонентів. У новій версії інсталяторів NSIS сценарій установки Nullsoft відповідає за завантаження зашифрованого корисного навантаження в пам'ять, її розшифровку та виконання її кодової області. NSIS був помічений в інсталяторі, що скидають сумнозвісні сімейства ransomware, такі як Cerber, Locky, CryptoWall, Wadhrama і CTB-Locker [54]. У багатьох зразках crypto-ransomware або wiper-ransomware, щоб переконатися в неможливості відновлення зашифрованих даних, тіньові копії томів видаляються за допомогою інструменту vssadmin.exe [55]. Також деякі зміни ransomware вносить в систему, щоб зберегти їх між перезавантаженнями системи і помістити в запуск, в залежності від платформи.

1.3.3 Етап зв'язку

Після завершення встановлення ransomware починає збирати інформацію про жертву. Ця інформація, яка згодом видаляється, включає IP-адресу жертви, місце розташування, операційну систему, версію браузера і його плагінів, інструменти безпеки, встановлені на пристрої, і так далі. Деякі сімейства ransomware вимагають початкового спілкування з основними зловмисниками для виконання своїх подальших дій. На етапі зв'язку ransomware починає з'єднуватися зі своїм командно-контрольним (C&C або C2) сервером.

Така поведінка часто зустрічається в багатьох інших типах шкідливого ПЗ. Але в атаках ransomware, особливо в разі crypto ransomware, цей зв'язок здійснюється в основному з метою обміну ключем шифрування та отримання необхідних інструкцій для продовження атаки. З'єднання з C&C-сервером здійснюється або через IP-адресу, або через доменне ім'я. Оскільки жорстко закодовані IP-адреси і доменні імена в самій шкідливій програмі були виявлені

аналітичними методами і привели до поразки атаки, зловмисники стали використовувати прийоми для протидії і анонімізації своїх комунікацій.

Щоб приховати місце розташування противника і домогтися анонімності, кіберзлочинці, що створюють ransomware, використовують системи, що забезпечують анонімні мережеві комунікації, такі як The Onion Router (Tor) і Invisible Internet Project (I2P) [46]. Інший недавно використаний прийом – алгоритми генерації доменів (DGA), які створюють доменні імена для операцій C&C з декількома рівнями перенаправлення для поліпшення обфускації і зниження ймовірності злому [46, 56]. У цьому механізмі код, вбудований в двійковий файл шкідливої програми, використовується для створення «насіння» для генерації псевдовипадкових доменів.

Потім програма-вимагач виконує DNS-запити для пошуку потенційних зареєстрованих доменів для зв'язку з сервером C&C [56]. У разі мобільних атак ransomware більшість з них використовують прості з'єднання HTTP / S для зв'язку з сервером C&C. Нещодавно помітили новий варіант Simplocker, який використовує Extensible Messaging and Presence Protocol (XMPP) для обходу заходів безпеки. Він використовує цей легітимний сервер ретрансляції повідомлень для зв'язку з сервером C&C. В результаті його комунікація виглядає нормально і ускладнює відстеження трафіку C&C. Крім того, всі повідомлення через XMPP можуть бути зашифровані за допомогою протоколу Transport Layer Security (TLS) [35].

Фаза комунікації є дуже важливою в деяких родинах здирницьких програм. Наприклад, CryptoLocker намагається знайти активний C&C-сервер і підключитися до нього через DGA, що генерує домени. Якщо з'єднання не вдалося, шкідливий експлойт не запускається, і зразок не надходить на етап виконання. TorrentLocker – ще один приклад, який не шифрує файли, якщо не вдається підключитися до його командного серверу [55]. На відміну від TorrentLocker, такі види ransomware, як Bart і нова версія RAA, не потребують підключення до C&C серверу для виконання своїх операцій і шифрування даних.

1.3.4 Етап виконання

Як зазначалося в підрозділі 1.2, основна відмінність ransomware від інших атак, заснованих на залякуваннях, полягає в перешкоджанні доступу користувачів до цифрових ресурсів (дані або НЕ дані). Ця мета досягається за допомогою різних механізмів, включаючи шифрування, блокування або видалення. У категоріях crypto-ransomware і wiper потрібен етап пошуку важливих файлів, які повинні бути атаковані.

Стратегія пошуку різниться для різних типів ransomware. Процес пошуку може бути як простим, коли шукаються файли з певними розширеннями, так і більш складним, коли враховуються останні звернення до файлів або ентропія файлів. Деякі зразки програм-вимагачів використовують функції управління томами Windows, такі як GetLogicalDrives і GetDriveType, щоб знайти мережеві диски для виконання деструктивних дій і шифрування вмісту, цільових файлів. Після перерахування всіх каталогів, в залежності від алгоритму криптографії або використовуваної стратегії, починається шкідлива операція над ресурсами даних. Шифруванню або маніпуляціям піддаються тільки ті файли, які відповідають заданим розширенням (або умовам).

У переважній більшості родин crypto-ransomware, що використовують алгоритми швидкої симетричної криптографії, розклад ключів обчислюється заздалегідь. Це призводить до того, що весь розклад ключів знаходиться в пам'яті протягом всього процесу шифрування. У разі асиметричних і гібридних крипто-рандомних програм ключ, необхідний для шифрування, передається на машину жертви на етапі обміну даними (або зв'язку). Однак в деяких варіантах цей ключ генерується на машині жертви і відправляється назад на C&C-сервер. Після підробки вибраних файлів, в залежності від типу ransomware, до кінця імені уражених файлів буде додано нове спеціальне розширення. Деякі види не тільки шифрують вміст файлів і роблять їх непридатними для використання, але і змінюють імена файлів. Через це жертва не зможе правильно оцінити розмір збитку.

Сімейства crypto-ransomware можуть використовувати різні криптографічні алгоритми поряд зі стандартними або спеціалізованими криптосистемами. Наприклад, RansomCrypt після запуску на машині починає перебирати всі файли і шифрувати їх за допомогою стандартного алгоритму TEA, простого блочного шифру. Інші сімейства, такі як Locky і CryptoLocker, можуть використовувати більш складні блокові шифри, такі як AES, поряд з іншим алгоритмом для шифрування вмісту цільових файлів.

У видах, що відносяться до категорії Wiper, на цьому етапі вміст цільових файлів може бути перезаписано небажаними даними. В атаках на відмову в доступі до ресурсів, що не відносяться до даних, цільові ресурси ідентифікуються і обмежуються механізмами блокування. При такій атаці замість маніпуляцій з ресурсом даних сам пристрій або деякі додатки стають марними.

Багато видів ransomware, що відносяться до цієї категорії, використовують повноекранне вікно на машині жертви і обмежують доступ користувача до цієї сторінки різними способами. Для цього створюється віртуальний робочий стіл, змінюються записи в реєстрі або завершуються деякі процеси. Хоча крадіжка інформації не входить в число зумовлених прагнень ransomware, деякі штами мають таку можливість. Ця крадіжка може здійснюватися або з метою шпигунства, або з метою латерального переміщення. Наприклад, Petya краде облікові дані зі скомпрометованої машини і використовує їх для поширення на інші пристрої. Крім того, SamSam, найбільш помітний зразок цільового ransomware, також володіє цією функцією.

Останні варіанти Cerber мають цю функцію у вигляді крадіжки гаманця Bitcoin. Крім того, у багатьох різновидах є і приголомшливі функції. Наприклад, HDDCryptor використовує утиліту для вилучення облікових даних з останньої сесії, щоб отримати доступ до раніше доступних мережевих дисків, які в даний момент не змонтовані. В кінцевому підсумку, після виконання яких-небудь шкідливих дій, багато сімейств ransomware підробляють головний завантажувальний запис (MBR) та замінюють його своїм власним завантажувачем для відображення записки з вимогою викупу.

1.3.5 Етап вимагання

На відміну від багатьох інших типів шкідливих програм, ransomware часто повідомляє жертвам, що вони постраждали від конкретної атаки, і щоб позбутися від неї, вони повинні слідувати інструкціям. На цьому етапі зазвичай відображається записка з вимогою викупу на мові, заснованій на геолокації IP-адреси комп'ютера жертви (у вигляді фонового зображення, HTML-файлу, текстового файлу і так далі). Записка з викупом містить необхідні інструкції про те, як зробити оплату і як повернути дані або пристрій в початковий стан. У багатьох родинах ransomware текстовий вміст викупної записки жорстко закодований в самому бінарному файлі шкідливої програми.

Інші варіанти можуть завантажувати його з C&C-сервера при першому зв'язку. Пізніше в вимогу про викуп додається тільки інформація про конкретного користувача і необхідні посилання Tor. Як і у всіх атаках, заснованих на залякуванні, на цьому етапі найчастіше використовуються методи соціальної інженерії, щоб переконати жертву заплатити викуп. Для цього багато сімейств crypto-ransomware і wiper-ransomware вказують крайній термін, протягом якого, якщо оплата не буде зроблена до цього часу, закритий ключ (необхідний ключ для розшифровки) буде назавжди знищений або запитувана сума буде подвоєна.

Крім того, більшість crypto-ransomware пропонує безкоштовну послугу розшифрування для невеликої кількості заражених файлів, щоб переконати жертву заплатити викуп. У багатьох родинах ransomware після відображення сторінки викупу порожнистий процес завершується сам по собі. Троян AIDS, перший задокументований ransomware, вимагав від жертв оплати міжнародним грошовим переказом або касовим чеком, відправленим на абонентську скриньку в Панамі [10,46].

В даний час існує багато анонімних або псевдо-анонімних способів оплати. І це одна з причин зростання цієї прибуткової атаки серед кіберзлочинців. Способи оплати варіюються від банківських переказів і систем онлайн-платежів на основі ваучерів до використання різних популярних криптовалют.

Наприклад, ранні версії CryptoLocker надавали різні варіанти оплати жертвам, включаючи cashU, Ukash, paysafecard, Green Dot MoneyPak (тільки для США) і Bitcoin. Хоча в більш нових версіях пропонуються тільки MoneyPak і Bitcoin. З огляду на популярність біткоїнів як криптовалюти, його псевдоанонімність і майже децентралізованість, а також можливість мати кілька біткоїн-адрес незалежно від реальної особистості користувача, використання біткоїнів набуло широкого поширення в злочинній діяльності, особливо в цифрових здирницьких атаках, таких як ransomware. Крім доступності біткоїнів у всіх географічних регіонах, ще однією перевагою є незворотність транзакцій.

Фінансовий мотив більше не є єдиним стимулом противника. Багато атак з метою викупу виникають в політичних цілях, для шпигунства, саботажу або маскування інших типів шкідливого ПЗ. Наприклад, дослідницька група Unit 42 з Palo Alto Networks [57] виявила новий штам ransomware під назвою RanRan з політичним мотивом замість грошового платежу. Він націлений на близькосхідні організації і вимагає у них гроші, змушуючи жертв розміщувати підбурювальні політичні оголошення проти близькосхідного політичного лідера (лідера країни жертви).

Rensenware – ще один приклад crypto-ransomware з негрошовим стимулом, який більше схожий на жарт. Щоб розшифрувати файли, він просить жертву набрати необхідну кількість очок в грі TH12 ~ Undefined Fantastic Object, зазначеної в примітці про викуп. Щоб проілюструвати мотиви, які стоять за шахрайством з ransomware, краще розділити запитуваний викуп на дві основні групи: грошовий і негрошовий.

1.3.6 Етап емансипації

Умовою виживання в світі бізнесу є виконання зобов'язань. Нелегальна кіберторгівля також не є винятком. Хакери, що стоять за програмою-викупом, повинні звільнити захоплені ресурси заручників після отримання викупу від жертви, щоб вони могли продовжувати заробляти гроші на наступних атаках. Деякі

різновиди ransomware приділяють велику увагу цьому принципу, оскільки вони навіть надають жертвам послуги онлайн-чату або інші можливості, щоб забезпечити цілісність процесу звільнення ресурсів, а якщо виникнуть які-небудь проблеми, вони можуть допомогти. В атаках crypto-ransomware після сплати викупу, зараженому користувачеві відправляється посилання на інструмент розшифровування, призначений для конкретної жертви.

TorrentLocker, CTB-Locker і TeslaCrypt – це приклади сімейства здирницьких програм, які діють подібним чином і надають інструменти для розшифрування інструменти після завершення оплати [55]. Однак існують деякі категорії, які не можуть відновити ресурси жертви після отримання викупу, навмисно або через помилку в викупних програмах. У під розділі 1.2 цей тип здирницьких ПЗ поміщений в категорію wiper-ransomware. Як приклад можна привести WannaCry, який через технічні деталі в коді, не міг визначити, яка жертва заплатила викуп. Тому, відповідно до звітів, ті, хто заплатив викуп, ніколи не отримували ключ дешифрування для відновлення файлів.

Те ж саме відноситься і до NotPetya. Навіть якщо жертва погоджується заплатити, NotPetya зітре ключ потокового шифру Salsa20, необхідний для розшифрування. Немає ніякої гарантії належного звільнення ресурсів з різних причин, включаючи порушення зв'язку, помилки в коді ransomware або непередбачувані наміри зловмисників.

Висновки за розділом 1

За останні кілька років такі атаки, як ransomware, Doxware і шкідливі криптомайнери, набули широкого розголосу. Кіберзлочинці невпинно шукають інноваційні методи цифрового вимагання, засновані на залякуванні людей. Ransomware вважається одним із найуспішніших способів заробітку на вимаганні на підпільному ринку.

Ransomware – це шкідливе ПЗ, яке вимагає гроші, беручи в заручники ресурси користувачів. Це вимагання можливе через страх жертви втратити цифрові активи

або позбутися доступу до них. Концепція ransomware або шкідливих програм, заснованих на вимаганні, була вперше офіційно представлена доктором Джозефом Поппом в 1989 році з випуском "AIDS Information Trojan". Механізми доставки у вигляді черв'яків забезпечили швидке поширення кампаній ransomware. Завдяки бізнес-моделі RaaS індустрія ransomware стала більш процвітаючою, і зловмисники можуть легко створювати спеціалізовані ransomware без особливих навичок і часу. З огляду на поступове зростання індустрії ransomware і швидке повернення інвестицій, можна очікувати, що розробники ransomware будуть продовжувати доповнювати свої варіанти новими функціями і можливостями, щоб розширити об'єктивну сферу і підняти свій бізнес. Тому розробка механізму захисту від такого типу атак дуже важлива.

Однак практично неможливо розробити ефективні системи захисту, не маючи загального уявлення про ці загрози. У багатьох критично важливих організаціях, що розглядають оплату як єдиний варіант, знання типу атаки може привести до прийняття різних рішень. Іншим аспектом дослідження є пропозиція шести-етапного спеціалізованого ланцюжка атак для загроз даного типу. Поділ процесу атаки на різні частини і розуміння технологій, які використовуються на кожному етапі, на додаток до формулювання проблеми, може допомогти визначити моделі поведінки, що демонструються ransomware, і запропонувати ефективні стратегії захисту.

РОЗДІЛ 2
ЗАДІЯНІ ТЕХНОЛОГІЇ В ФОРМУВАННІ ЗАГРОЗ RANSOMWARE. ТРАДИЦІЙНІ МЕХАНІЗМИ ЗАХИСТУ НА ОСНОВІ ATTACK CHAIN

2.1 Роль задіяних технологій в формуванні загроз типу ransomware

Мотивовані недавнім розвитком технологій, атаки ransomware значно виросли за обсягом, різноманітністю та складністю. Розуміння того, як діють ті чи інші види ransomware та які технології містяться в потоці атак, дозволяє нам краще підібрати належний захист. Очевидно, що розуміння характеристик векторів зараження, доставки шкідливого навантаження і особливостей мережевого трафіку з C&C-серверами для отримання інструкцій допоможе командам безпеки знати, чого очікувати, та вжити належних контрзаходів для запобігання або мінімізації збитку, що наноситься ransomware в даний момент. Далі наведений опис технологій, які використовують зловмисники для реалізації атак.

2.1.1 Роль криптографії

Ransomware використовує цілий ряд технік для блокування доступу користувачів до свого ресурсу. Найбільш поширеною і цікавою технікою є криптографія. Традиційно криптографія є технологією, яка забезпечує інформаційну безпеку "на льоту". Вона носить оборонний характер і забезпечує конфіденційність, аутентифікацію і безпеку користувачів. Однак ця технологія може бути використана проти безпеки.

Ідея криптовірусології була вперше висунута Адамом Янгом і Моті Юнгом, яка являє собою наступальне використання криптографії. Криптовірологія – це область наукових досліджень, яка фокусується на поєднанні криптографії та шкідливого програмного забезпечення. CryptoRansomware використовує цю технологію, щоб взяти дані в заручники. Поки жертва не заплатить викуп, ключ для

розшифрування не буде їй надано. Для цього використовуються різні симетричні і асиметричні алгоритми шифрування, описані в підрозділі 1.2.2.

Для досягнення прийнятної швидкості, високої продуктивності і стійкості більшість програм-викупів використовують гібридні методи. Багато програм, які стосуються цієї категорії, зазвичай використовують швидкий симетричний алгоритм, наприклад AES, для шифрування файлів, а потім застосовують алгоритм з відкритим ключем, наприклад RSA і ECC, для шифрування секретного ключа. ECC використовує більш короткий ключ шифрування, ніж RSA. В результаті він працює швидше і вимагає менше обчислювальної потужності, ніж RSA при тій же довжині ключа. Доказом цієї концепції є еквівалентна стійкість 160-бітного ECC і RSA з розміром ключа 1024 біта.

Але реалізація RSA простіша, ніж ECC, а ймовірність помилки нижча через відсутність складності. AES, симетричний блоковий шифр, який використовує загальний секретний ключ для шифрування і дешифрування, є одним з найбільш часто використовуваних алгоритмів в атаках здирницьких ПЗ. Цей алгоритм був використаний в різних режимах та в різних штамах ransomware.

Наприклад, ранні версії TorrentLocker використовували алгоритм AES в режимі CTR (Counter) для шифрування ресурсів даних. Однак, через помилку, приводила до легкого розшифрування, більш пізні версії замінили режим роботи з CTR на CBC (Cipher Block Chaining) [55, 58, 59]. TeslaCrypt використовує AES і застосовує CBC як режим роботи. Petya і NotPetya, які включені в категорію wiper-ransomware, відповідно до запропонованої класифікації, використовують потоковий шифр Salsa20 для шифрування дисків.

Загальнодоступність криптографічних бібліотек і простота їх використання – один з ключових чинників швидкого зростання шкідливих атак ransomware в останні роки. Крім ролі шифрування в групах crypto і wiper-ransomware, ця технологія також використовується для захисту зв'язку між ransomware і її C&C-сервером [58]. Оскільки багато сімейств ransomware отримують ключ шифрування при спілкуванні з сервером C&C, для успішної роботи дуже важливо захистити

комунікацію C&C. Методи шифрування ускладнюють виявлення шкідливого зв'язку C&C на мережевому рівні.

Групи зловмисників, що стоять за атаками ransomware, використовують різні методи для захисту каналу C&C. Наприклад, CryptoWall версії 3.0 здійснює зв'язок зі своїм командним центром через мережу I2P, в той час як попередні версії використовували Tor для обфускації C&C-комунікацій [59]. Цибулева маршрутизація – один з анонімних способів зв'язку, який зазвичай пропонується в більшості атак ransomware, – також використовує криптографію. Вона використовує множинні і вкладені процеси шифрування для досягнення конфіденційності.

2.1.2 Роль соціальної інженерії

Соціальна інженерія завжди була популярним інструментом в руках шахраїв. На початку 2000-х років вона стала більш агресивною в кібератаках [19]. Згідно з запропонованого шестиептапного ланцюжка атаки ransomware, методи соціальної інженерії грають важливу роль на етапах зараження і вимагання. Як правило, соціальна інженерія використовується в атаці ransomware шляхом стимулювання емоцій користувача, таких як цікавість, страх, терміновість для виконання певних дій. З огляду на прогрес і складність заходів безпеки, можна сказати, що методи соціальної інженерії є найпростішим способом поширення шкідливого ПЗ.

Як уже згадувалося, одним із основних векторів зараження, що вимагає взаємодії з користувачем, є спам електронною поштою. Більшість атак ransomware розпочинається шляхом заманювання жертв відвідати шкідливу веб-сторінку або відкрити заражене вкладення в фішинговому листі за допомогою методів соціальної інженерії. З цією метою багато спам-кампаній маскуються під звичайну кореспонденцію, таку як рахунки і повідомлення про доставку [31]. Locky, одна з найбільш сумно відомих ransomware в 2016 році, використовувала цей метод для поширення і збудження користувачів на отримання шкідливого вкладення.

Основним психологічним фактором шантажу в атаках scareware є страх. Різні сімейства ransomware також використовують стратегії соціальної інженерії, щоб

скористатися емоційною нестабільністю людей на етапі вимагання. Багато записок про викуп містять таймер зворотного відліку, що означає – злочинні групи будуть збільшувати суму викупу в геометричній прогресії або, в деяких випадках, назавжди видалять ряд файлів після закінчення терміну дії.

Крім того, зазначений термін призведе до того, що у жертв не буде бажання шукати кращі рішення, а також вони будуть помилятися в прийнятті рішень. Такі методи шантажу будуть більш ефективні в компаніях і організаціях, таких як лікарні, де "час" грає вирішальну роль, так що більшість жертв вимушена заплатити викуп. WannaCry, SamSam, Defray і BitPaymer є прикладами таких випадків.

2.1.3 Роль ботнетів

Спам-ботнети є однією з основ великомасштабних кіберзлочинних атак. З огляду на те, що фішингові спам-листи є одним із основних векторів зараження, питання про спамерські ботнети необхідно розглядати як один із ключових чинників, що беруть участь в поширенні ransomware. Якщо коротко, ботнети – це мережа із сотень і мільйонів зламаних машин, так званих зомбі, під керуванням «ботмайстера». Спам-кампанії на основі ботнетів шляхом програмування великої кількості розподілених ботів здатні передавати десятки тисяч спам-листів багатьом користувачам за короткий проміжок часу [60].

Ботнети завжди відігравали важливу роль у багатьох кібератаках, включаючи DDoS, банківські трояни, розсилку спаму грошовим мулів, ransomware і майнерів криптовалюти. Архітектура ботнетів варіюється від простих клієнт-серверних моделей до тимчасових. CryptoLocker, одна з найстрашніших і сумнозвісних програм-вимагачів в 2013 році, використовувала ботнет Gameover ZeuS для поширення серед своїх жертв. ZeuS використовував одноранговий ботнет Cutwail для передачі великої кількості фішингових листів. В основному він використовувався для фінансових злочинів. Necurs, один з найбільших відомих ботнетів в історії з великою кількістю заражених ботів, був створений в рамках кампаній з розповсюдження ПЗ для розсилки спам-повідомлень декільком

мільйонам користувачів. Він брав участь у багатьох кіберзлочинах – від організації DDoS-атак до поширення шкідливого ПЗ.

Сліди Necurs були виявлені в поширенні програм-вимагачів, включаючи Locky, Jaff, GlobeImposter і Scarab [31]. Ботнет Necurs отримав великий дохід від доставки таких шкідливих програм, як рандомне ПЗ Locky і банківський троян Dridex. Однак після значної перерви дана технологія спрямувалась на більш витончені шахрайства, такі як афери з акціями pump-and-dump. Kelihos був ще одним ботнетом, який пропонував своїм клієнтам "спам як послугу". Він використовувався для поширення деяких сімейств програм-вимагачів, включаючи Troldesh (також відому як Shade), Wildfire, CryptFIle2 і MarsJoke. Використання ботнетів в атаках може бути набагато небезпечніше, ніж те, що спостерігалося до сих пір.

Virobot є однією із останніх відомих програм з метою викупу з використанням технології ботнету. Virobot, ідентифікований Trend Micro як RANSOM_VIBOROT.THIAHAH [53], являє собою новий штам, що володіє одночасно можливостями здирницьких ПЗ та ботнетів. Це означає, що як тільки Virobot вражає машину-жертву, і вона стає частиною спамерської бот-мережі для розсилки самої програми з метою викупу більшій кількості інших жертв.

2.1.4 Роль анонімних мереж

Одним із видів використання анонімних мереж є їх застосування в атаках цифрового вимагання. Існує безліч причин для використання технології анонімних мереж в кіберзлочинності. Найбільш помітною з них є відсутність можливості відстеження правоохоронними органами та владою. Використання анонімності в комунікаціях нейтралізує вбудовані стратегії чорних списків в багатьох інструментах безпеки. Ця технологія чітко простежується на трьох етапах (тобто зв'язку, вимагання та емансипації) пропонованого ланцюжка атаки. Багато сімейств програм-вимагачів використовують різні анонімні мережі, такі як Tor та I2P, для зв'язку з сервером C&C в обхід перевірок мережевого трафіку.

Tor – це оверлейна мережа, що забезпечує анонімний зв'язок між організаціями за протоколом TCP. У ній використовується набір машин-добровольців для направлення інтернет-трафіку. Анонімність сторін спілкування зазвичай досягається за рахунок цибулевої маршрутизації. У цибулевій мережі повідомлення інкапсулюються в слої шифрування. Однак ця техніка може бути переможена такими методами, як аналіз часу.

I2P – ще один приклад, що забезпечує анонімний одноранговий зв'язок за допомогою наскрізного шифрування. Для цього використовується часникова маршрутизація (технологія анонімного, зашифрованого обміну інформацією через комп'ютерну мережу, яка використовується в анонімній мережі I2P). CryptoWall версії 3.0 – типова програма-вимагач, що використовує I2P для встановлення зв'язку зі своїм командним центром [59]. Підпільні ринки в основному використовують анонімні мережі в поєднанні з криптовалютою, такими як біткоїн, для торгівлі та контрабанди товарів. В основному злочинці, які стоять за викупними програмами, надають жертвам приховані URL-адреси сервісів в записці про викуп, для доступу до яких (для виплати викупу і звільнення ресурсів заручників) необхідно встановити додатки типу Tor Browser або скористатися сервісами типу Tor2web. Такий спосіб зв'язку запобігає підслуховування мережевого трафіку.

Наприклад, на етапах вимагання та звільнення після завершення шифрування файлів CTB-Locker буде здійснювати всі комунікації через Tor. Зазвичай це робиться через численні проксі-сайти, які діють як ретранслятори до прихованої служби Tor [55]. TeslaCrypt видає жертві записку з вимогою викупу, в якій містяться інструкції щодо доступу до прихованої служби Tor і способу оплати викупу в Bitcoin. Аналогічним чином, програма cerber ransomware надає користувачеві список шлюзів Tor2web для оплати.

2.1.5 Роль DGA

C&C-сервери є важливою частиною багатьох родин ransomware, які грають координуючу роль елементів атаки. Переважна більшість видів ransomware повинні

взаємодіяти зі своїм C&C-сервером, щоб зробити руйнівні дії або після отримання викупу очистити машину жертви і звільнити ресурси. Адреса C&C-сервера може бути жорстко закодованою у вигляді IP-адрес або доменних імен в самому бінарному файлі шкідливого ПЗ, що легко виявляється і блокується за допомогою статичного аналізу.

У багатьох випадках стійкість атаки залежить від доступності командного центру та отримання від нього інструкцій. Кампанії Ransomware використовують різні техніки для обходження систем безпеки, щоб запобігти руйнуванню своїх C&C-серверів. Саме тут в гру вступають DGA як секретний механізм зв'язку з C&C-серверами. Застосування цієї технології укладнює відключення C&C-серверів, хоча б до тих пір, поки алгоритм не буде повністю перепрограмовано. Алгоритми генерації доменів періодично виробляють велику кількість псевдовипадкових доменів на основі початкового значення протягом короткого періоду часу. Ці домени часто являють собою рядки Тарабарського, які додаються до домену верхнього рівня (TLD). В [61] згенеровані псевдовипадкові домени розділені на шість окремих груп відповідно до їх структурної схеми.

Бот-пастухи, які керують C& C-серверами, реєструють одне або кілька згенерованих доменних імен. Ransomware посилає DNS-запити до згенерованих доменів, щоб дозволити і підключитися до того, який зареєстрований. Таким чином, в результаті цих запитів може бути отримано кілька відповідей NXDomain [61]. Кількість доменних імен варіюється в залежності від структури і дизайну DGA. Наприклад, Gameover ZeuS генерує 1000 унікальних доменів в день [56]. Цей метод допомагає зміцнити атаки проти стратегій чорних списків і технік, заснованих на сигнатурах.

Хоча в цій технології все ще є слабкі місця, використання динамічного насіння в ransomware, які зв'язуються з C&C через механізм DGA, допомагає зміцнити їх командні сервери проти підходів sinkholing.

2.1.6 Роль криптовалюти

Ransomware є однією з галузей, що швидко розвиваються, тому що вона пропонує спосіб заробити гроші, не вимагаючи особливих навичок або зусиль. Однак в даний час кіберзлочинці керуються не тільки фінансовими, а й політичними мотивами. Таким чином, викуп необхідний противником, може бути як грошовим, так і негрошовим, в залежності від мети атаки.

Групам зловмисників необхідно забезпечити безпеку фінансових операцій, щоб гарантувати успіх атаки. Тому вони схильні використовувати глобальні і децентралізовані грошові системи, а не фіатну валюту. Цифрова валюта і технологія блокчейн створили можливості для монетизації кіберзлочинів за рахунок усунення посередників і забезпечення анонімності. Сьогодні криптовалюта стала гарячою темою на форумах з комп'ютерної безпеки, оскільки її слід був помічений в багатьох атаках таких як ransomware, криптомайнер і фішингові атаки.

Криптовалюта сприяють успіху атак завдяки завдяки тому, що їх практично неможливо відстежити. З появою в 2009 році біткоїнів як першої децентралізованої криптовалюти, в світі тіньової економіки відбулася революція, і увагу кіберзлочинців було залучено до цього нового способу переказу грошей. Біткоїн – це однорангова криптовалюта, яка використовує загальнодоступну книгу транзакцій, відому під назвою як блокчейн [13].

У більшості атак, таких як WannaCry, оплата проводиться за допомогою Bitcoin. Одна з труднощів використання цифрової валюти в кібератаки є коливання ринку, що призводить до того, що злочинні групи не знають, скільки саме вони вимагають від своїх жертв. Тому деякі сімейства програм-вимагачів, такі як Scarab, додають можливість переговорів з приводу суми викупу на етапі вимагання.

На додаток до біткоїнів, який є одним з найбільш широко використовуваних методів оплати, інші криптовалюти, такі як Monero, стають все більш популярними серед злочинців. Цей вид криптовалюти має додаткові функції безпеки і конфіденційності, які запобігають відстеження транзакцій. Наприклад, Kirk ransomware використовує Monero як засіб оплати викупу.

2.1.7 Роль RaaS

За останні кілька років загрози вимагання різко зросли. Однією з причин такого прогресу є концепція ransomware-as-a-service, звана RaaS. Поява RaaS-платформ дало можливість будь-якому користувачеві з поганими намірами для створення своїх власних варіантів ransomware, навіть без попередніх знань. Таким чином, основні автори ransomware зосереджуються на розробці та просуванні шкідливого коду і делегують його поширення філіям [46].

Завдяки легкому доступу до RaaS, кіберзлочинці можуть легко перейти на сайт, що надає RaaS, і, не докладаючи особливих зусиль, створити свій власний варіант ransomware. Групи провайдерів RaaS отримують частину доходу від викупу за кожне успішне зараження. RaaS надає хороші можливості монетизації для власників ботнетів або тих, хто має доступ до великої кількості комп'ютерів будь-яким способом. Tox і Shark є прикладами платформ RaaS. Оператори таких платформ в основному використовують анонімні мережі, такі як Tor для пропозиції своїх послуг. Крім того, багато відомих сімейств здирницьких ПЗ, такі як Cerber, використовують цю бізнес-модель для широкого розповсюдження серед користувачів та отримання більшого прибутку. Таким чином, RaaS можна розглядати як одним з факторів успіху атак ransomware [15].

2.2 Традиційні механізми захисту на основі attack chain

Загрози кібербезпеки постійно розвиваються, а зловмисники шукають нові способи обходу захисних систем. За останні кілька років кіберсвіт став свідком різноманітних атак з використанням програм-викупів зі страшними тенденціями. Цей вид шкідливого ПЗ швидко став однією з найнебезпечніших загроз кібербезпеки, з якими стикаються приватні особи і підприємства у всьому світі. Різні сімейства ransomware використовують різноманітні методи, щоб не потрапити в поле зору систем моніторингу безпеки. Оскільки результат атаки ransomware практично незворотній, перевагу слід віддавати методам запобігання та / або

виявлення на ранніх стадіях. Захист від атак ransomware в деякій мірі схожа на процедури відображення інших кібератак.

Ці підходи, засновані на сигнатурах або аномаліях, або розгортаються як моніторинг трафіку в мережі або в якості рішення для захисту кінцевих точок на хості. Оскільки на практиці існують обмеження в стратегії на основі сигнатур, особливо в зв'язку з помітним зростанням числа варіантів ransomware і використанням антикриптографичних методів, таких як пакування і обфускація, поведінкові методи виявлення привернули увагу в сфері кібербезпеки.

В результаті рішення, засновані на поведінці, стали більш ефективними завдяки їх здатності пропонувати докладні характеристики і розпізнавати атаки "нульового дня". Однак ці методи також страждають від обмежень, включаючи високий відсоток помилкових спрацьовувань, помітне споживання ресурсів і складність реалізації. Як правило, оборонні підходи включають в себе аналіз, виявлення, запобігання і відновлення. Далі описуються сучасні дослідження в області захисту від ransomware з точки зору attack chain.

2.2.1 Захист на стадії зараження

Найефективніша стратегія обходження будь-якої атаки полягає в тому, щоб запобігти її. Розуміння того, як різні штами ransomware заражають пристрої, має вирішальне значення для протидії таким загрозам. Дослідження спаму і його шкідливого вмісту може допомогти в аналізі різновидів ransomware, а також розпізнати їх до зараження системи.

Шкідливі вкладення, які призводять до зараження і випуску ransomware, в основному мають формат файлів MS Office, pdf або zip. Такі рішення, як відключення макросів в документах Microsoft Office, для користувачів, що бажають скористатися всіма функціональними можливостями, будуть небажані. Крім того, ці рішення не поширюються на інші типи файлів, що містять корисне навантаження. Оскільки зловмисники використовують методи соціальної інженерії для досягнення

успіху на етапі зараження, навчання користувачів є чіткою стратегією, яка рекомендується в більшості літературних джерел.

Однак в деяких дослідженнях технічно розглядається питання виявлення спаму і шкідливого вмісту в електронних листах. Багато досліджень в області виявлення спам-листів і фішингових сайтів також можуть бути поширені на ПЗ. В [62] основна увага приділяється мобільним фішинговим атакам і механізмам захисту від них, а також пропонується комплексна таксономія пропонованих стратегій. В [63] для виявлення шкідливої електронної пошти представлений новий набір загальних описових характеристик.

Автори використовували методи машинного навчання для запропонованих ними ознак, які були вилучені з компонентів електронної пошти, і оцінили Random Forest як кращий класифікатор у своїх результатах. Радд та ін. [64] використовували методи машинного навчання, щоб відрізнити шкідливі вкладення електронної пошти від доброякісних. Вони використовували два класифікатора (тобто глибокі нейронні мережі та ансамблі дерев рішень з градієнтним посиленням) на наданому наборі даних. Представлений ними метод розглядає два типи вкладень: архіви zip і документи Microsoft Office. Ще одним рішенням, яке може бути використаний під час фази зараження, є пастка для спаму, що відноситься до категорії honeypot.

Вектори зараження в родинах Android ransomware в основному включають шкідливі програми, пропоновані як легітимні програми в магазинах додатків, і шкідливі цільові сторінки, пов'язані з SMS або іншими носіями інформації для користувачів. Хоча мобільні ransomware завдають меншої шкоди, ніж аналоги, їх слід розглядати як серйозну загрозу через широкого поширення мобільних пристроїв. Деякі дослідники [59] представили RanDroid, автоматизований полегшений підхід для ідентифікації

Android ransomware. RanDroid призначений для перевірки APK-файлів перед їх установкою на пристрої користувачів. Він використовує статичний і динамічний аналіз для добування інформації, такої як поява екранів блокування і загрозливих рядків, з APK. У випадку з різновидами ransomware, які використовують методи поширення по типу хробака, обмеження доступу до загальних мережних ресурсів

може стати порятунком для системи. Крім того, як згадувалося раніше, ще одним методом поширення здирницьких ПЗ є набори експлойтів.

Набори експлойтів – це набори інструментів, які автоматизують використання вразливостей. Використання експлойтів дає можливість зловмисникам уникнути необхідності взаємодії з користувачем і соціальної інженерії. У таких випадках оновлення операційної системи, додатків та відмова від встановлення непотрібних програм або застарілих плагінів може бути дуже корисним.

2.2.2 Захист на етапі інсталяції

Незалежно від вектора зараження, корисне навантаження доставляється в систему жертви або у вигляді виконуваного файлу, або у вигляді скрипта, макросів, вбудованих в файл, двійкових файлів, і намагається встановитися для продовження процесу атаки. Кращими стратегіями захисту на цьому етапі є моніторинг файлів і процесів на кінцевій точці. Однак ці підходи застосовуються з невеликими змінами на етапі виконання. Статичний і динамічний аналіз – це два основні методи для вивчення файлів і створення набору даних сигнатур, що відносяться до доброякісного та шкідливого коду.

Статичний аналіз – це швидкий спосіб дослідження файлів і виявлення потенційно шкідливого код. Оскільки статичні методи не виконують код, вони не можуть ідентифікувати сімейства програм-вимагачів, які використовують складні методи. Крім того, як і інші шкідливі програми, більшість видів програмного забезпечення використовують методи обфускації та пакування, щоб перешкодити статичному аналізу і обійти системи безпеки. Таким чином, на допомогу приходить метод динамічного аналізу (також відомий як аналіз поведінки).

Динамічні методи, виконуючи код в контрольованому середовищі, дозволяють спостерігати за його поведінкою та можливостями. Для цієї мети використовуються такі методи, як "sandbox" або пісочниця, використовуються для створення сигнатур нових і невідомих ransomware. Ці аналітичні інструменти допоможуть відслідковувати і ретельно вивчати процеси, модифікації реєстру і мережеву

активність, які є основними складовими етапу інсталяції. Деякі спеціалісти в сфері кібербезпеки розглянули проблему ін'єкції коду і запропонували способи її вирішення. Запропонований ними механізм враховує як коротку, так і довгу історію кожного процесу і всієї системи.

Виявлення функції шифрування всередині двійкового коду – ще одне рішення, яке може бути використано під час фази встановлення і задіяно в якості додаткового методу до засобів захисту. Лестрінгант та інші [65] запропонували підхід для автоматичного розпізнавання криптографічних примітивів всередині двійкового коду. Їх метод заснований на ізоморфізмі графів потоків даних (DFG). Оскільки DFG є природним способом відображення залежностей між операціями, краще їх застосовувати при ідентифікації криптографічного алгоритму.

У запропонованому підході, насамперед, будується DFG, відповідно до вхідного двійкового коду. Потім цей DFG нормалізується за допомогою правил перезапису. Нарешті, в DFG шукаються підграфи, ізоморфні сигнатури даного криптографічного алгоритму. З огляду на те, що останні два етапи вимагають великих обчислювальних витрат, для досягнення прийнятної продуктивності, двійковий код повинен бути фрагментований і використаний в якості вхідних даних.

Сюй та інші [66] представили програму CryptoHunt, яка здатна розпізнавати широко поширені використовувані криптографічні функції, включаючи TEA, AES, RC4, MD5 і RSA всередині двійкового коду, навіть при різних умовах обфускації. Вони запропонували техніку, звану бітово-точним символьним відображенням циклів для цієї мети. HelDroid, розроблений Андроніо [67], націлений на виявлення мобільних програм-вимагачів на пристроях Android. Він заснований на статичному аналізі і розглядає поведінку ransomware на рівні додатку. Автори застосували текстовий класифікатор, заснований на ознаках NLP, для виявлення загрозливих фраз. Д

Діагностична здатність запропонованого методу залежить від набору навчальних даних. Меркальдо [3] розробив підхід до виявлення, заснований на формальних методах, для розпізнавання інструкцій коду ransomware на платформі Android. Їх методика ідентифікує сімейства здирницьких програм за байткодами

додатків, а не за вихідним кодом. З цієї причини вона не залежить від мови програмування вихідного коду і обфускації. Автори повторно використовували існуючі складні засоби перевірки моделей, щоб уникнути зниження продуктивності.

EldeRan [9] був представлений як підхід машинного навчання для динамічного аналізу і класифікації атак ransomware. Для цього він відстежує ранні дії додатків на етапі їх установки. В рамках цього підходу найбільш значущі динамічні характеристики ransomware визначаються за допомогою критерію взаємної інформації (MI). EldeRan використовує класифікатор регулярної логістичної регресії завдяки його швидкості, простоті навчання і можливості поновлення для того, щоб відрізняти програми-вимагачі від хорошого ПЗ.

Дослідники з [5] запропонували метод, заснований на структурній ентропії і алгоритмах нечіткої логіки, щоб відрізнити здирницькі ПЗ для Android від легітимного мобільного додатка. Вони проводили аналіз безпосередньо на виконуваних файлах.

Підхід, представлений в [65], був останньою роботою в області виявлення ransomware на етапі установки на момент написання диплому, яка була надана для подолання слабкості динамічних стратегій. Чжан та інші дослідники [6] виконують класифікацію ransomware на основі статичного аналізу. Для цього вони перетворюють послідовності опкодів зразків ransomware в послідовності N-грам, а потім обчислюють TF-IDF для кожної з них, щоб вибрати N-грами з ознаками. Автори використовували п'ять алгоритмів машинного навчання для побудови моделей класифікації і застосували свої моделі на 1 787 зразках ransomware з восьми родин. Вони заявили, що запропонована ними методологія досягає високої точності як в бінарній, так і в мультикласифікації.

В [7] використовувалася техніка послідовного пошуку шаблонів для визначення та вилучення найкращих характеристик крипто-рандомних програм з метою їх класифікації та відмінності від доброякісних додатків. Набір даних, використаний ними, включав журнали динамічних бібліотек посилань (DLL), реєстру і дій файлової системи. Ці журнали були зібрані протягом перших 10 секунд після запуску програм-вимагачів і доброякісних програм. Нарешті, вони

використовували алгоритми класифікації, включаючи J48, Random Forest, Bagging і MLP, щоб оцінити корисність обраних ними ознак.

Також Хомаюн [7] представив систему під назвою DRTHIS, що розгортається на рівні туману, для виявлення ransomware та ідентифікації їх відповідних сімейств. Для класифікації вони використовували і порівнювали два методи глибокого навчання, а саме довгу короткострокову пам'ять (LSTM) і згорткову нейронну мережу (CNN). Вони знову використовували послідовність операцій, що виконуються екземплярами як ransomware, так і доброякісних додатків в перші 10 секунд після впровадження.

Інша дослідницька робота була запропонована Роде [68], яка здатна передбачити шкідливість файлу протягом перших 5 секунд після його виконання. Вони використовували модель рекурентної нейронної мережі (RNN) для передбачення шкідливої поведінки. Аргумент автора на користь використання характеристик машинної активності в якості вхідних даних моделі замість використання викликів API полягає в тому, що виклики API уразливі до злому і призводять до помилок в класифікації зразків нейронними мережами. Вони також стверджують, що моделі RNN перевершують інші класифікатори машинного навчання і більш стійкі до переоцінки.

Хоча останні три підходи можуть бути розгорнуті на етапі виконання, доречно їх згадати і в цьому підрозділі. Тому що перший підхід зосереджений тільки на добуванні ознак і проблеми класифікації, а другий враховує скорочення часу динамічного виявлення і використання нейронних мереж, і обидва вони можуть бути запущені в середовищі пісочниці. Перша частина роботи, представлена в [23], тобто абстрактний опис поведінки великого класу сучасних атак ransomware, також може бути реалізована на цьому етапі.

2.2.3 Захист на етапі зв'язку

Багатьом кібератакам необхідно підтримувати зв'язок з командним центром, щоб завершити процес атаки, поширити і заразити більше пристроїв або вивести

інформацію жертви. Ransomware не є винятком. У багатьох родинах використовується асиметрична криптографія, оскільки пара ключів генерується, якщо зв'язок порушений заходами безпеки або взагалі не встановлений, атака не дійде до руйнівної фази виконання. Відповідно, застосування захисного підходу на цьому етапі може бути ефективним в запобіганні подальшого збитку. Виявлення шкідливих C&C-комунікацій – тема не нова і розглядається вже давно. Деякі кампанії ransomware використовують закодовані IP-адреси або доменні імена в самому бінарному файлі для комунікацій, які легко виявити за допомогою статичних аналітичних інструментів.

Цей список доменів і IP-адрес, відомих як шкідливі, може бути використаний в системах моніторингу на основі мережевих сигнатур. Тому щоб обійти засоби мережевої безпеки, багато видів ransomware використовують DGA для створення каналів зв'язку з C & C-сервером. Ця тактика нейтралізує підходи, засновані на чорних списках та сигнатурах в мережі. В результаті виявлення і розпізнавання трафіку DGA та використання таких методів, як машинне навчання, пошук інформації і аналіз даних допоможуть розробити більш ефективні рішення для боротьби з ransomware атак на етапі передачі даних. Відмінність шкідливого C&C-трафіку від легального трафіку давно вивчається, особливо в контексті розпізнавання ботнетів.

Рішення, представлене в [70], вирішує проблему виявлення випадково згенерованих доменів за допомогою DGA без необхідності зворотного розробки шкідливого ПЗ. Суть методу полягає в тому, що запити, зроблені шкідливим ПЗ або ботом, приведуть до відповідей у вигляді неіснуючих доменів (NXDomain). Ахмадіан та інші [51] запропонували підхід до розпізнавання DNS-запитів, які видаються DGA в родинах здирницьких програм, та застосовують цей метод для виявлення, підключення до діючого C&C-сервера. Автори використовували ланцюг Маркова для виявлення запитів Тарабарського. Вони стверджують, що запропонована ними система здатна ідентифікувати види ransomware, які використовують DGA для зв'язку з командним центром і обміну відкритим ключем.

Крім того, робота, представлена Андроніо [67], може бути реалізована і на цьому етапі. Це означає, що вони використовують підхід для виявлення процесу перехоплення загрозливого тексту з сервера C&C, коли такий текст не вбудований в корисне навантаження ransomware. Кабадж та колеги [70] представили систему виявлення криптовалюти crypto-ransomware на основі мережі (SDN), яка визначається програмно. Їх метод був розроблений виключно на основі спостережень за характеристиками трафіку двох сімейств програм з метою викупу, а саме CryptoWall та Locky.

Вони стверджують, що аналіз послідовності HTTP-повідомлень і їх відповідного розміру вмісту досить для розпізнавання таких загроз. Альмашхадані та інші [71] досліджували мережевий трафік криптовалюти для викупу, використовуючи Locky як приклад дослідження. Після поведінкового аналізу вони запропонували мережевий метод класифікації для виявлення атак.

2.2.4 Захист на етапі виконання

Хоча захист на етапі виконання є дещо пізнім, можна стверджувати, що на цьому етапі розгортаються найбільш практичні рішення щодо захисту раніше невідомих сімейств ransomware. DoDR ransomware вимагає операцій читання і запису файлів для шифрування або фальсифікації їх вмісту. Одним із найбільш ефективних і часто використовуваних методів захисту від ransomware на етапі виконання є моніторинг активності файлової системи за допомогою різних підходів, включаючи перехоплення таблиці дескрипторів системних служб (SSDT).

Також в класі crypto-ransomware стратегія захисту полягає в використанні недоліків в розробці і реалізації алгоритмів криптографії. У разі використання симетричної криптографії, оскільки ключ залишається на машині жертви до тих пір, поки користувач не вийде в мережу і ключ не буде відправлений назад на C&C-сервер, для дампа пам'яті можуть бути використані інструменти криміналістики пам'яті. Ще одним заходом безпеки на цьому етапі є перевірка операцій по перерахуванню папок, які часто зустрічаються в родинах ransomware.

Однак сканери файлової системи також демонструють таку поведінку. Моніторинг та захист головної файлової таблиці (Master File Table, MFT), яка містить інформацію про всі збережені файли та каталоги на томі NTFS, є однією зі стратегій захисту на етапі виконання. У зв'язку з маніпулюванням MBR в атаках цифрових здирників, особливо в категорії locker-ransomware, спостереження за змінами MBR також рекомендується.

Контроль і обмеження доступу до криптографічних інструментів, запропоновані Янг [20], можуть бути першим контрзаходом, який фокусується на фазі виконання для захисту. Однак цей метод не здатний виявити екземпляри ransomware, які використовують вбудовані методи шифрування всередині себе. Як уже згадувалося, на етапі виконання здирницькі програми жадібно переглядають файлову систему в пошуках цільових файлів.

Continella запропонував ShieldFS, додатковий драйвер, який захищає вбудовану файлову систему Windows від загроз ransomware. Він створює набір адаптивних моделей, що містить більше 1,7 мільярда пакетів запитів вводу-виводу (IRP), створених різними доброякісними додатками, і оновлює його, відстежуючи низькорівневу активність файлової системи з плином часу. Запропонований підхід об'єднує цю інформацію з такими даними, як ентропія записів, тимчасова мітка і т.д., щоб відрізнити здирницькі ПЗ від сумлінних. Будь-який процес, що порушує такі моделі, буде визначено як шкідливий, і його робота буде згорнута. Крім того, ShieldFS шукає індикатори, що ілюструють використання симетричних криптографічних примітивів. Для цього він досліджує пам'ять потенційно шкідливих процесів на предмет слідів типових розкладів ключів блокових шифрів.

Харраз і інші [22] заявили, що, вивчаючи запити вводу-виводу і захищаючи MFT в файлової системі NTFS, можна виявити та запобігти значній кількості нових атак вимагачів. В іншій спробі автори розробили систему динамічного аналізу під назвою UNVEIL, яка здатна аналізувати, розпізнавати і моделювати поведінку атак ransomware. Їх методи засновані на моніторингу доступу до файлової системи і вивченні показників неспівпадіння скріншотів, зроблених до, під час і після виконання ransomware. Компонент моніторингу файлової системи має прямий

доступ до буферу даних, які беруть участь в запитах введення-виведення. Він спостерігає за активністю введення-виведення файлової системи через драйвер мініфільтра файлової системи Windows, а не використовує техніку "гачків". У разі категорії locker-ransomware автори використовували OCR-двигун з відкритим вихідним кодом для отримання загрозливого тексту (часто зустрічається в записці з викупом) із скріншотів.

Однак UNVEIL не є рішенням для кінцевих точок і був розроблений з метою аналізу та моделювання атак. Харраз та співавтори [23] запропонували Redemption як рішення для захисту кінцевої точки, здатного відрізнити шкідливі доступи до файлової системи від доброякісних. За словами авторів, воно вимагає мінімального редагування ОС.

З огляду на те, що деякі типи програм-вимагачів використовують власні функції шифрування, недостатньо контролювати виклики стандартних криптографічних бібліотек. Тому Scaife [1] запропонував підхід, орієнтований на дані, під назвою CryptoDrop для виявлення і зупинки атак здирників, які маніпулюють файлами. Замість моніторингу програм CryptoDrop перевіряє дані користувача на предмет підозрілих змін. Автори використовували три основні показники для розпізнавання цих шкідливих змін: зміна типу файлу, вимір подібності за допомогою хеш-функції і ентропія Шеннона.

Дослідник Кім запропонував метод виявлення шкідливого ПЗ на основі білого списку. Вони застосували політику контролю доступу до процедури роботи з файлами. Білий список містить записи про шаблони використання додатків і не потребує оновлення довіреною стороною. Запропонована ними схема складатиметься з таких компонентів моніторингу файлів в режимі ядра: компонента контролю доступу в режимі користувача і БД контролю доступу. Їх метод фокусує свою увагу виключно на документах і системних файлах.

В [2] автори представили підхід, заснований на "медових файлах", для виявлення і запобігання атак ransomware. Як тільки "медові файли", розгорнуті навколо цільового середовища, зчитуються шкідливим процесом, запропонований інструмент під назвою R-Locker блокує атаку.

2.2.5 Захист на етапі вимагання

Групи зловмисиків, що стоять за атаками, шукають не тільки безпечні і невідслідковані, але і прості способи оплати та обміну для жертв. Найбільш відомою цифровою валютою, що використовується в кіберзлочинності, є біткоїн. Однак слід зазначити, що Monero також був помічений в інтернет-атаках, особливо криптомайнерами. Змушуючи жертв платити викуп, хакери, які стоять за ransomware, можуть зміцнити свої позиції, при цьому немає ніякої гарантії відновлення даних і повторення атаки на ту ж жертву. Хоча багато руйнівні операції були проведені до етапу вимагання та доступ до ресурсів було попереджено, цей етап також може надати можливість для захисту.

Більшість досліджень щодо захисту на етапі вимагання зосереджені на аналізі та категоризації транзакцій біткоїнів. Наприклад, деякі дослідники [13] розглянули питання аналізу транзакцій Bitcoin шляхом вивчення тимчасових міток виплати викупу при атаці CryptoLocker. Хуанг і інші [43] провели наскрізний аналіз значної частини екосистеми ransomware, включаючи доходи, партнерські схеми та інфраструктуру. Вони відстежили фінансові операції декількох сімейств ransomware з моменту придбання жертвою біткоїнів до переведення в готівку його операторами ransomware.

Також вчені [48] представили модульну структуру під назвою BitIodine, здатну аналізувати блокчейн і об'єднувати адреси, що належать одному і тому ж суб'єкту. Вони використовували цей фреймворк для створення інструментів криміналістики біткоїнів. Автори приділили особливу увагу візуалізації інформації, витягнутої з мережі біткоїнів.

В дослідженні у джерелі [22] відзначається, що біткоїни-адреси, що використовуються в зловмисних цілях, мають схожі записи транзакцій, включаючи коротку тривалість діяльності, невеликі суми коштів, невеликі записи транзакцій і так далі. Фактично, вони розрізняють і класифікують адреси на основі історії транзакцій. Дослідження Конті показало економічний вплив атак ransomware з точки зору оплати біткоїнів. Автори також представили схему для ідентифікації, збору і

аналізу біткоїн-адрес, керованих одним і тим же користувачем. Вони випустили набір даних, що містить ідентифіковані Bitcoin-адреси, які стосуються атак викупного ПЗ. В [72] представлений керований даними метод виявлення і збору інформації про транзакції Bitcoin, пов'язаних з незаконною діяльністю, заснований на слідах публічного блокчейна Bitcoin. Автори реалізували цей метод на GraphSense, криптовалютної аналітичної платформи з відкритим вихідним кодом, і застосували його для емпіричного аналізу транзакцій, пов'язаних з 35 родинами здирницьких програм.

2.2.6 Захист на етапі емансипації

Ідентифікація сімейства ransomware за інформацією, що міститься в записці з викупом, залишеної на машині жертви, або за допомогою методів аналізу може бути корисною для розблокування або розшифровки уражених файлів. Оскільки деякі варіанти ransomware вже були виявлені сторонніми компаніями з безпеки і випустили свої контрзаходи. Тому всі дослідження, в ході яких були виявлені сімейства ransomware, також можуть бути використані на цьому етапі. Коли жертва дає викуп, щоб відновити доступ до ресурсів, вона провокує інші злочинні угруповання, які націлюються на неї тими ж або іншими способами для аналогічних атак з метою отримання викупу [16].

Невибагливим вирішенням проблеми викупу є наявність безвідмовного резервного плану. На додаток до захисних рішень необхідно мати план резервного копіювання для протидії і пом'якшення наслідків атак ransomware. Резервні копії файлів повинні зберігатися в безпечному і ізольованому місці, що не підлягає впливу загроз ransomware. Оскільки деякі сімейства ransomware почали використовувати файли резервних копій як частину свого етапу виконання. Перевірка точності резервних копій і відновлення файлів з них в тестовому середовищі повинні розглядатися як частина плану резервного копіювання.

Контінелла [73] використовував механізм тіньового копіювання операцій записів для відновлення пошкоджених файлів. CloudRPS [38] надає користувачам

план резервного копіювання поряд з аналізом і запобіганням атак ransomware. Інші спеціалісти [40] запропонували RDS3 і реалізували її в якості стратегії захисту від ransomware. RDS3 забезпечує можливість відновлення шляхом прихованого резервного копіювання даних в вільному просторі обчислювального пристрою.

У запропонованій в [23] схемі посередництва при запитах на доступ до файлів і перенаправлення привілейованих запитів в захищену область підтримується постійний стан вихідних даних користувача, що дозволяє забезпечити можливість відновлення.

Наступні дослідники [41] запропонували підхід до відновлення файлів і систем, заражених ransomware, за допомогою техніки резервного копіювання. Їх методологія полягає в тому, що коли ransomware викликає функції криптографічної бібліотеки, спрацьовує запропонована програма і зберігає секретні ключі в безпечному сховищі. У статті використано припущення, що автори ransomware використовують готові криптографічні бібліотеки, такі як CNG на платформі Windows. Колоденкер та його колеги [42] реалізували PayBreak як механізм проактивного захисту від загроз crypto-ransomware.

Запропонована модель відстежує програми, що викликають криптографічні функції, і перехоплює виклики таких функцій. Потім за допомогою механізму депонування ключів симетричні сеансові ключі надійно зберігаються в сховищі ключів. Надаючи таку можливість, PayBreak дозволяє жертвам отримати заражені файли без сплати викупу. FlashGuard, представлений в [43], являє собою стійкий до вимагання накопичувач (SSD), що забезпечує систему відновлення на рівні прошивки. Розробники модифікували механізм збору сміття накопичувача, щоб зберегти копії уражених і зашифрованих даних. В результаті він здатний відновлювати всі перезаписані сторінки, повертаючись до їх попередніх версій.

Висновки за розділом 2

Керуючись останніми технологічними розробками, масштаби, різноманітність та складність атак-вимагачів значно зросли. Розуміння того, як працюють конкретні

типи вимагальних програм та які технології включені в процес атаки, може дозволити нам краще вибрати відповідний захист. Очевидно, розуміння характеристик вектора, доставки шкідливого програмного забезпечення та мережевого трафіку сервера C&C для вказівки допоможе команді безпеки отримати очікувані результати та вжити відповідних контрзаходів для запобігання або мінімізації поточного збитку для програми-вимогателя.

У підрозділі 2.1 наводиться опис задіяних технологій в формуванні атаки ransomware, а також детальний аналіз традиційних механізмів захисту на кожному етапі запропонованого attack chain.

Незважаючи на існуючі дослідження в області ransomware, залишається кілька проблем, які потребують вирішення. Однією із основних проблем є відсутність повної бази даних примірників ransomware з репрезентативними характеристиками, щоб статті, засновані на машинному навчанні та статистичних методах, могли використовувати загальний набір даних для тестування свого методу і порівняння його з іншими.

Розглядаючи розподіл досліджень за категоріями, можна помітити, що більша увага приділяється наданню захисних рішень на етапі виконання за рахунок жертвування деякою кількістю файлів. З огляду на незворотності наслідків таких атак необхідно більше працювати над превентивними рішеннями на фазах, що передують виконанню. Витяг відмінних ознак на етапі встановлення також є ще однією цікавою темою для дослідження.

РОЗДІЛ 3
КОМПЛЕКС ТЕХНОЛОГІЙ ЗАХИСТУ ВІД АТАК RANSOMWARE, ЗАСНОВАНИЙ НА ЧОТИРЬОХ ЕТАПАХ. МЕТОДИ ВИЯВЛЕННЯ RANSOMWARE. ВСТАНОВЛЕННЯ ТЕХНОЛОГІЇ HONEYDRIVE

3.1 Комплекс технологій захисту від атак ransomware, заснований на чотирьох етапах

Атаки ransomware не є новими в сфері кібербезпеки, але експоненціальна крива зростання зробила її актуальною загрозою для кінцевих користувачів. Для збереження інформаційних систем від атак даного типу пропонується безліч технологій, що працюють у чотири етапи:

I. «predicate» (прогнозування): виявлення вразливостей інформаційної системи;

II. «prevent» (запобігання): запобігання інцидентів;

III. «respond» (відповідь): реагування на порушення, мінімізування шкоди, аналіз;

IV. «detect» (виявлення): розпізнавання інцидентів та загроз, ізолювання та стримування їх.

Для запобігання та виявлення шкідливого коду рекомендуються методи:

1. honeypots (фальшиві комп'ютерні ресурси, які мережеві адміністратори використовують в якості приманки і виявляють будь-який незаконний доступ);

2. cryptolock (зупиняє процес виконання програми, яка фальсифікує набір індикаторів, загальних для ransomware, це може привести до створення ефективної системи виявлення, яка значно зменшує втрати даних жертви);

3. sandboxes (надають жорстко контрольований набір ресурсів для запуску гостьових програм, таких як, наприклад, простір на диску і в пам’яті).

А. Кроки по виявленню та запобіганню, обов'язкові для кожного користувача.

- Регулярне резервне копіювання файлів ;

- макроси вимкнені;

- обережно відкривати небажані вкладення;

- не давати більше повноважень на ведення логів;

- використання антивірусів.

B. Загрози та антивіруси для різних ОС.

1. Загрози на базі Windows і Android: віруси-трояни, Petya і т.д.

2. Linux: Tron Horse, локальні скрипти, Web, черви, цілеспрямовані атаки, Rootkit і т.д.

У Linux використовуються два типи атак: на рівні ядра та на рівні ОС.

3. MAC: У MAC WannaCry, WanaCrypt0r і WCry – це програми-вимагачі, які шифрують файли в системі apple MAC; для захисту. MAC система Clam AV і комерційний продукт, який використовується в якості антивіруса.

C. Сервіс та технології.

1. Служба швидкого виявлення (Rapid Detection Service).

2. F-Secure protection.

3. Послуга для бізнесу.

4. Deepguard

3.2 Чотири методи виявлення ransomware

Рекомендації Microsoft по боротьбі з ransomware полягають в тому, що перевірений надійний режим резервного копіювання – кращий спосіб зменшити шкоду від атаки ransomware. Хоча антивірус все ще рекомендований для використання, він може не оновлюватися досить швидко, щоб блокувати атаку. Microsoft також пропонує AppLocker для блокування програм в загальних місцях для комп'ютерів в керованому домені.

Однак все ще існує ймовірність того, що нові варіанти шкідливих програм будуть записуватися в неконтрольованій області. Виявити ransomware складно через його мінливу природу; він вже обійшов захист периметра брандмауера або спам-фільтра. Не існує простої сигнатури, яка вказувала б на присутність ransomware. Багато хто використовує розширення locky, але шкідливі програми розвиваються і

можуть мати розширення .encrypted або .nochance в залежності від варіанту. Виявлення буде залежати від оновлюваного списку шаблонів імен файлів, який адміністратору мережі буде складно підтримувати в актуальному стані. Тому пошук певних імен файлів або розширень як доказ атаки був відкинутий як відповідний метод.

В якості альтернативного методу була запропонована система, заснована на машинному навчанні. Цей підхід шукав загрозливий текст, пов'язаний з запискою про викуп, а також аналізував потоки даних, щоб визначити, чи відбувається шифрування. На жаль, це рішення призначене для платформи Android і не може бути перенесено на популярну платформу Windows. Знання про те, як виявити активність в програмі-викуп, є головною проблемою захисту від ransomware. Харраз, Амін та інші радять відстежувати активність в таблиці основних файлів (MFT), а також пропонують використовувати ресурси-приманки в якості методу виявлення активності.

По-перше, в пошуках комерційного вирішення проблеми компанія Varonis в своєму продукті DatAdvantage використовує аналітику поведінки користувачів (UBA) для визначення базового рівня нормальної активності. Надалі, коли виникає аномальна активність, наприклад, тисячі модифікацій файлів за короткий час, це може викликати розсилку електронною поштою, що попереджає адміністратора і користувача про те, що стався незвичайний доступ. Інший комерційний продукт – HitmanPro, який виявляє незвичайну поведінку системи, а не типові статичні антивірусні сигнатури.

Функція HitmanPro з обміну виявленої активністю з VirusTotal дає можливість дізнатися більше про атаки. Другий підхід полягає в розміщенні деяких ключових файлів по всій мережі і відстеження змін. Ця ідея tripwire використовує файли-свідки, які відслідковуються на предмет зміни або видалення. Якщо файл-свідок був змінений, служба сервера Lanman зупинялася.

На рис 3.1 показаний елементарний сценарій для виконання аналогічного завдання: якщо простежується відміна копії файлу від оригіналу, мережеві служби будуть зупинені.

```
if ((Get-FileHash . \Readme.txt).hash -ne (Get-FileHash .\original\ReadMe.txt).hash )
        {Stop-Service "LanmanServer" -force}
```

Рис 3.1 Мінімальний сценарій Powershell виявляє зміни та реагує на них

Третій метод виявлення змін полягав у використанні функції, вбудованої в Windows Server, File Server Resource Manager (FSRM). «The suggestion of a canary resource» бере свою назву від практики шахтарів, що спускають канарок в шахти в якості раннього попередження про токсичні гази. Функція контролю доступу називається File Screening і може використовуватися для блокування записів неавторизованих файлів. Ця ідея була розширена для використання PowerShell для блокування доступу користувача-порушника.

Четверте та останнє рішення: продукт EventSentry здатний відстежувати журнали безпеки Windows і запускати дії, коли активність користувача перевищує поріг. Це продукт управління інформацією безпеки (Security information management - SIM) для об'єднання файлів журналів. Дії можуть полягати у відправці електронного листа або виклику виключення сервера. Цей продукт доступний у вигляді повнофункціонального комерційного продукту, проте безкоштовна версія EventSentry Light забезпечує функціональність для проведення необхідного моніторингу і дій.

Більш ефективним методом виявлення, ніж четвертий, є системи SIEM, але для простоти реалізації було обрано саме EventSentry Визначивши, що існує кілька підходів до виявлення ransomware, необхідно було провести подальше дослідження, щоб визначити, яке рішення буде найкраще відповідати вимогам, щоб викликати дію при виявленні вторгнення.

3.3 Модель реагування на попередження

У якийсь момент методи запобігання не зможуть захистити від нових і невідомих методів атак, тому наступною лінією захисту стають системи виявлення

вторгнень. Якщо розглядати використання honeypot як системи виявлення вторгнень, то honeypot не запобігають вторгнення, але можна порівняти з сигналізацією, коли індикатор вторгнення дає системному адміністраторові можливість запобігти подальшому поширенню шкоди системі.

Метою дослідження було визначити відповідний метод виявлення ransomware та впровадити його, щоб додати додатковий рівень безпеки в мережу; для захисту мережі дії повинні бути зроблені після отримання інформації про атаку, проте, відключення сервера, коли користувач законно оновлює колекцію файлів, було б суворою реакцією. І навпаки, відсутність швидкої реакції на атаку ransomware призведе до того, що ще більше файлів будуть зашифровані.

Для того, щоб використання нешкідливого ПЗ не викликало занадто жорсткі дії, була визначена ієрархія заходів у відповідь. Модель реагування на попередження показана на рисунку 3.2

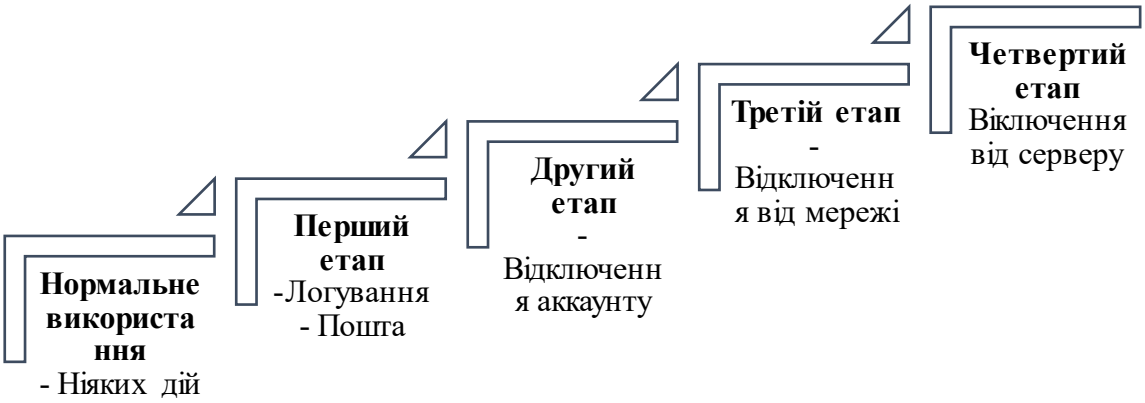

Рис. 3.2 Багаторівнева реакція на виявлення

A. Перший етап.

Спрацьовує при першому виявленні зміни. Це необхідно для того, щоб відправити системному адміністратору повідомлення про те, що в контрольованій папці були внесені зміни.

B. Другий.

Генерується при виявленні більшої активності. На цьому рівні необхідно визначити ім'я користувача або ім'я станції атакуючої шкідливої програми. За

допомогою цієї інформації користувач може відключити свій мережевий обліковий запис або відключити сеанси станції.

C. Третій.

Наступний рівень активності пропонує зупинити мережеві служби.

D. Четвертий.

Проводиться при досягненні четвертого порога змін. На цьому етапі буде визначено, що попередження адміністратора та блокування доступу користувачів недостатньо, щоб зупинити поширення збитку, тому остаточним захистом буде відключення сервера

3.4. Вибраний метод виявлення за допомогою технології honeypot

Стежки, що розміщують файли-свідки, розкидані по мережі. Аналіз дій ransomware показав, що атака часто відбувається в алфавітному порядку через підключення диски, тому в якості доповнення до стежки була обрана початкова буква алфавіту в області honeypot. Хоча ім'я файлу, таке як «####### Tripwire.txt», в алфавітному порядку буде одним з перших, це можна легко запобігти, змінивши порядок атакованих файлів, тобто всі файли, виявлені раніше, будуть атаковані останніми. Отже, використання файлу-свідка як тріпвайра для виявлення активності було виключено.

Аналогічним чином була відкинута і аналітика поведінки користувачів, оскільки після того, як UBA дізнається про нормальні дії, він зможе виявити незвичайний доступ до області зберігання, наприклад, неавторизованих користувачів або зламаного облікового запису. Система захисту, нездатна забезпечити безпеку в очікуванні збору базових даних, не дає впевненості в тому, що прогнозовані атаки будуть перехоплені коли-небудь в майбутньому.

Таким чином, залишилося два підходи виявлення здирницького ПЗ: спочатку папка "honeypot" контролюється за допомогою FSRM File Screen, а потім спостерігаються зміни в журналах подій Windows. FSRM може бути оновлений відомими іменами файлів і розширеннями останніх атак, розміщених на GitHub. Це

ефективний метод блокування записів програм-вимагачів в певну папку honeypot. Далі EventSentry був налаштований відповідно до інструкцій [74] для налаштування аудиту файлів за подією 4663: Була зроблена спроба доступу до об'єкта.

Дії налаштовані за трьома рівнями: електронна пошта, зупинка служби сервера і, нарешті, відключення служби. Вони будуть пов'язані з фільтрами, з необхідними граничними значеннями для запуску дії. Визначення цього порога вимагає деякого розгляду, занадто низький поріг може привести до появи безлічі помилкових попереджень, і навпаки, занадто високий поріг може привести до відсутності спрацьовування. Кожна мережа буде мати різні характеристики використання, але для експерименту можна обрати десятисекундний період.

Подвоєння нормальної активності є базовим рівнем для початку будь-якої дії, тому більше 50 змін файлів підвищували рівень першого етапу реагування; в три рази вище базового, тобто 150, підвищували рівень другого, в десять разів вище базового, 500, запускали третій рівень, і, нарешті 1000 активували четвертий рівень. Можливість копіювати, вставляти фільтри та змінювати порогові значення дозволяє виконати цей процес ефективно.

3.5. Встановлення технології Honeydrive для виявлення атак ransomware

HoneyDrive – це головний honeypot-дистрибутив Linux. Він являє собою віртуальний пристрій (OVA) зі встановленою редакцією Xubuntu Desktop 12.04.4 LTS. Він містить понад 10 попередньо сконфігурованих програмних пакетів медових точок, таких як Kippo SSH honeypot, Dionaea і Amun, Honeyd low-interaction honeypot, Glastopf web honeypot і Wordpot, Conpot SCADA / ICS honeypot, Thug і PhoneyC honeyclients та інші.

Крім того, він включає безліч корисних попередньо налаштованих скриптів і утиліт для аналізу, візуалізації та обробки даних, які він може захопити, таких як Kippo-Graph, Honeyd-Viz, DionaeaFR, стек ELK і багато іншого. Нарешті, майже 90 відомих інструментів для аналізу шкідливого ПЗ, криміналістики і мережевого

моніторингу також присутні в дистрибутиві. На рисунку 3.4 зображений робочий стіл віртуальної машини HoneyDrive.

Рис 3.3 Honeydrive

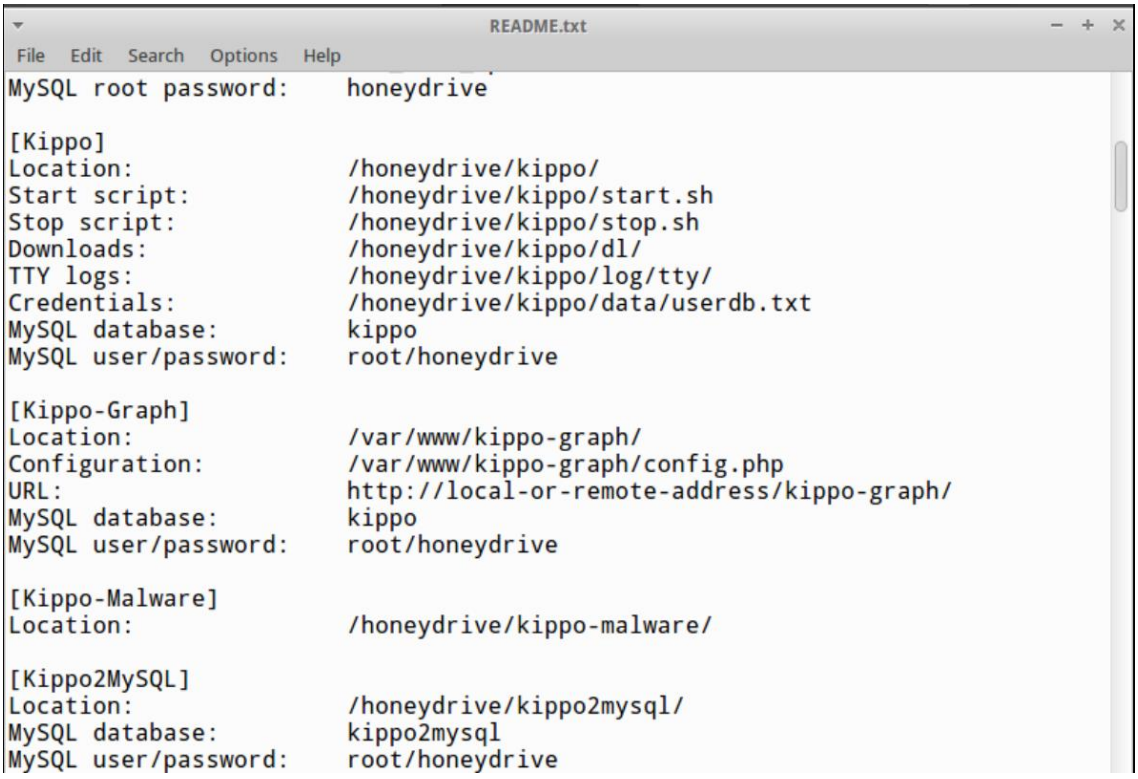

Рис. 3.4 Текстовий файл з інформацією README.txt

Слід приділити увагу файлу readme, простому текстового файлу, в якому збережені шляхи до файлів і команди кількох встановлених honeypots'ів.

3.5.1 Налаштування Kippo

Вся інформація про налаштування знаходяться в текстовому файлі, але ось основний алгоритм дій:

- cd /honeydrive/kippo/
- /honeydrive/kippo/start.sh
- Ifconfig (IP-адреса віртуального honeypot)
- Ввести цей IP в адресний рядок браузера, завантажити.

Тепер, коли сервер працює правильно, можна ввімкнути переадресацію портів, щоб вхідний трафік перенаправлявся на honeypot. Після цього потрібно перейти на http: // yourip / kippo-graph /, щоб подивитися цікаву інформацію про паролі, які намагалися використовувати зловмисники, імена користувачів, IP-адреси та інших дуже цікавих речах.

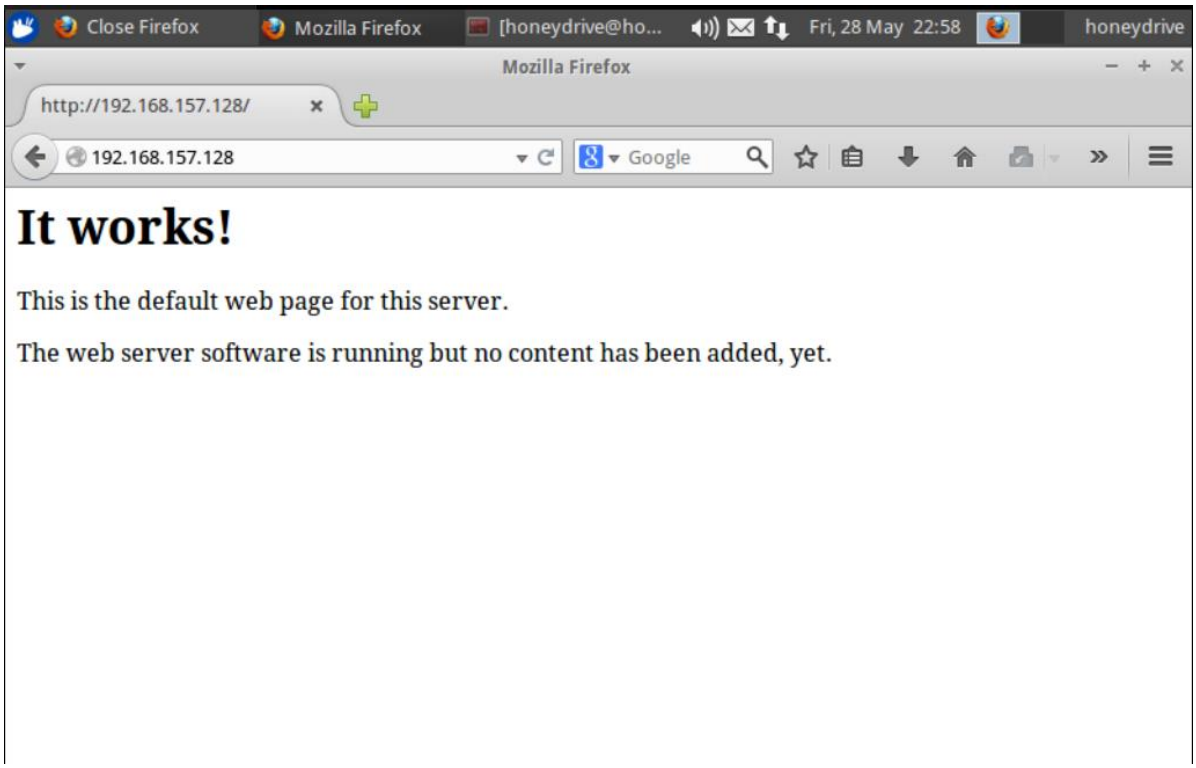

Рис. 3.4 Сторінка, яка сповіщає, що ми налаштували honeypot

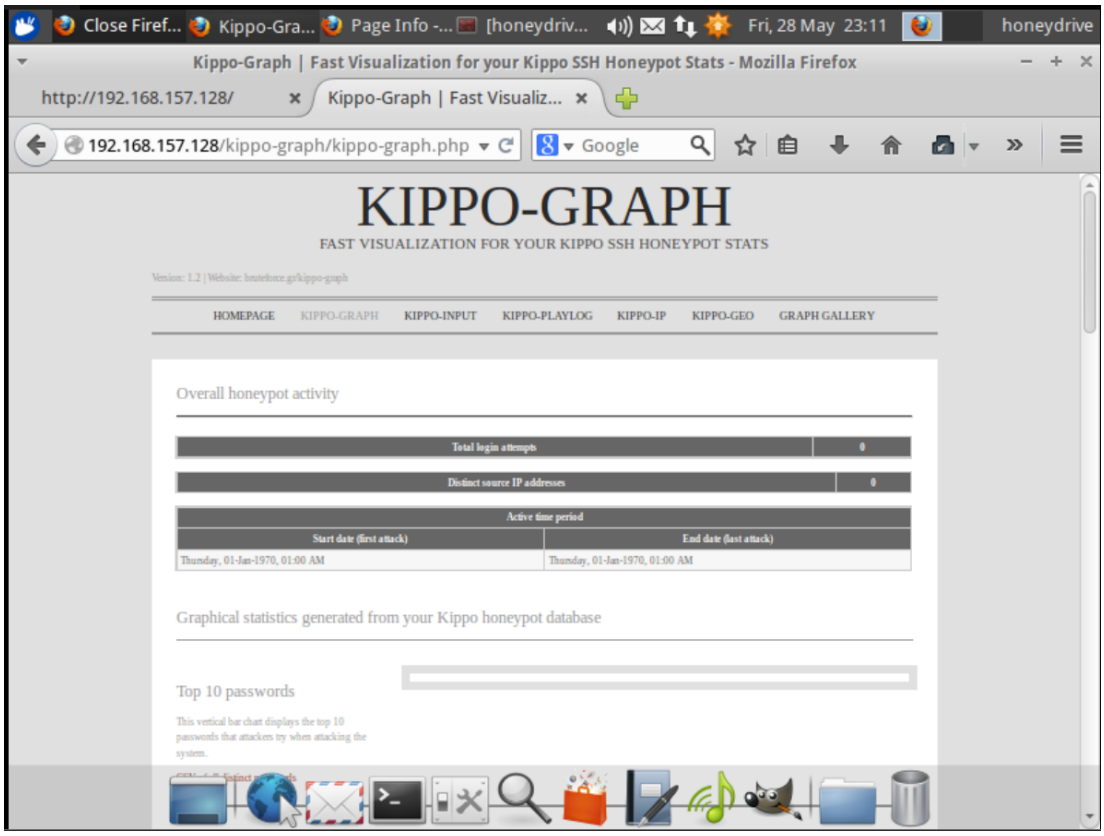

Рис. 3.5 Статистика та записи Kippo

Висновки до розділу 3

Був розроблений комплекс технологій захисту від атак ransomware, заснований на чотирьох етапах та розглянута багаторівнева реакція на виявлення. Для запобігання та виявлення шкідливого коду рекомендую використовувати такі методи як: honeypots (фальшиві комп'ютерні ресурси, які мережеві адміністратори використовують в якості приманки і виявляють будь-який незаконний доступ); cryptolock (зупиняє процес виконання програми, яка фальсифікує набір індикаторів, загальних для ransomware, це може привести до створення ефективної системи виявлення, яка значнозменшує втрати даних жертви); sandboxes (надають жорстко контрольований набір ресурсів для запуску гостьових програм, таких як, наприклад, простір на диску і в пам’яті).

Проаналізований вибраний метод виявлення за допомогою технології honeypot.

Хоча можна розгорнути фальшиві папки типу honeypot з файлами-тріпвайрами для взаємодії з ransomware, природа папок-обманок така, що немає ніякої гарантії, що шкідливе ПЗ спробує вторгнутися в ці області, і, отже, обійти цей захист. Такий обмежений погляд на систему є недоліком "медових точок", оскільки відсутність в "медової точці" попереджень про атаки не є показником того, що інші області не піддаються атакам. Оскільки шкідливі програми автоматизовані і можуть довільно атакувати будь-яке місце, розміщення honeypot в будь-якому місці для виявлення активності є поліпшенням у порівнянні з відсутністю моніторингу взагалі. Принципи honeypot, що стосуються збору інформації про атаку та її використання для захисту, як і раніше цінні. Honeypot може ідентифікувати користувача, а також обсяг змінюваних файлів, і це може послужити підставою для прийняття відповідних заходів. Сповіщення користувачів електронною поштою також повинні супроводжуватися навчанням по підвищенню обізнаності користувачів, можливо, повідомлення повинно містити прохання відключити мережевий кабель. Досліджено чотири методи виявлення атак ransm

Було встановлено HoneyDrive для розуміння, як працюють технології honeypot, а саме Kippo.

ВИСНОВКИ

У дипломній роботі розглянуто поняття ransomware, проведений аналітичний огляд та класифікація усього шкідливого забезпечення, де особлива увага приділяється вітці scareware. На базі класифікації сформований attack chain та розглянуті традиційні методи захисту на кожному етапі перебування шкідливого ПЗ в системі. Проаналізовані залучені технології, які використовують зловмисники для формування атак ransomware.

На основі досліджень побудовано комплекс технологій захисту, що побудований на чотирьох етапах. Для досягнення поставленої мети роботи використано дослідження ransomware через призму роботи honeypot, який базується на вибраній комбінації методів виявлення.

За результатами проведення дослідження сформований висновок про те, викуп може вести себе по-різному на різних платформах, тому, використовуючи деякі методи, такі як CryptoLock, Heldroid, жертва може захистити свої дані. MAC і Linux мають дуже безпечне середовище, тому загрози не можуть легко вплинути на них, але дослідження показало, що зловмисники також атакують MAC і Linux, але їх методи захисту все ще не знайдені.

Практична цінність кваліфікаційної роботи полягає у вдосконаленні технологій захисту проти атак ransomware та представлення чотирьох-етапного комплексу захисту від атак ransomware, а також обрання найбільш ефективного методу виявлення з технологією honeypot.

Мету роботи, а саме створення експериментальної бази для наукових досліджень та побудова ефективної захисної стратегії проти атак типу ransomware, досягнуто, поставлені задачі виконані.

Дана дипломна робота була апробована на науково-практичній конференції «Інформаційно-телекомунікаційні системи і технології та кібербезпека: наукові виклики, нові завдання».

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. N. Scaife, H. Carter, P. Traynor, K.R.B. Butler, CryptoLock (and drop it.: Stopping ransomware attacks on user data.

2. J.A. Gómez-Hernández, L. Álvarez González, P. García-Teodoro, R-Locker: Thwarting ransomware action through a honeyfile-based approach.

3. E.Mercaldo, V. Nardone, A. Santone, C.A. Visaggio, Ransomware steals your phone. Formal methods rescue it, in: International Conference on Formal Techniques for Distributed Objects, Components, and Systems – Springer.

4. D. Sgandurra, L. Munoz-Gonzalez, R. Mohsen, E.C. Lupu, Automated dynamic analysis of ransomware: Benefits, limitations and use for detection – 2016.

5. A. Cuzzocrea, F. Martinelli, F. Mercaldo, A novel structural-entropy-based classification technique for supporting android ransomware detection and analysis.

6. H. Zhang, X. Xiao, F. Mercaldo, S. Ni, F. Martinelli, A.K. Sangaiah, Classification of ransomware families with machine learning based on N-gram of opcodes.

7. S. Homayoun, A. Dehghantanha, M. Ahmadzadeh, S. Hashemi, R. Khayami, Know abnormal find evil: frequent pattern mining for ransomware threat hunting and intelligence.

8. 2017 Internet Crime Report, IC3 [Електронний ресурс] – Режим доступу: https://pdf.ic3.gov/2017_IC3Report.

9. 2018 Data Breach Investigations Report, Verizon [Електронний ресурс] – Режим
доступу: https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf.

10. J. Bates, Trojan horse: AIDS information introductory diskette version 2.0, Oxon, UK, 1990, pp. 3–6.

11. A.L. Young, M. Yung, Cryptovirology: Extortion-based security threats and countermeasures, 1996, pp. 129–141.

12. N. Lee, Cyber warfare: weapon of mass disruption, Springer, New York, NY, 2013, pp. 99–118.

13. K. Liao, Z. Zhao, A. Doupe, G.J. Ahn, Behind closed doors: measurement and analysis of cryptolocker ransoms in bitcoin – 2016 — 1–13.

14. CR. Srinivasan, Hobby hackers to billion-dollar industry: the evolution of ransomware.

15. B.A.S. Al-rimy, M.A. Maarof, S.Z.M. Shaid, Ransomware threat success factors, taxonomy, and countermeasures: a survey and research directions.

16. C. Everett, Ransomware: to pay or not to pay? Comput. Fraud Secur.

17. A. Azmoodeh, A. Dehghantanha, M. Conti, K.K.R. Choo, Detecting cryptoransomware in IoT networks based on energy consumption footprint — 1–12.

18. S. Gibbs, Ransomware attack on san Francisco public transit gives everyone a free ride — 2016 [Електронний ресурс] – Режим доступу:

https://www.theguardian.com/technology/2016/nov/28/passengers-free-ride-san-francisco-muni-ransomware.

19. F. Touchette, The evolution of malware, Netw. Secur.

20. A.L. Young, M. Yung, Cryptovirology: The birth, neglect, and explosion of ransomware, Commun. ACM 60 (7. (2017. 24–26.

21. A.L. Young, Cryptoviral extortion using Microsoft's crypto API — 2006 — 67–76.

22. A. Kharraz, W. Robertson, D. Balzarotti, L. Bilge, E. Kirda, Cutting the Gordian knot: A look under the hood of ransomware attacks, in: International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment: 12th International Conference, DIMVA2015, Springer, Milan, Italy — 2015, — 3–24.

23. A. Kharraz, E. Kirda, Redemption: real-time protection against ransomware at end-hosts — 2017.

24. N. Hampton and Z. A. Baig, "Ransomware: Emergence of the cyber-extortion menace," in Australian Information Security Management, Perth — 2015.

25. A. Gazet, "Comparative analysis of various ransomware virii", 2008, pp. 77-90.

26. M. Garnaeva, J. van der Wiel, D. Makrushin, A. Ivanov and Y. Namestnikov, “Kaspersky Security Bulletin 2015. Overall statistics for 2015,” [Електронний ресурс] – Режим доступу: https://securelist.com/analysis/kaspersky-securitybulletin/73038/kaspersky-security-bulletin-2015-overallstatistics-for-2015/.

27. C. Everett, “Ransomware: to pay or not to pay?” Computer Fraud & Security — 8-12—2016.

28. Cisco, “Cisco 2015 Midyear Security Report,” Cisco, San Jose— 2015.

29. L. Spitzner, Honeypots: tracking hackers, Boston: Addison Wesley — 2002.

30. C.N. Gutierrez, E.H. Spafford, S. Bagchi, T. Yurek, Reactive redundancy for data destruction protection (R2D2..

31. Symantec Security Response Team, What you need to know about the WannaCry Ransomware — 2017 [Електронний ресурс] – Режим доступу: https://www.symantec.com/blogs/threatintelligence/wannacry-ransomware-attack.

32. A. Dahan, Night of the devil: Ransomware or wiper? A look into targeted attacks in Japan using MBR-ONI, 2017 [Електронний ресурс] – Режим доступу: https://www.cybereason.com/blog/ night-of-the-devil-ransomware-or-wiper-a-look- into-targeted-attacksin-japan.

33. C. Cimpanu, Ordinypt ransomware intentionally destroys files, currently targeting Germany — 2017 [Електронний ресурс] – Режим доступу: https://www.bleepingcomputer.com/news/ security/ordinypt-ransomware- intentionally-destroys-files-currentlytargeting-germany.

34. I. Yaqoob, I.A.T. Hashem, A. Ahmed, S.A. Kazmi, C.S. Hong, Internet of things forensics: Recent advances, taxonomy, requirement, and open challenges, Future Gener. Comput. Syst. 92 — 2019.

35. Monika P. Zavarsky, D. Lindskog, Experimental analysis of ransomware on windows and android platforms: Evolution and characterization, in: 2nd International Workshop on Future Information Security, Privacy & Forensics for Complex Systems — 2016 — 465–472.

36. N. Scaife, H. Carter, P. Traynor, K.R.B. Butler, CryptoLock (and drop it.: Stopping ransomware attacks on user data, in: 2016 IEEE 36th International Conference on Distributed Computing Systems, ICDCS — 2016 — 303–312.

37. J.A. Gómez-Hernández, L. Álvarez González, P. García-Teodoro, R-Locker: Thwarting ransomware action through a honeyfile-based approach — 2018 — 389–398.

38. M. Spagnuolo, F. Maggi, S. Zanero, Bitiodine: extracting intelligence from the bitcoin network, in: N. Christin, R. Safavi-Naini (Eds.., FC 2014, in: LNCS, vol. 8437, International Financial Cryptography Association — 2014 — 457–468.

39. J.K. Lee, S.Y. Moon, J.H. Park, CloudRPS: a cloud analysis based enhanced ransomware prevention system, J. Supercomout. —(2017 — 3065–3084.

40. K.P. Subedi, D.R. Budhathoki, B. Chen, D. Dasgupta, Dasgupta, RDS3: Ransomware defense strategy by using stealthily spare space, in: 2017 IEEE Symposium Series on Computational Intelligence, SSCI, Honolulu, HI — 2017 — 1–8.

41. K. Lee, K. Yim, J.T. Seo, Ransomware prevention technique using key backup — 2017.

42. E. Kolodenker, W. Koch, G. Stringhini, M. Egele, PAYBREAK: Defense against cryptographic ransomware, in: Processing of the ACM on Asia Conference on Computer and Communications Security, Abu Dhabi, United Arab Emirates — 2017 — 599–911.

43. J. Huang, J. Xu, X. Xing, P. Liu, M.K. Qureshi, FlashGuard: Leveraging intrinsic flash properties to defend against encryption ransomware, in: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS'17, Dallas, TX, USA — 2017 — 2231–2244.

44. I. Yaqoob, E. Ahmed, M.H.u. Rehman, A.I.A. Ahmed, M.A. Al-garadi, M. Imran, M. Guizani, The rise of ransomware and emerging security challenges in the internet of things, Comput. Netw —2017.

45. A. Zimba, Z. Wang, H. Chen, Multi-stage crypto ransomware attacks: A new emerging cyber threat to critical infrastructure and industrial control systems, ICT Express — 2018.

46. K. Savage, P. Coogan, H. Lau, The evolution of ransomware, SECURITY RESPONSE — 2015.

47. E.M. Hutchins, M.J. Cloppert, R.M. Amin, Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains — 2011.

48. P. O'Kane, S. Sezer, D. Carlin, The evolution of ransomware, IET Netw. 7 (5. — 2018 — 321–327.

49. X. Luo, Q. Liao, Awareness education as the key to ransomware prevention, Inf. Syst. Secur — 2007 — 195–202.

50. P. Bajpai, A.K. Sood, R. Enbody, A key-management-based taxonomy for ransomware, in: 2018 APWG Symposium on Electronic Crime Research, eCrime, San Diego, CA — 2018 — 1–12.

51. M.M. Ahmadian, H.R. Shahriari, S.M. Ghaffarian, Connection-monitor & connection-breaker: A novel approach for prevention and detection of high survivable ransomware, in: Paper Presented At the 12th International Iranian Society of Cryptology Conference on Information Security and Cryptology, ISCISC, IEEE, Iran, Rasht — 2015 — 79–84.

52. A. Pektas, T. Acarman, Classification of malware families based on runtime behaviors, J. Inf. Secur. Appl. — 2017 — 91–100.

53. Trend Micro, SynAck ransomware leverages process Doppelgänging for evasion and infection — 2018 [Електронний ресурс] –
Режим доступу: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/synack-ransomwareleverages-process-doppelg-nging-for-evasion-and-infection.

54. A. Lelli, Microsoft Malware Protection Center, Ransomware operators are hiding

malware deeper in installer packages — 2017 [Електронний ресурс] – Режим доступу: https://cloudblogs.microsoft.com/microsoftsecure/2017/03/15/ransomwareoperators-are-hiding-malware-deeper- in- installer-packages.

55. J. Wyke, A. Ajjan, The Current State of Ransomware, Tech. Rep. December, Sophos — 2015 [Електронний ресурс] – Режим доступу: https://www.sophos.com/en-us/medialibrary/PDFs/ technicalpapers/sophos-current-state-of-ransomware.pdf

56. A.K. Sood, S. Zeadally, A taxonomy of domain-generation algorithms, IEEE Secur. Priv. 14 (4. — 2016— 46–53.

57. R. Falcone, J. Grunzweig, Targeted ransomware attacks middle eastern government organizations for political purposes, 2017 [Електронний ресурс] – Режим доступу: https://researchcenter.paloaltonetworks.com/2017/03/unit42-targetedransomware-attacks-middle-eastern-government-organizations-politicalpurposes.

58. C. Puodzius, How encryption molded crypto-ransomware —2016 [Електронний ресурс] – Режим доступу: http://www.welivesecurity.com/2016/09/13/how-encryption-moldedcrypto-ransomware.

59. A. Palisse, H. Le Bouder, J.L. Lanet, C. Le Guernic, A. Legay, Ransomware and the legacy crypto API.

60. Y. Xie, F. Yu, K. Achan, R. Panigrahy, G. Hulten, I. Osipkov, Spamming botnets: Signatures and characteristics, in: Proceedings of ACM SIGCOMM — 2008.

61. S. Pletinckx, C. Trap, C. Doerr, Malware coordination using the blockchain: An analysis of the cerber ransomware, in: 2018 IEEE Conference on Communications and Network Security, CNS, Beijing — 2018 — 1–9.

62. D. Goel, A.K. Jain, Mobile phishing attacks and defence mechanisms: State of art and open research challenges — 2018 — 519–544.

63. E.M. Rudd, R. Harang, J. Saxe, MEADE: Towards a malicious email attachment detection engine, in: IEEE Symposium on Technologies for Homeland Security, HST, 2018, arXiv:1804.08162.

64. I. Jeun, Y. Lee, D. Won, Collecting and filtering out phishing suspicious URLs using spam trap system.

65. P. Lestringant, F. Guihery, P.A. Fouque, Automated identification of cryptographic primitives in binary code with data flow graph isomorphism.

66. D. Xu, J. Ming, D. Wu, Cryptographic function detection in obfuscated binaries via bit-precise symbolic loop mapping, in: Proceedings of the 38th IEEE Symposium on Security and Privacy, SP — 2017 — 921–937.

67. N. Andronio, S. Zanero, F. Maggi, HelDroid: Dissecting and detecting mobile ransomware, in: Research in Attacks, Intrusions, and Defenses, Springer — 2015 — 382–404.

68. M. Rhode, P. Burnap, K. Jones, Early-stage malware prediction using recurrent neural networks, Comput. Secur. 77 — 2018 — 578–594.

69. M. Antonakakis, R. Perdisci, Y. Nadji, N. Vasiloglou, S. Abu-Nimeh, W. Lee, D. Dagon, From throw-away traffic to bots: Detecting the rise of DGAbased malware, USA —2012 — 491–506.

70. K. Cabaj, M. Gregorczyk, W. Mazurczyk, Software-defined networkingbased crypto ransomware detection using HTTP traffic characteristics, Comput. Electr. Eng. 66 — 2018.

71. A.O. Almashhadani, M. Kaiiali, S. Sezer, P. O'Kane, A multi-classifier network-based crypto ransomware detection system: A case study of Locky ransomware, IEEE Access 7 —2019 — 47053–47067.

72. M. Paquet-Clouston, B. Haslhofer, B. Dupont, Ransomware payments in the bitcoin ecosystem, in: 17th Annual Workshop on the Economics of Information Security, WEIS —2018 — arXiv:1804.04080.

73. A. Continella, A. Guagnelli, G. Zingaro, G. De Pasquale, A. Barenghi, S. Zanero, F. Maggi, ShieldFS: A self-healing ransomware-aware filesystem — 2016 — 336–347.

74. I. Koecher, "Defeating Ransomware with EventSentry & Auditing," [Електронний ресурс] –

Режим доступу: http://www.eventsentry.com/blog/2016/03/defeatingransomware-with eventsentry-auditing.html.

ДОДАТОК А

Таблиця 2.1

Індикатори, витягнуті з деяких зразків ransomware на основі attack chain

Зразки здирницький програм	Показники, які беруть участь в:					
	Етап зараження	Етап інсталяції	Етап зв'язку	Етап виконання	Етап вимагання	Етап емансипації
Cerber	-Спам електронною поштою -Набір експлойтів -Реклама	-Шкідлива програма встановлення NSIS -Ін'єкція коду -Видалення тіньових записів томів -Модифікація реєстру для сталості	-Мінімальна мережева активність -Використання DGA -Передача статистики	-Шифрування -Список каталогів -Викрадення Bitcoin-гаманця	-Вимагання грошей (біткоіни) -Tor	-Розфифрування

Продовження таблиці 2.1

Зразки здирницький програм	Показники, які беруть участь в:					
	Етап зараження	Етап інсталяції	Етап зв'язку	Етап виконання	Етап вимагання	Етап емансипації
WannaCry	-Експлуатація вразливостей -Розповсюджується самостійно	-Видалення тіньових записів томів -Модифікація реєстру	-Використання жорстко заданого URL	-Шифрування -Список каталогів -Перерахування сеансу RDP	-Вимагання грошей (біткоїни) -Tor	- Нічого
CryptoLocker	-Спам електронною поштою -Експлуатація вразливостей	-Ін'єкція коду -Видалення тіньових записів томів	-Використання DGA -Обмін ключами -Передача статистики	-Шифрування -Список каталогів -Викрадення контактів -Модифікація MBR	-Вимагання грошей (cashU, Ukash, MoneyPak та біткоїни)	-Розфифрування

Продовження таблиці 2.1

Зразки здирницький програм	Показники, які беруть участь в:					
	Етап зараження	Етап інсталяції	Етап зв'язку	Етап виконання	Етап вимагання	Етап емансипації
Locky	-Спам електронною поштою -Набір експлойтів	-Шкідлива програма встановлення NSIS - Видалення тіньових записів томів	- Використання жорстко заданого URL - Використання DGA -Обмін ключами	- Шифрування -Список каталогів	- Вимагання грошей (біткоїни) -Tor	- Розфифрування
Petya	- Шкідливеоновлення програми звітності (M.E.Doc) - -Експлуатація вразливостей	-Ухилення від процесу - Встановлення чорного ходу -Ескалація привілеїв	-	-Встановлення власної користувальницької ОС -Шифрування файлової системи під час завантаження диска -Список каталогів -Викрадення облікових даних -Модифікація MBR	- Вимагання грошей (біткоїни)	- Нічого