ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Дослідження шляхів та розробка рекомендацій щодо аналізу шкідливого програмного забезпечення для реагування на кіберінциденти на базі рішення Check Point NGFW»

зі спеціальності *125 Кібербезпека*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Денис ДЄДІЩЕВ
(підпис)

Виконав: здобувач вищої освіти групи БСД-43
ДЄДІЩЕВ Денис
(прізвище, ім'я)

Керівник асистент БОЙКО Анна
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Бакалавр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Галина ГАЙДУР
“___” _____ 2024 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дєдіщеву Денису Олеговичу
(прізвище, ім’я)

1. Тема кваліфікаційної роботи: «Дослідження шляхів та розробка рекомендацій щодо аналізу шкідливого програмного забезпечення для реагування на кіберінциденти на базі рішення Check Point NGFW

керівник кваліфікаційної роботи Бойко Анна, асистент
(прізвище, ім’я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «___» _____ 2024 року № ____.

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 31.05.2024 р.

3. Вихідні дані до кваліфікаційної роботи
рішення Check Point NGFW;
зразок файлу шкідливого програмного забезпечення задіяного в цільової атаці UAC-0050 "Повістка до суду".

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Дослідження методів аналізу шкідливого програмного забезпечення.
2. Аналіз методів та засобів захисту в рамках реагування на шкідливе програмне забезпечення на базі Check Point NGFW.
3. Розроблення рекомендацій щодо реагуванню на шкідливе програмне забезпечення за допомогою проведеного аналізу на базі Check Point NGFW.

5. Перелік графічного матеріалу
Презентація PowerPoint.

6. Дата видачі завдання 15.04.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення актуальності загрози шкідливим програмним забезпеченням.	10.02.2024 р.	
2.	Аналіз існуючих інструментів для аналізу шкідливого програмного забезпечення.	20.02.2024 р.	
3.	Аналіз рішення Check Point NGFW.	01.03.2024 р.	
4.	Визначення прикладу для наглядного відображення аналізу ШПЗ на базі реального кіберінциденту.	15.03.2024 р.	
5.	Розроблення рекомендацій щодо застосування результатів аналізу шкідливого програмного забезпечення для протидії ШПЗ на базі рішення Check Point NGFW.	01.04.2024 р.	
6.	Практична реалізація аналізу шкідливого програмного забезпечення та використання Check Point NGFW для протидії ШПЗ.	10.04.2024 р.	
7.	Оформлення результатів дослідження.	01.05.2024 р.	
8.	Підготовка доповіді до захисту.	31.05.2024 р.	

Здобувач вищої освіти _____ Денис ДЄДІЩЕВ
(підпис) *(ім'я, прізвище)*

Керівник кваліфікаційної роботи _____ Анна БОЙКО
(підпис) *(ім'я, прізвище)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу

здобувача ДЄДІЩЕВА Дениса

на тему: «Дослідження шляхів та розробка рекомендацій щодо аналізу шкідливого програмного забезпечення для реагування на кіберінциденти на базі рішення Check Point NGFW»

Актуальність: Реагування на зловмисну активність шкідливого програмного забезпечення має важливе значення для запобігання несанкціонованому доступу, витоку даних і втраті даних. Рішення NGFW забезпечує фільтрацію трафіку, що проходить крізь нього дозволяючи організаціям підтримувати видимість стану безпеки та завчасно реагувати на нові загрози.

Аналіз шкідливого програмного забезпечення дозволяє видобути необхідні дані про певне ШПЗ, коректне використання яких дозволяє ефективно протидіяти ШПЗ навіть у випадку коли інші рішення по типу антивірусного захисту не справляється зі своєю задачею, що може призвести до простою, що впливає на продуктивність і безперервність бізнесу. Тому тема кваліфікаційної роботи є актуальною та своєчасною.

Позитивні сторони:

1. На основі проведеного аналізу, в роботі встановлено зміст проблеми шкідливого програмного забезпечення та визначено мету та завдання його аналізу, а також складові частини його процедури.
2. Досліджено безкоштовні рішення для аналізу шкідливого програмного забезпечення, якими може скористатись будь-яка за розміром організація.
3. Запропоновано варіанти використання результатів проведеного аналізу на базі реального кіберінциденту, який в свій час потурбував більшу частину організацій України.
4. Текст викладено достатньо грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Наведено багато наглядних прикладів при виконанні технічної частини даної кваліфікаційної роботи.

Недоліки:

1. У кваліфікаційній роботі бажано було б провести більш детальний аналіз шкідливого програмного забезпечення, щоб видобути з його результатів не тільки алгоритму дій та IoC`s, а розібрати зловмисний код та скрипти, які були написані зловмисником.

Відзначене зауваження не впливає на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку **“добре”**, а здобувач(ка) **ДЄДІЩЕВ Денис** – присвоєння кваліфікації бакалавр з кібербезпеки за спеціалізацією Інформаційна та кібернетична безпека.

Рецензент:

(науковий ступінь, вчене звання)	*(підпис)*	*(ім’я, прізвище)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ

на здобуття освітнього ступеня бакалавра

Направляється здобувач ДЄДІЩЕВ Денис до захисту кваліфікаційної роботи
(прізвище, ім'я)

спеціальності 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)

на тему: «Дослідження шляхів та розробка рекомендацій щодо аналізу шкідливого програмного забезпечення для реагування на кіберінциденти на базі рішення Check Point NGFW».

Кваліфікаційна робота і рецензія додаються.

Директор інституту _____ Віталій САВЧЕНКО
(підпис) *(ім'я, прізвище)*

Висновок керівника кваліфікаційної роботи

Здобувач ***ДЄДІЩЕВ Денис*** обрав тему роботи, метою якої було дослідити методи та засоби аналізу шкідливого програмного забезпечення для реагування на кіберінциденти. Перелік використаних джерел свідчить про вміння здобувачем розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання кваліфікаційної роботи ***ДЄДІЩЕВ Денис*** показав добру теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача ***ДЄДІЩЕВА Дениса*** на оцінку **"добре"** та присвоїти йому кваліфікацію бакалавр з кібербезпеки за спеціалізацією Інформаційна та кібернетична безпека.

Керівник кваліфікаційної роботи _____ Анна БОЙКО
(підпис) *(ім'я, прізвище)*
"____" _____ 2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач **ДЄДІЩЕВ Денис** допускається до захисту даної кваліфікаційної роботи в Екзаменаційній комісії.

Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

_____ Галина ГАЙДУР
(підпис) *(ім'я, прізвище)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 46 сторінки, 46 рисунків, 2 таблиці, 12 джерел.

Об'єкт дослідження – шкідливе програмне забезпечення.

Предмет дослідження – методи та засоби аналізу шкідливого програмного забезпечення та подальше використання його результатів для реагування на кібінцидент у контексті Check Point NGFW.

Мета роботи – дослідити процес аналізу шкідливого програмного забезпечення для отримання результатів на основі яких виконується реагування на кіберінциденти за допомогою рішення Check Point NGFW.

Методи дослідження –інструменти для ручного та автоматичного аналізу шкідливого програмного забезпечення, використання Check Point NGFW для блокування виявлених IoC`s.

Рішення Next-Generation Firewall (NGFW) виконує ключову роль у захисті периметра мережі організації. NGFW забезпечує видимість мережевої активності кінцевих точок у реальному часі, що дозволяє організаціям швидко реагувати на кіберінциденти.

В роботі досліджено проблему аналізу шкідливого програмного забезпечення, визначено його мету та завдання. Проведено аналіз існуючих методів та засобів аналізу шкідливого програмного забезпечення. Досліджено методи та засоби використання результатів аналізу ШПЗ для подальшого реагування на кіберінцидент на базі Check Point NGFW.

На основі досліджень проведених в роботі запропоновано методи аналізу шкідливого програмного забезпечення на базі відкритого програмного забезпечення та Sandbox. Розроблено рекомендації фахівцям з кібербезпеки щодо реалізації отриманих результатів аналізу ШПЗ.

Галузь використання – кібербезпека інформаційних ресурсів організації.

АНАЛІЗ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, SANDBOX, CHECK POINT NGFW, КІБЕРІНЦИДЕНТ

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

NGFW – Next-Generation Firewall

SIEM – Security Information and Event Monitoring

Host – хост (будь-який пристрій або комп'ютерна система, яка має унікальну IP-адресу і може бути доступною у мережі)

ШПЗ – Шкідливе програмне забезпечення

ПЗ – Програмне забезпечення

SEG – Security Management Gateway

MSG – Mail Security Gateway

Sandbox – Пісочниця (система ізоляції для виконання та аналізування небезпечного програмного забезпечення)

IoC`s – Indicators of Compromise

SMS – Security Management Server

http – Hypertext Transfer Protocol

SMB – Server Message Block

ВСТУП

Актуальність дослідження. Шкідливе програмне забезпечення є одною з головних загроз інформаційній безпеці організаціям, установам та звичайним користувачам. З метою отримання несанкціонованого доступу до інформаційних систем, зловмисники постійно виконують спроби поширення шкідливого програмного забезпечення, через це, розуміння які саме алгоритми дій виконує певне ШПЗ та здобуття його індикаторів компрометації є одним з найважливіших задач у підтримці інформаційної безпеки, оскільки поширення даної інформації та внесення її до відповідних баз даних суттєво збільшує вірогідність успішного відбиття та реагуванню на зловмисну активність ШПЗ. Наразі, в світі створено команди CERT для поширення важливої інформації про кіберінциденти та платформи MISP для поширення виявлених IoC`s, більшість з яких пов’язана з ШПЗ.

Аналіз шкідливого програмного забезпечення надає змогу отримати розуміння алгоритму дій певного ШПЗ та видобути IoC`s, які після отримання необхідно занести до чорних списків мережевого обладнання та антивірусного захисту для уникнення можливості повторної активності даного ШПЗ в захищеній мережі.

Хоча процедура аналізу ШПЗ може бути безкоштовна, дане рішення підходить скоріше для середніх та великих організацій та установ в яких наявний Security Operation Center (SOC), оскільки дана процедура націлена насамперед на непоширені зразки ШПЗ, в таких випадках аналізом ШПЗ буде займатись відповідний спеціаліст з кіберзахисту, який також матиме можливість перевірити чи наявна подібна активність у відповідній мережі за допомогою рішення типу SIEM, у випадку поширеного ШПЗ, інформацію про його загрозу та алгоритм дій повідомляють відповідні CERT та його IoC`s будуть поширюватись за допомогою платформ типу MISP, в той час як невеликі організації та установи рідше будуть зустрічатись з цілеспрямованою атакою за допомогою ШПЗ, отже результати аналізу з інших джерел має покрити основні потреби підтримки інформаційної

безпеки відповідних організацій та установ.

Рішення NGFW виконує ключову роль у захисті периметра мереж організацій та установ, що в свою чергу забезпечує видимість мережевої активності кінцевих точок у реальному часі, це дозволяє спеціалістам з кіберзахисту швидко реагувати на кіберінциденти.

Вищесказане визначає актуальність теми даної кваліфікаційної роботи, основний зміст якої становлять дослідження процедури аналізу шкідливого програмного забезпечення та використання результатів даного аналізу для реагування на кіберінциденти за допомогою рішення Check Point NGFW.

Об'єкт дослідження – шкідливе програмне забезпечення.

Предмет дослідження – методи та засоби аналізу шкідливого програмного забезпечення та подальше використання його результатів для реагування на кібінцидент у контексті Check Point NGFW.

Мета роботи – дослідити процес аналізу шкідливого програмного забезпечення для отримання результатів на основі яких виконується реагування на кіберінцидента зи допомогою рішення Check Point NGFW.

Наукові завдання:

дослідити процедуру аналізу шкідливого програмного забезпечення;

проаналізувати ШПЗ на прикладі одного з кіберінцидентів;

проаналізувати результати виконаного аналізу ШПЗ;

розглянути рішення Check Point NGFW;

розробити рекомендацій щодо застосування результатів аналізу ШПЗ для реагування на кіберінциденти.

Методи дослідження – дослідити інструменти для ручного та автоматичного аналізу шкідливого програмного забезпечення, використання Check Point NGFW для блокування виявлених IoC`s.

Практичне значення одержаних результатів: розроблено рекомендації щодо застосування результатів аналізу ШПЗ для реагування на кіберінциденти.

1 АНАЛІЗ ІСНУЮЧИХ ТИПІВ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ЇХ ВПЛИВ НА ОРГАНІЗАЦІЇ

1.1. Аналіз існуючих типів шкідливого програмного забезпечення

Шкідливе програмне забезпечення (malware) - це програми, які прикріплюються до інших файлів та можуть пошкоджувати, копіювати або змінювати дані на комп'ютері користувача без його згоди. Віруси можуть швидко поширюватись через файлові системи та мережеве середовище.

Існує величезна кількість варіацій та модифікацій різного шкідливого програмного забезпечення, але з них можна виділити одинадцять основних типів, а саме:

1) Virus (Віруси) – є одними з найдавніших та найпоширеніших форм шкідливого програмного забезпечення. Вони вбудовуються в інші файли або програми та можуть руйнувати, модифікувати або викрадати дані на комп'ютері користувача.

Віруси добре відомі своєю здатністю поширюватись швидко через інфіковані файли та електронні листи. Вони можуть призвести до серйозних втрат даних та порушень безпеки, якщо їх не виявити та не нейтралізувати вчасно.

Наприклад, вірус Melissa, який з'явився у 1999 році, поширювався через електронну пошту та заражав документи Microsoft Word, спричинивши великі збитки для багатьох компаній.

2) Worms (Черв'яки) – розповсюджуються самостійно через мережі, використовуючи вразливості у мережевих протоколах або програмному забезпеченні.

Черв'яки можуть швидко поширювати інфекції через комп'ютерні мережі, збільшуючи ризик масштабних атак та порушень безпеки. Вони можуть призвести до великих збитків і втрат даних, якщо не прийняті відповідні заходи безпеки.

Яскравий приклад - черв'як WannaCry, який у 2017 році спричинив масштабну кібератаку, вразивши сотні тисяч комп'ютерів по всьому світу.

3) Trojan (Троянські коні) – приховано встановлюються на комп'ютерах користувачів під виглядом безпечних або корисних програм. Вони виконують шкідливі дії без відома користувача.

Троянські коні можуть використовуватися для викрадення особистої інформації, створення "задніх дверей" для нелегального доступу до системи, а також для встановлення додаткового шкідливого програмного забезпечення.

Наприклад, троян Zeus використовувався для крадіжки банківських даних, завдавши фінансових втрат багатьом користувачам та організаціям.

4) Spyware (Шпигунське ПЗ) – використовується для збору конфіденційної інформації про користувачів без їх згоди або знання.

Шпигунське програмне забезпечення може використовуватися для викрадення паролів, банківських даних, особистих повідомлень та інших конфіденційних даних. Це створює серйозну загрозу для приватності користувачів та безпеки їх інформації.

Наприклад, програма SpyEye була широко використовувана для збору конфіденційних даних з комп'ютерів користувачів. SpyEye здобула популярність серед зловмисників завдяки своїй здатності красти інформацію про банківські рахунки, логіни, паролі та інші важливі дані. Ця шкідлива програма могла інфікувати комп'ютери через фішингові електронні листи або заражені веб-сайти, після чого вона працювала у фоновому режимі, збираючи та передаючи зловмисникам зібрані дані. SpyEye часто використовувалася у поєднанні з іншими типами шкідливого ПЗ, що робило її ще більш небезпечною та ефективною у викраденні конфіденційної інформації.

5) Adware (Рекламне ПЗ) – відображає нав'язливу рекламу на комп'ютерах користувачів з метою генерації прибутку для авторів.

Рекламне програмне забезпечення не завдає прямих шкідливих дій, але може призводити до дратівливості для користувачів та зниження продуктивності системи через нав'язливу рекламу. Крім того, деякі форми рекламного ПЗ можуть

також відстежувати поведінку користувачів та збирати їх особисті дані для маркетингових цілей.

Прикладом є програмне забезпечення Fireball, яка поширювалася через безкоштовні програми і відображала рекламу на комп'ютерах користувачів.

6) Ransomware (Програма-вимагач) – шифрує файли на комп'ютері користувача та вимагає викуп за їх розшифрування.

Програма-вимагач може призвести до серйозних втрат даних та фінансових втрат для користувачів та організацій. Ця форма атаки стає все більш поширеною та вишуканою, і вона вимагає відповідного заходу захисту та резервного копіювання даних.

Один з найвідоміших прикладів - шкідливе ПЗ NotPetya, яке в 2017 році спричинило великі збитки багатьом організаціям по всьому світу. Це ПЗ поширилося шляхом використання вразливостей у програмному забезпеченні та завдало шкоди компаніям у багатьох галузях, включаючи банківський, транспортний і енергетичний сектори. NotPetya призвело до тимчасової недоступності комп'ютерних систем, видалення або пошкодження даних та значних фінансових втрат для постраждалих компаній. [1]

7) Rootkits (Прихована-програма) – шкідливе програмне забезпечення, яке приховує свою присутність на комп'ютері шляхом модифікації операційної системи або інших системних компонентів.

Дане шкідливе програмне забезпечення може використовуватися для незаконного доступу до системи або для прихованого збору інформації. Вони можуть бути особливо небезпечними через їх вміння приховуватись від виявлення антивірусними програмами та іншими засобами безпеки.

Одним з найвідоміших прикладів rootkit є Stuxnet, який був використаний для атаки на промислові системи в Ірані. Stuxnet був виявлений у 2010 році і став першим відомим шкідливим програмним забезпеченням, яке було спеціально розроблено для саботажу промислових систем. Його метою були центрифуги, що використовуються для збагачення урану в іранських ядерних установках. Stuxnet був здатний приховано проникати в комп'ютерні системи, що контролюють ці

центрифуги, і змінювати їхню роботу, змушуючи їх працювати на небезпечних швидкостях, що призводило до їх поломки. Водночас, Stuxnet обманював операторів, показуючи нормальні показники роботи систем. [2]

8) Keyloggers (Журналювання клавіш) – записує натискання клавіш користувача на клавіатурі без їх знання. Це може включати паролі, особисті повідомлення та іншу конфіденційну інформацію.

Журналювання клавіш може бути використано для крадіжки особистих даних та ідентифікаційної інформації. Вони становлять серйозну загрозу приватності користувачів та безпеці їх особистих даних.

Наприклад, Keylogger Ardamax працює у фоновому режимі, фіксуючи кожне натискання клавіші та зберігаючи ці дані у прихованих файлах. Ardamax може також робити скріншоти екрану, записувати звукові розмови через мікрофон та навіть відслідковувати активність у веб-браузері.

9) Botnets (Мережа ботів) – мережи комп'ютерів, які контролюються з віддаленої локації і використовуються для виконання шкідливих дій, таких як розсилка спаму, атаки з відмовою в обслуговуванні (DDoS) та інші.

Мережу ботів можуть використовувати для масштабних атак та викликати серйозні перебої у роботі мереж та веб-сайтів. Вони представляють значну загрозу для інтернет-інфраструктури та безпеки даних.

Прикладом є ботнет Mirai, який у 2016 році здійснив масштабні DDoS-атаки на різні сервіси по всьому світу. Mirai інфікував пристрої Інтернету речей (IoT), такі як камери спостереження та домашні маршрутизатори, перетворюючи їх на заражені хости, які могли бути використані для здійснення атак. Однією з найвідоміших атак ботнету Mirai стала атака на провайдера DNS Dyn у жовтні 2016 року, яка призвела до недоступності таких популярних сайтів, як Twitter, GitHub, Netflix та Spotify. Ця атака продемонструвала, наскільки вразливими можуть бути IoT-пристрої та які серйозні наслідки можуть мати DDoS-атаки, якщо їх здійснювати з використанням великої кількості інфікованих пристроїв. Після атак вихідний код Mirai був опублікований у відкритому доступі, що призвело до

створення численних варіацій цього ботнету і збільшення кількості атак з його використанням.[3]

10) Phishing (Фішинг) – форма шахрайства в інтернеті, при якій зловмисники намагаються отримати конфіденційну інформацію, таку як паролі, номери кредитних карток та інші особисті дані, шляхом використання підроблених веб-сайтів, електронних листів або інших засобів комунікації.

Фішинг може набувати різних форм і методів, включаючи спам-електронні листи, підроблені веб-сайти, повідомлення в соціальних мережах та навіть додатки для спілкування. Ці атаки можуть бути спрямовані на широку аудиторію або на конкретні цілі, і вони можуть мати серйозні наслідки для безпеки та конфіденційності інформації користувачів.

Наприклад, кампанія фішингових листів, що імітують банки, може призвести до викрадення банківських даних багатьох користувачів. Так, у травні 2017 року стався відомий фішинговий інцидент "Google Docs Phishing Scam", коли зловмисники відправляли електронні листи, які маскувалися як запрошення до спільного доступу до документів Google Docs. У листі було вказано, що користувач був запрошений до документу Google Docs, і було надано посилання для доступу до нього. Проте посилання веділо на підроблений веб-сайт, де зловмисники просили надати доступ до облікового запису Google. Після введення логіну та пароля зловмисники могли отримати повний доступ до облікового запису користувача, включаючи електронну пошту, документи та інші приватні дані. [4]

11) Zero-Day Exploits (Атака нульового дня) – використання вразливості в програмах або операційних системах, які тільки що були виявлені та які не мають оновлень або виправлень.

Наприклад, експлоіт EternalBlue, виявлений у 2017 році, був використаний для поширення черв'яків WannaCry та NotPetya. Цей експлоіт використовував вразливості у протоколі SMB (Server Message Block), що дозволило зловмисникам віддалено виконувати код на комп'ютерах з підтримкою Windows, що привело до масштабного поширення шкідливого програмного забезпечення та значних втрат для користувачів та організацій.[5]

1.2 Аналіз загроз, які несуть шкідливі програмні забезпечення для організацій

У сучасному цифровому середовищі організації стикаються зі значними викликами в області кібербезпеки через поширення шкідливого програмного забезпечення (ШПЗ) та чисельні атаки зловмисниками. Це проблема, яка стає все більш актуальною через зростання кількості та складності атак, які впливають на бізнес-процеси, інформаційні ресурси та репутацію організацій. У цьому розділі розглянемо основні типи загроз, які несе ШПЗ для організацій та їх можливі впливи.

1) Фінансові втрати – ШПЗ може призвести до серйозних фінансових втрат для організацій. Наприклад, DDoS-атаки можуть перевантажити мережу організації, призводячи до припинення доступу до веб-сайту або онлайн-сервісів, що в свою чергу унеможливлює продовження бізнес процесу на період недоступності серверів, що призводить до фінансових втрат. Також чисельні випадки атак ransomware, що шифрують важливі дані організації та вимагають викуп за їх розшифрування, інколи організації дешевше заплатити викуп за ключи для розшифрування даних ніж намагатись відновити їх іншим шляхом або втрати їх назовсім.

Крім того, шкідливе програмне забезпечення може використовуватися для крадіжки фінансової інформації, такої як банківські реквізити або паспортні дані, що може призвести до фінансових втрат та шахрайства.

2) Втрати даних – Атаки з використанням ШПЗ можуть призвести до втрати важливої інформації для організацій. Це може включати втрату конфіденційних даних клієнтів, внутрішніх документів та інших важливих ресурсів. Наприклад, при знищенні даних на серверах де зберігається база даних клієнтів у випадку, якщо немає можливості їх відновити завдяки резервного копіювання це завдасть значної шкоди для просування цієї організації на ринку з яким вона працює. Втрати даних можуть мати серйозні наслідки для репутації організації та її можливостей продовження діяльності.

3) Порушення конфіденційності – ШПЗ може порушити конфіденційність працівників, клієнтів та організацій в цілому шляхом збирання та використання інформації без наданої на це згоди. Наприклад, шпигунське програмне забезпечення може відслідковувати активність працівників певної організації в Інтернеті, перехоплюючи особисті повідомлення та викрадаючи конфіденційні дані, зазвичай при порушенні конфіденційності найбільше всього завдається шкоди репутації організації після чого йдуть неминучі фінансові збитки.

4) Втрата доступу до систем – Деякі типи ШПЗ можуть призвести до втрати доступу до систем та інформаційних ресурсів організації. Наприклад, атаки ransomware можуть призвести до шифрування важливих даних організації та вимагати викуп за їх розшифрування, в світі вже бували випадки шифрування даних обладнання в медичних структурах, що в свою чергу унеможливлювало їх роботу через що створювалась загроза життю та здоров'ю пацієнтів цих закладів. Інший приклад, при знищенні шкідливим програмним забезпеченням даних серверів, які відповідають за роботу мобільних операторів можливо паралізувати зв'язок між мільйонами користувачів даного оператора та створити іншим мобільним операторам більшу завантаженість.

Шкідливе програмне забезпечення є великою загрозою для організацій у всьому світі. Аналіз, проведений в цьому розділі, підтверджує, що воно призводить до різних видів шкоди, включаючи фінансові втрати, втрату важливих даних, порушення конфіденційності та втрату доступу до систем. Фінансові втрати можуть бути великими через атаки типу DDoS або шифрування даних ransomware. Втрати даних можуть призвести до серйозної втрати інформації, що є життєво важливою для діяльності організації. Порушення конфіденційності можуть спричинити проблеми з репутацією та втратою довіри клієнтів. Втрата доступу до систем може паралізувати бізнес-процеси. Отже, для захисту від цих загроз необхідно розробляти та впроваджувати ефективні стратегії та заходи безпеки в рамках інформаційних систем організацій.

2 МЕТОДИ ТА ЗАСОБИ АНАЛІЗУ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

2.1 Методи та інструменти ручного аналізу шкідливого програмного забезпечення

1) Wireshark – це програма для аналізу мережі, яка дозволяє перехоплювати та аналізувати мережевий трафік в реальному часі. Користувачі можуть використовувати Wireshark для виявлення проблем з мережевим з'єднанням, аналізу протоколів мережі, усуненню мережевих проблем, тощо. Дана програма підтримує багато протоколів мережі, таких як TCP, UDP, IP, HTTP, FTP, DNS, SNMP, тощо, що в свою чергу дозволяє аналізувати трафік в повному об’ємі.

2) Sysinternals – це набір утиліт для адміністрування та діагностики операційних систем Windows, вони дозволяють виконувати різні завдання, такі як моніторинг системи, керування процесами та службами, аналіз файлової системи та реєстру, і багато іншого. Деякі з найвідоміших утиліт Sysinternals включають Process Explorer, Autoruns, Process Monitor, TCPView , Disk Usage (DU), тощо. Для аналізу шкідливого програмного забезпечення зазвичай використовується лише три з них, а саме:

TCPView – це утиліта, яка дозволяє переглядати активні з'єднання TCP та UDP на комп'ютері. Вона надає детальну інформацію про всі активні мережеві з'єднання, включаючи порти, IP-адреси, статус з'єднання, об’єм трафіку та дані, які передаються, наприклад при відкритті певного веб-ресурсу та перегляду на ньому медіа в TCPView будуть дані про дане медіа та веб-ресурс, але зазвичай в зашифрованому виді, в залежності від протоколів з’єднання. TCPView допомагає адміністраторам мережі виявляти та аналізувати активний мережевий трафік для виявлення потенційних проблем або загроз безпеці.

Autoruns – це утиліта для перегляду та керування автозапуском програм та служб у операційній системі Windows. Вона відображає всі точки автозапуску, такі

як реєстраційні ключі, папки автозапуску, послуги Windows, тощо. Autoruns дозволяє користувачам відключати або видаляти непотрібні або потенційно небезпечні точки автозапуску, що може допомогти зберегти швидкість та безпеку системи. Зазвичай, при проведенні аналізу шкідливого програмного забезпечення, Autoruns використовується, щоб виявити нові процеси, які додались до автозапуску, наприклад ШПЗ типу Adware або Trojan можуть самостійно створювати точки автозапуску без відома користувача, щоб при кожному запуску операційної системи виконувати свої функції, тобто для того щоб закріпитись в ній.

Process Explorer – це детальний менеджер завдань для операційних систем Windows, який надає більше інформації, ніж стандартний диспетчер завдань. Він дозволяє переглядати всі активні процеси та їх характеристики, включаючи взаємозв'язки між процесами, використання пам'яті, обробку файлів, тощо. Process Explorer допомагає виявляти та аналізувати потенційно шкідливі процеси, які можуть бути запущені в певній операційній системі.

3) HashMyFiles – це утиліта для операційних систем Windows, яка дозволяє обчислити хеш-суму для одного чи декількох файлів одночасно. Хеш-сума - це унікальний числовий ідентифікатор, який генерується з вмісту файлу за допомогою певного алгоритму. Це дає можливість перевірити цілісність файлів, порівняти їхні хеш-суми та виявити будь-які зміни. В рамках аналізу шкідливого програмного забезпечення, HashMyFiles використовується для отриманні індикаторів, а саме хеш-суми файлів зі шкідливим програмним забезпеченням, які після потрібно буде заносити до чорних списків на блокування. Також, у випадку, коли певний файл зі ШПЗ вже був відомий, тобто виробники антивірусного захисту вже з ним стикалися, за допомогою його хеш-суми можна знайти інформацію про нього за допомогою репутаційних баз даних, такі як: X-Force, Virus Total, Hybrid Analysis, тощо.

2.2 Інструменти для автоматичного аналізу шкідливого програмного забезпечення

Серед інструментів автоматичного аналізу шкідливого програмного забезпечення найбільш комплексним та зручним методом є використання спеціально створених для цього Sandbox`s.

Sandbox – це ізольоване середовище з мінімальними привілеями та обмеженим доступом, зазвичай розгорнуто в віртуальному середовищі, яке використовують для виконання програм або процесів, з точки зору інформаційної безпеки, дане рішення використовують для аналізу шкідливого програмного забезпечення, наприклад коли на корпоративну пошту надходить лист, відбувається його перевірка на наявність різних шкідливих додатків шляхом відкриття в Sandbox даних листів та їх вкладень з перевіркою антивірусними засобами захисту, перед тим як відправити лист далі, до вказаного одержувача даного листа.

Sandbox, як правило, буває у двох варіантах, тонкий клієнт та товстий клієнт, зазвичай, коли мова йде про тонкий клієнт мається на увазі веб-ресурси, які безкоштовно дають змогу завантажити файли до певного розміру до своїх Sandbox, мінусом даного рішення є можливість перегляду зразків, які були завантажені для аналізу іншими користувачами, нерідко серед файлів, що завантажувались, зустрічались файли з конфіденційною або чутливою інформацією, які були випадково завантажені для перевірки на наявність вірусів, цим часто користувались зловмисники, зараз існує цілий напрям де за допомогою налаштованих ботів, зловмисник перевіряє завантажені файли на відомих веб-ресурсах для Sandbox та у випадку виявлення певного шаблону важливої інформації – завантажує зразок файлу на сервер зловмисника.

Серед найбільш популярних, ефективних та безкоштовних Sandbox для аналізу файлів зі шкідливим програмним забезпеченням є:

1) Virus Total – найбільш відома репутаційна база для перевірки різноманітних індикаторів від IP-адрес до назв файлів, яка збирає дані більш ніж з

80 різних вендорів, які займаються антивірусним захистом. Надає можливість без реєстрації завантажити файл розміром до 650 MB. З недоліків варто відмітити, що хоча перевірка індикаторів доступна усім, але зразки завантажених файлів доступні лише з преміум підпискою. Також, при завантажені файлу немає можливості обирати необхідні налаштування такі як версія та тип операційної системи, час перевірки, тощо. На Рис.1.1 можна побачити загальний інтерфейс даного Sandbox.

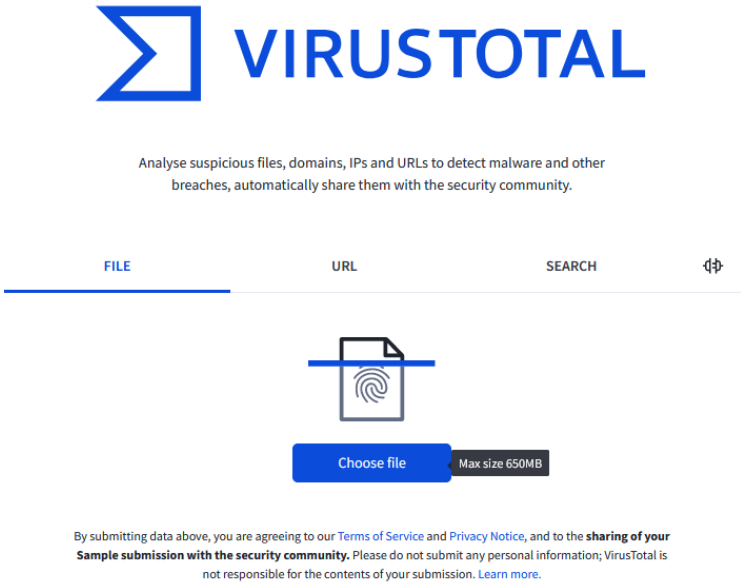


Рис. 2.1. Sandbox – Virus Total

2) Hybrid Analysis – один з найпопулярніших Sandbox, хоча репутаційна база індикаторів значно менше ніж у Virus Total, проте дане рішення дає змогу обрати тип операційної системи, аналіз завантаженого файлу виконується повністю в автоматизованому режимі та його тривалість складає 5 хвилин. Максимальний розмір для безкоштовного завантаження складає 100 MB. На рис.2.2 можна побачити загальний інтерфейс даного Sandbox.

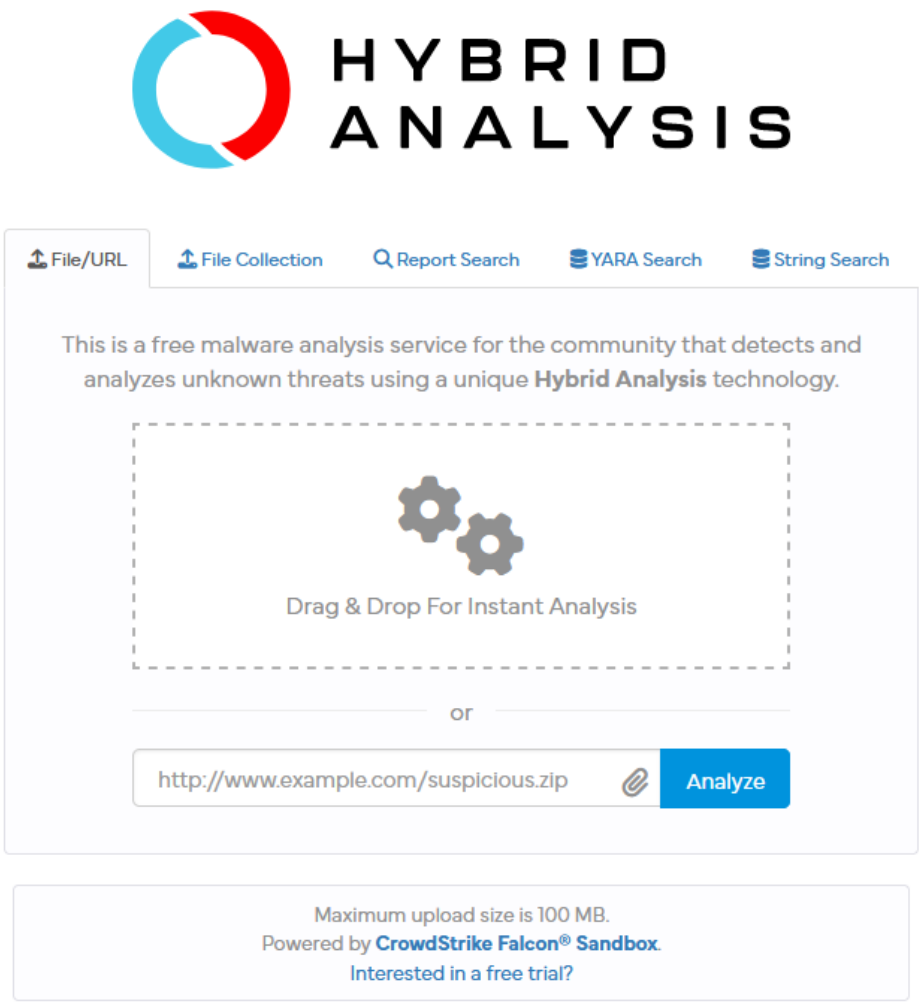


Рис. 2.2. Sandbox – Hybrid Analysis

3) Triage – найбільш варіативний для налаштування та взаємодії з звантаженими файлами до даного Sandbox з наведеного списку. Даний веб-ресурс дозволяє обрати тип операційної системи, мову операційної системи, типу інтернет доступу, браузер, час аналізу, також він дозволяє інтерактивний доступ до віртуальної машини на якій виконується аналіз файлу. Усі зразки завантажених файлів доступні в публічному просторі безкоштовно. Максимальний розмір для безкоштовного завантаження складає 100 MB. На рис.2.3 можна побачити загальний інтерфейс даного Sandbox.

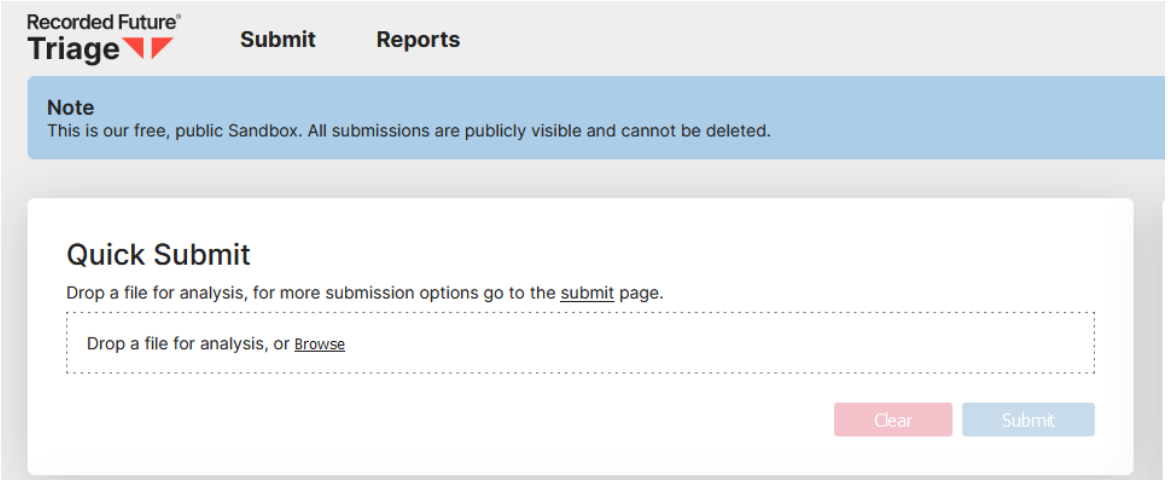


Рис. 2.3. Sandbox – Triage

4) Valkyrie – з переваг в порівнянні з іншими Sandbox в даному списку є можливість автоматичного формування звіту та співставлення усіх виявлених дій шкідливого програмного забезпечення з матрицею MITRE ATT&CK. Максимальний розмір для безкоштовного завантаження складає 150 MB. На рис. 1.4 можна побачити загальний інтерфейс даного Sandbox.

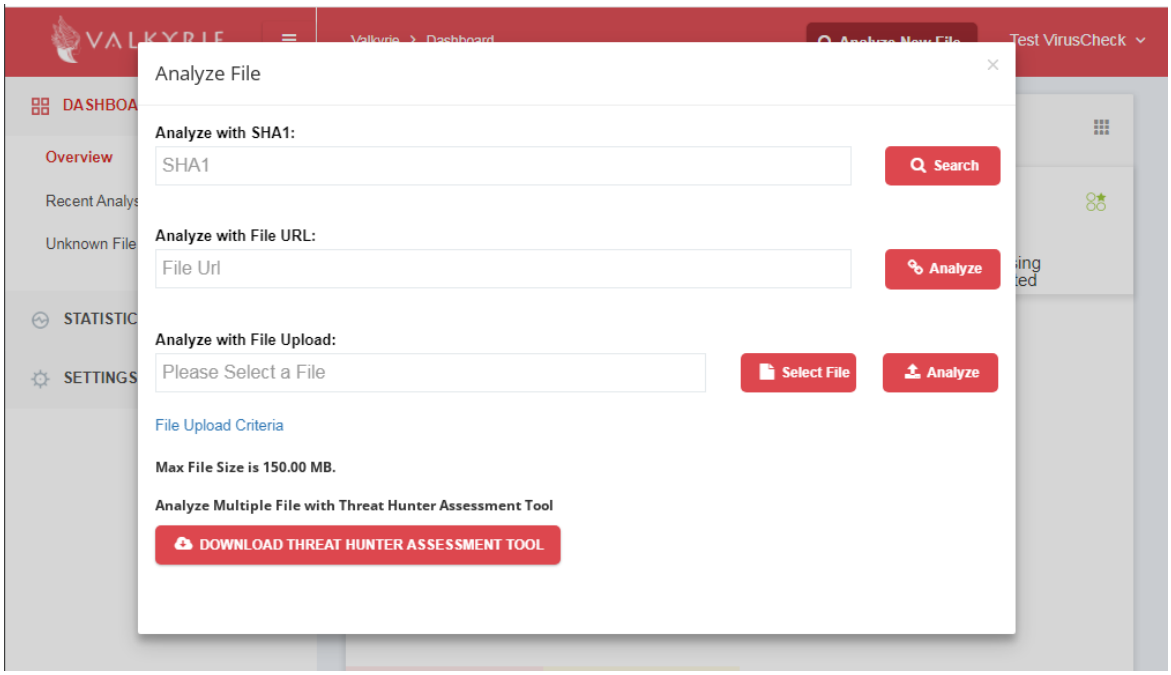


Рис. 2.4. Sandbox – Valkyrie

Також існує багато інших Sandbox`s від всесвітньо відомих вендорів таких як Fortinet, Cisco, Check Point, Symantec, тощо. Зазвичай технологія Sandbox використовується даними вендорами в рішеннях типу SEG/MSG для аналізу

поштових повідомлень.

2.3. Приклад аналізу шкідливого програмного забезпечення на основі зразка з кіберінциденту "Повістка до суду" – CERT-UA#8150

В якості наглядного прикладу для аналізу шкідливого програмного забезпечення було обрано зразок з реального кіберінциденту "Повістка до суду" – CERT-UA#8150, яке вперше відбулося 29.11.2023, причиною даного кіберінциденту стала компрометація облікових записів одного з органів судової влади України зловмисниками.

Суть даного інциденту полягає в тому, що за допомогою скомпрометованих облікових записів було надіслано більше ніж 15 000 електронних листів різним організаціям та установам України, які містили у вкладенні архів:

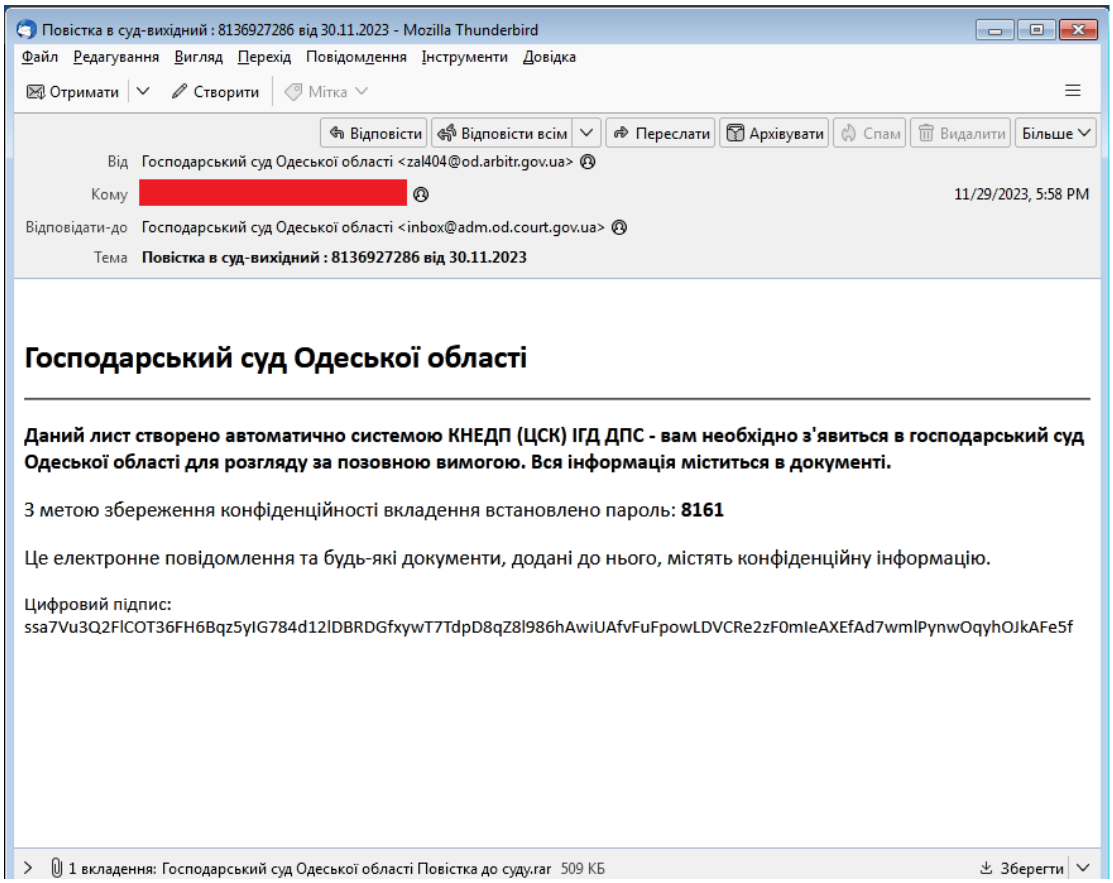


Рис. 2.5. Приклад надісланого електронного листа

Оскільки дані електронні листи, приклад якого можна побачити на рис. 2.5,

прийшли від поштових скриньок з легітимним доменом gov[.]ua та мали цифровий підпис – більшість систем захисту та спам фільтрів пропустили дані листи далі до вказаних отримувачів, оскільки сам архів був з паролем, у рішень типу SEG/MSG не було можливості проаналізувати файли, які знаходились в архіві. Варто зазначити, що у більшості державних установ та організацій, налаштованими політиками фільтрації електронних листів не було перенаправлення електронних листів з вкладенням, яке неможливо проаналізувати, а саме архівів з паролем у вкладенні електронних листів до карантину, що в свою чергу також сприяло отримання даних листів вказаними отримувачами.

Пароль до архіву був вказаний в електронному листі, в даному випадку 8161. При відкритті даного архіву за допомогою вказаного паролю було отримано файл формату .doc, який можна побачити на рис. 2.6:

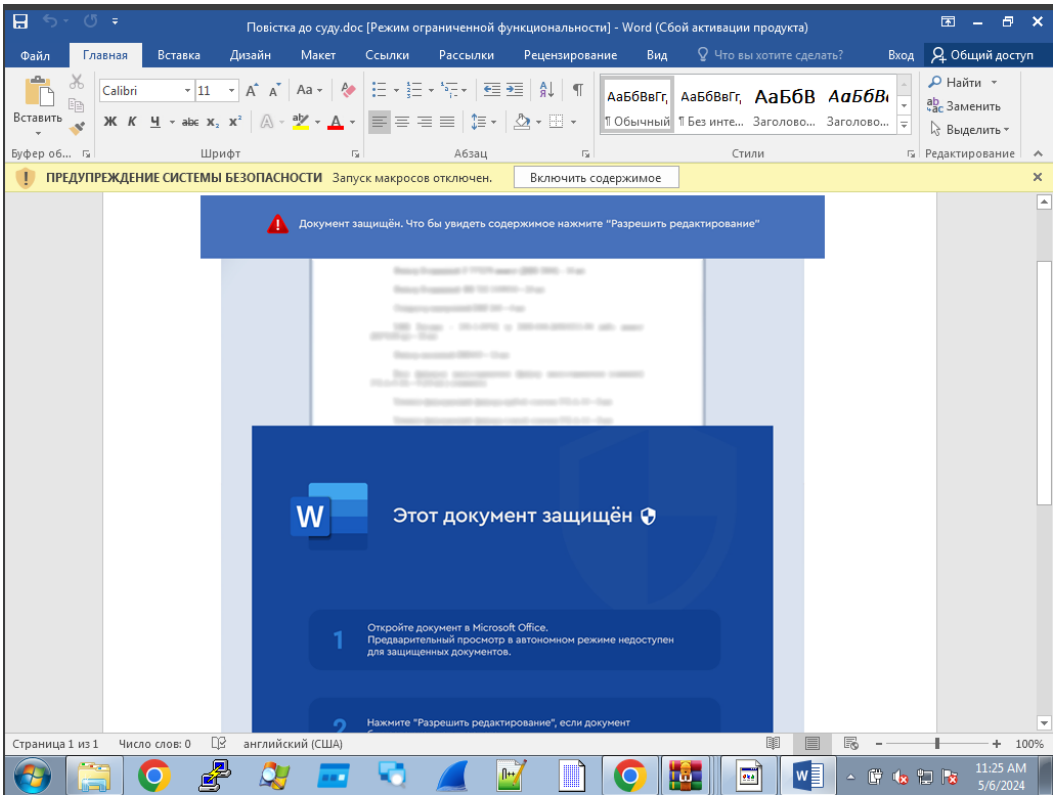


Рис. 2.6. Приклад відкритого документу в форматі .doc

В даному документі додано скріншот з текстом, який просить користувача натиснути на кнопку для включення змісту під видом вимоги захищеності даного змісту, що вводить в оману користувача, який відкрив даний документ, далі все

залежить від уважності користувача, наприклад уже зараз, можна побачити, що на жовтій стрічці вказано “Запуск макросів вимкнено” дане повідомлення має застерегти користувача, у випадку, якщо він пройшов курси з кібергігієни, якщо діяти згідно інструкцій наведених на скріншоті вище та перейти до вкладки “Відомості”, на рис. 2.7 можна побачити більш детальний опис даного застереження:

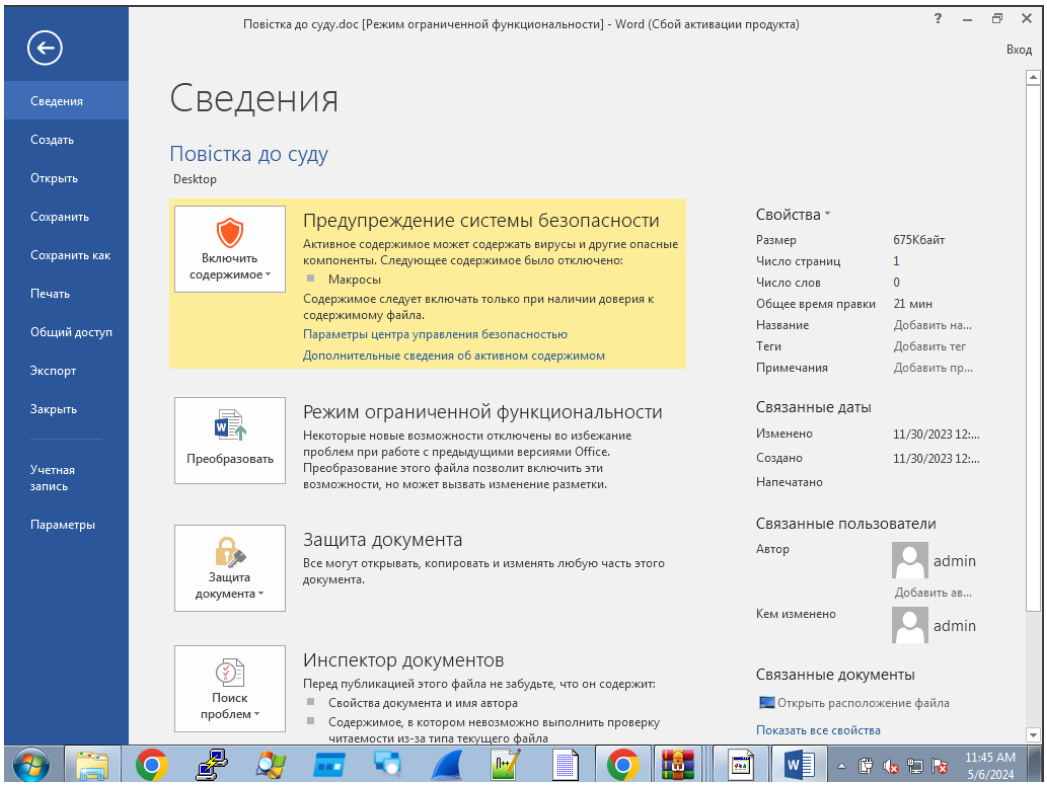


Рис. 2.7. Вкладка “Відомості” про відкритий документ формату .doc

Якщо користувач не помітить застереження або все одно натисне на кнопку “Включити вміст” відбудеться активація макросу та почнется комунікація з хосту на якому відкрили даний файл до зловмисного ресурсу, по протоколу SMB, в фоновому режимі з метою завантаження та запуску файлу "scandoc.exe", який в свою чергу зазначений виконуваний файл є обфускованою за допомогою SmartAssembly .NET-програмою, призначенням якої є дешифрування та запуск програми для віддаленого управління RemcosRAT. [6]

При взаємодії з зразком в ході аналізу шкідливого програмного забезпечення усі дії необхідно виконувати в лабораторних умовах, а саме в ізольованому віртуальному середовищі, для уникнення зараження основного хосту.

Зазвичай, спочатку виконується ручний аналіз, головною метою якого зрозуміти, які дії має виконати звичайний користувач щоб запустити дане ШПЗ, зібрати наглядні підтверджуючи докази виконання зловмисних дій та за можливістю визначити алгоритм дій даного ШПЗ.

Перед запуском файлу з шкідливим змістом, виконується запуск наступного програмного забезпечення:

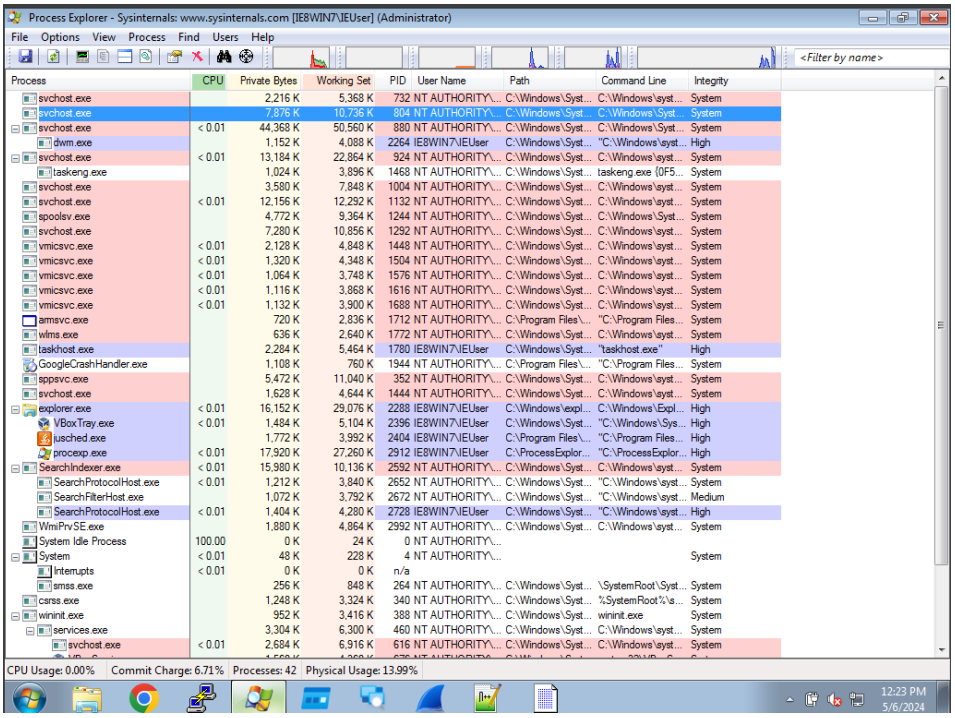


Рис. 2.8. Відкритий Sysinternals – Process Explorer

Запуск “Process Explorer”, який можна побачити на рис 2.8, необхідний для виявлення нових процесів, які будуть утворюватися під час та після запуску ШПЗ.

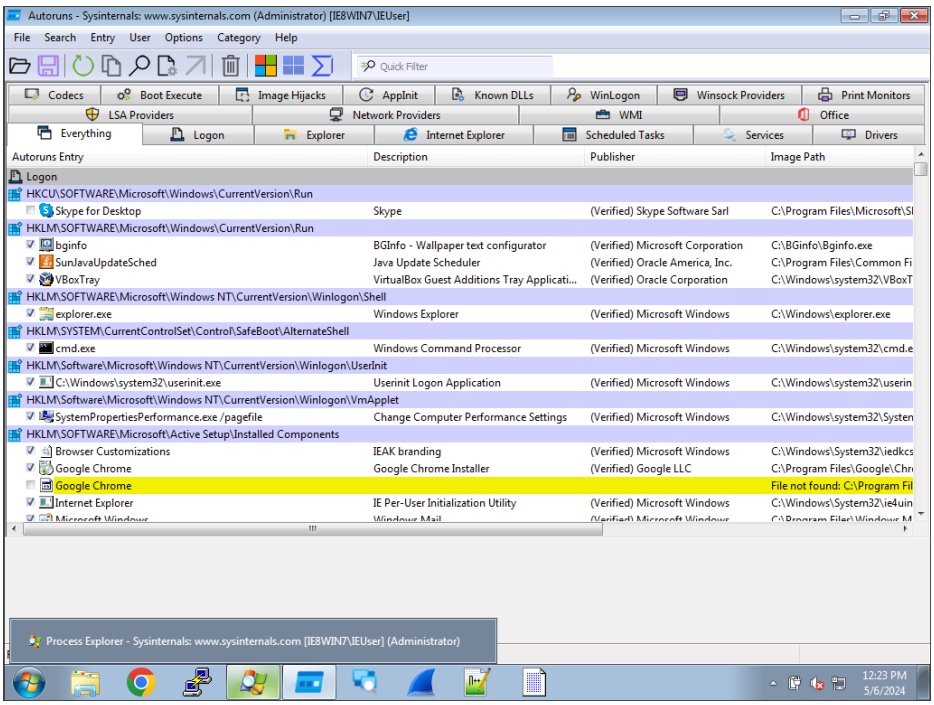


Рис. 2.9. Відкритий Sysinternals – Autorans

Запуск “Autorans”, який можна побачити на рис 2.9, необхідний для виявлення нових точок автозапуску, які будуть утворюватися під час та після запуску ШПЗ.

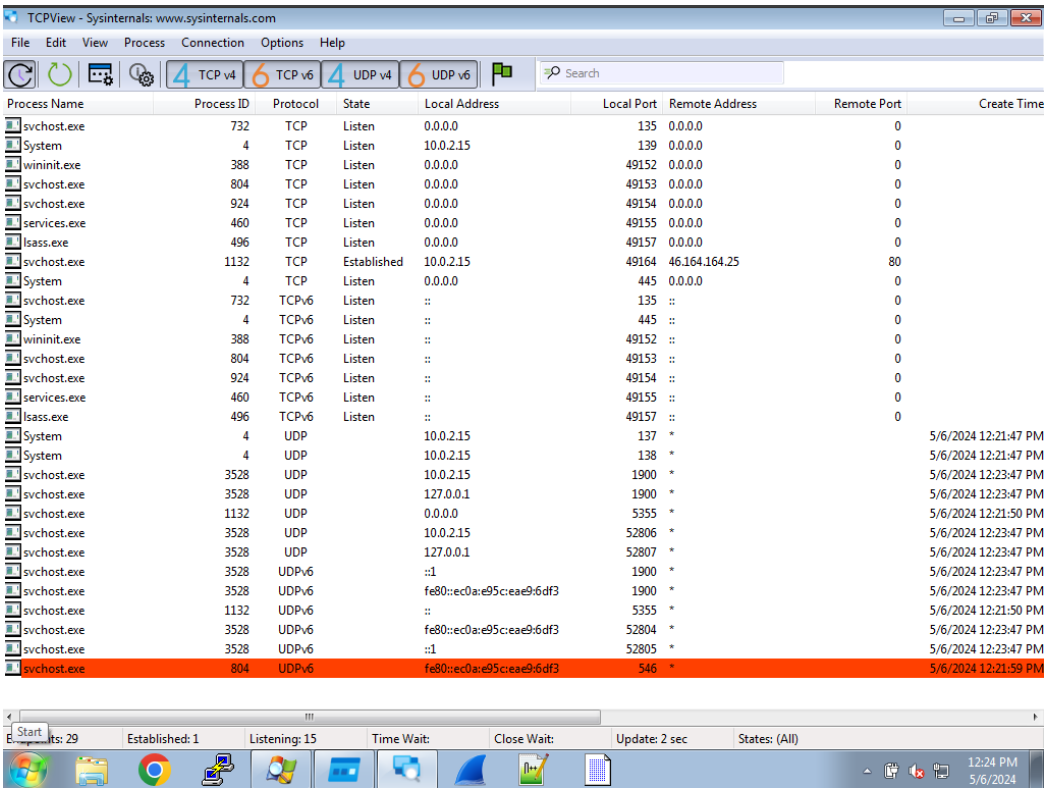


Рис. 2.10. Відкритий Sysinternals – TCPView

Запуск “TCPView”, який можна побачити на рис 2.10, необхідний для виявлення нових TCP-з’єднань, які будуть утворюватися під час та після запуску ШПЗ.

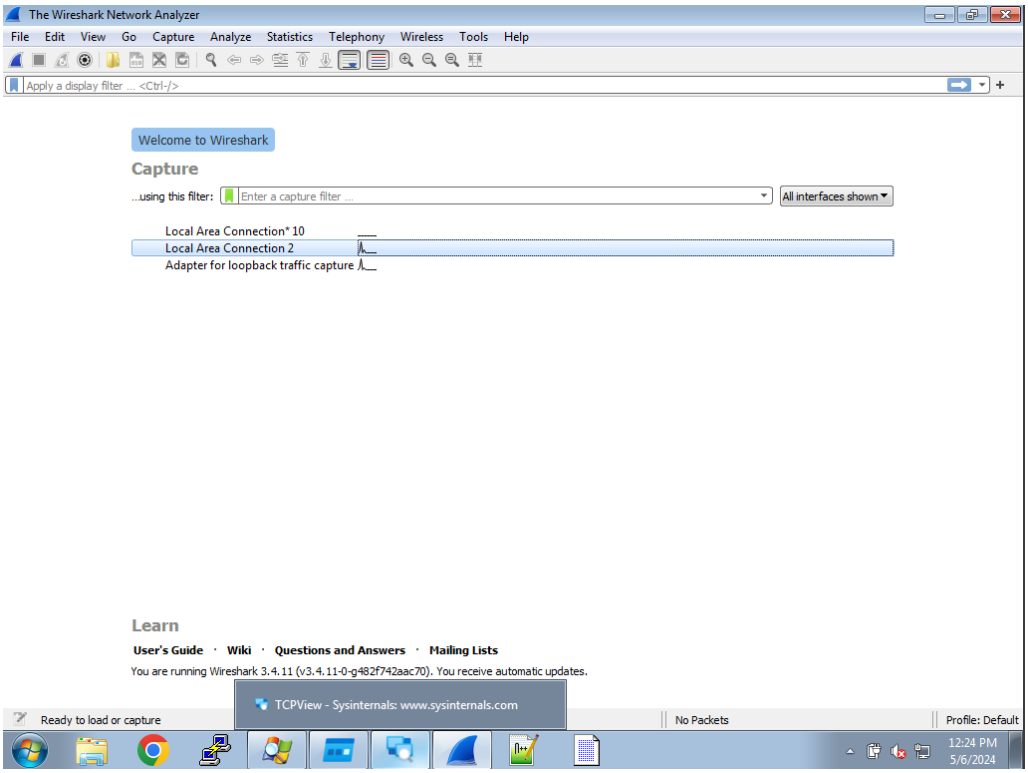


Рис. 2.11. Відкритий Wireshark

Запуск “Wireshark”, який можна побачити на рис 2.11, необхідний для перехоплення трафіку з даного хосту, який буде утворюватися під час та після запуску ШПЗ.

Після підготовки, можна запускати файл з зловмисним змістом, як було вказано вище у випадку даного зразка ШПЗ наявний файл – це документ в форматі .doc з прихованими в ньому макросами, для їх активації натискається кнопка “Включити вміст” після чого відбувається комунікація у фоновому режими з зловмисним ресурсом, який має наступну IP-адресу 89[.]23[.]98[.]22 по 445 (SMB) порту, дана активність була зафіксована наступним програмним забезпеченням:

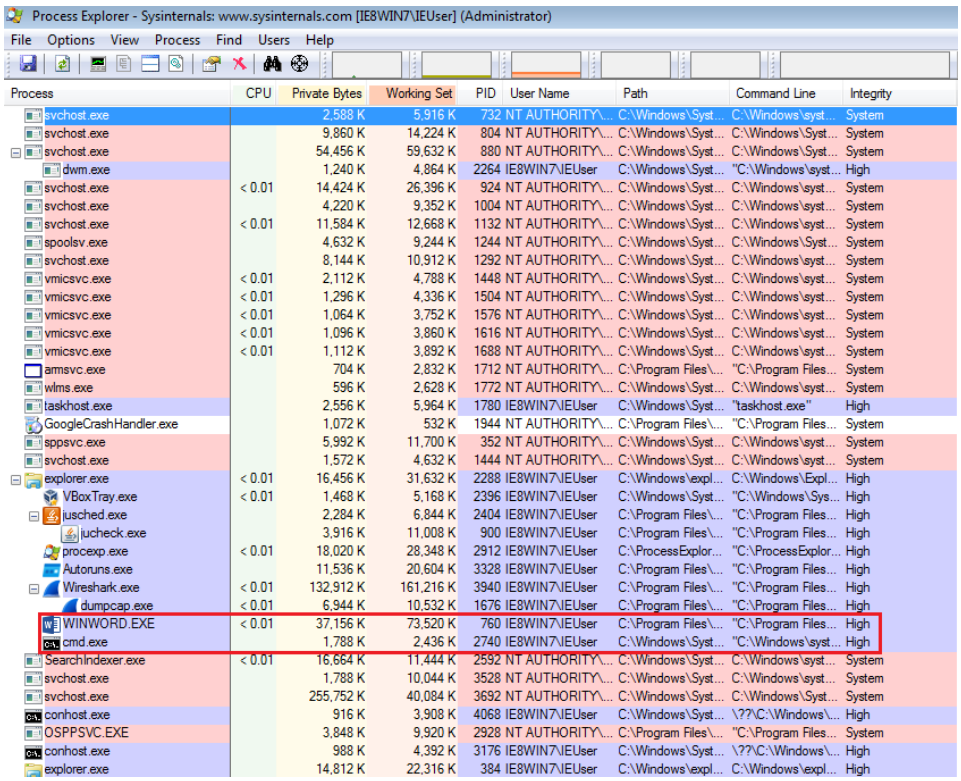


Рис. 2.12. Зафіксована активність за допомогою Sysinternals – Process Explorer

За допомогою програмного забезпечення “Process Explorer” на рис 2.12 можна побачити запущені процеси відкритого документа та відкритої командної строки, яка з’явилась під час виконання макросу та швидко зникла після успішного виконання заданого зловмисником коду.

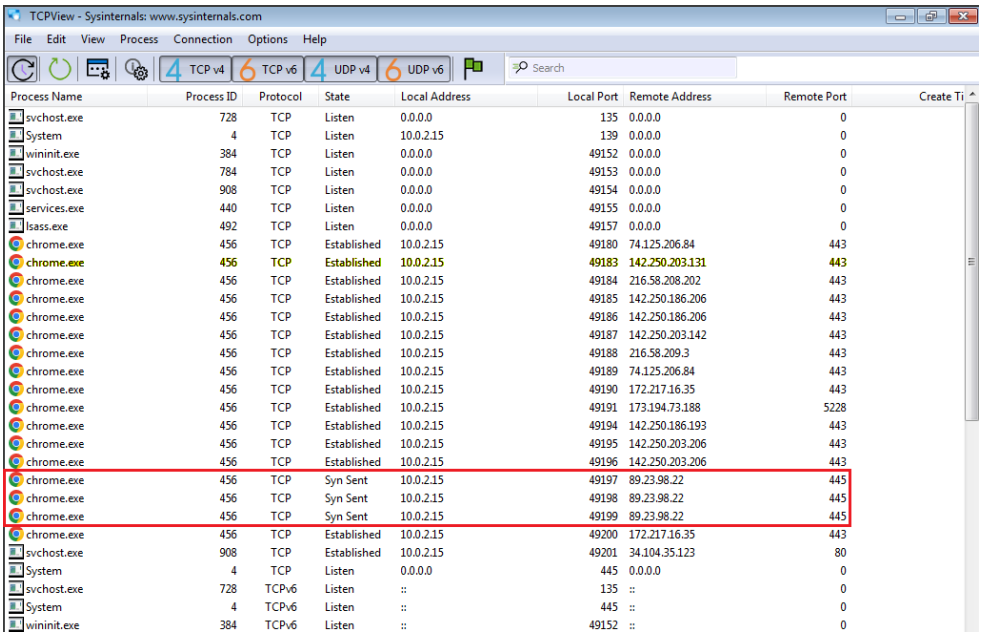


Рис. 2.13. Зафіксована активність за допомогою Sysinternals – TCPView

За допомогою програмного забезпечення “TCPView” на рис. 2.13 можна побачити спроби комунікацій до зловмисного ресурсу за протоколом SMB по 445 порту, також відображається процес, за допомогою якого відбулась спроба комунікації, в даному випадку це браузер Chrome, оскільки під час запуску зловмисного файлу він був відкритий на робочій станції.

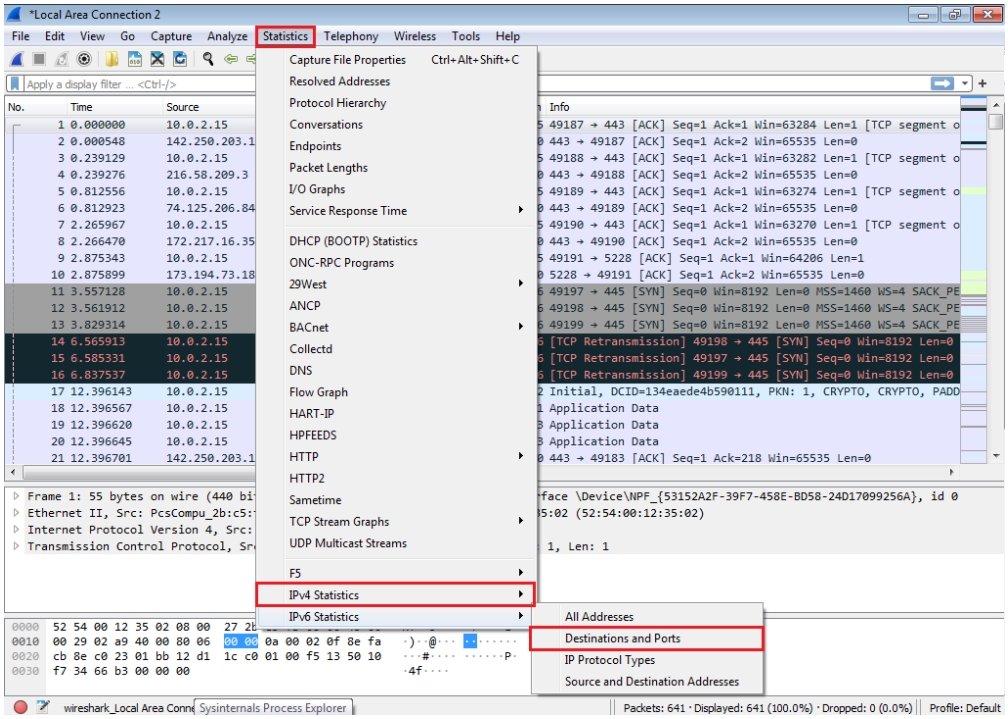
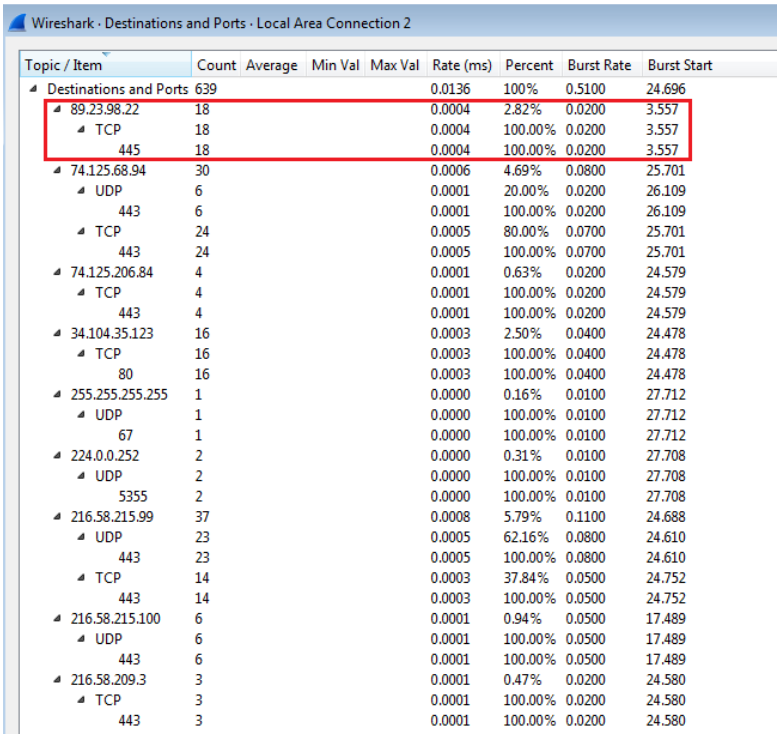


Рис. 2.14.1. Відкриття загальної зафіксованої активності трафіку за допомогою Wireshark

Після захоплення трафіку за допомогою програмного забезпечення “Wireshark” на рис. 2.14.1 можна побачити як загальну статистику так і дані про окремі пакети в цілому. В даному випадку немає сенсу аналізувати окремі пакети, тому відразу переглядається загальний зафіксований трафік по співвідношенню IP-адреси та протоколу:



Wireshark · Destinations and Ports · Local Area Connection 2

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Destinations and Ports	639				0.0136	100%	0.5100	24.696
89.23.98.22	18				0.0004	2.82%	0.0200	3.557
TCP	18				0.0004	100.00%	0.0200	3.557
445	18				0.0004	100.00%	0.0200	3.557
74.125.68.94	30				0.0006	4.69%	0.0800	25.701
UDP	6				0.0001	20.00%	0.0200	26.109
443	6				0.0001	100.00%	0.0200	26.109
TCP	24				0.0005	80.00%	0.0700	25.701
443	24				0.0005	100.00%	0.0700	25.701
74.125.206.84	4				0.0001	0.63%	0.0200	24.579
TCP	4				0.0001	100.00%	0.0200	24.579
443	4				0.0001	100.00%	0.0200	24.579
34.104.35.123	16				0.0003	2.50%	0.0400	24.478
TCP	16				0.0003	100.00%	0.0400	24.478
80	16				0.0003	100.00%	0.0400	24.478
255.255.255.255	1				0.0000	0.16%	0.0100	27.712
UDP	1				0.0000	100.00%	0.0100	27.712
67	1				0.0000	100.00%	0.0100	27.712
224.0.0.252	2				0.0000	0.31%	0.0100	27.708
UDP	2				0.0000	100.00%	0.0100	27.708
5355	2				0.0000	100.00%	0.0100	27.708
216.58.215.99	37				0.0008	5.79%	0.1100	24.688
UDP	23				0.0005	62.16%	0.0800	24.610
443	23				0.0005	100.00%	0.0800	24.610
TCP	14				0.0003	37.84%	0.0500	24.752
443	14				0.0003	100.00%	0.0500	24.752
216.58.215.100	6				0.0001	0.94%	0.0500	17.489
UDP	6				0.0001	100.00%	0.0500	17.489
443	6				0.0001	100.00%	0.0500	17.489
216.58.209.3	3				0.0001	0.47%	0.0200	24.580
TCP	3				0.0001	100.00%	0.0200	24.580
443	3				0.0001	100.00%	0.0200	24.580

Рис. 2.14.2. Загальної зафіксована активність трафіку за допомогою Wireshark

За допомогою програмного забезпечення “Wireshark” на рис. 2.14.2 можна побачити відправлені пакети до зловмисного ресурсу з хоста на якому відбулась активація ШПЗ.

У випадку програмного забезпечення “Autorans” не було зафіксовано зловмисної активності, оскільки даний файл формату .doc з макросом не ініціював нові точки автозавантаження.

Оскільки зазвичай подібні зловмисні ресурси працюють не більше місяця після початку своєї активності, наразі – відповіді від даного ресурсу не отримано, отже зловмисне програмне забезпечення "scandoc.exe" не було завантажено на хост, тому подальше ручне розслідування без наступних зразків – неможливе.

При автоматизованому аналізі шкідливого програмного забезпечення не так важливо звідки його завантажувати на аналіз в спеціалізовану пісочницю, але варто пам’ятати, що зберігання у відкритому виді, тобто без архівування з паролем файлів, що містять ШПЗ – небезпечно, оскільки існує ризик зараження основного хосту.

Аналіз за допомогою пісочниці Virus Total:

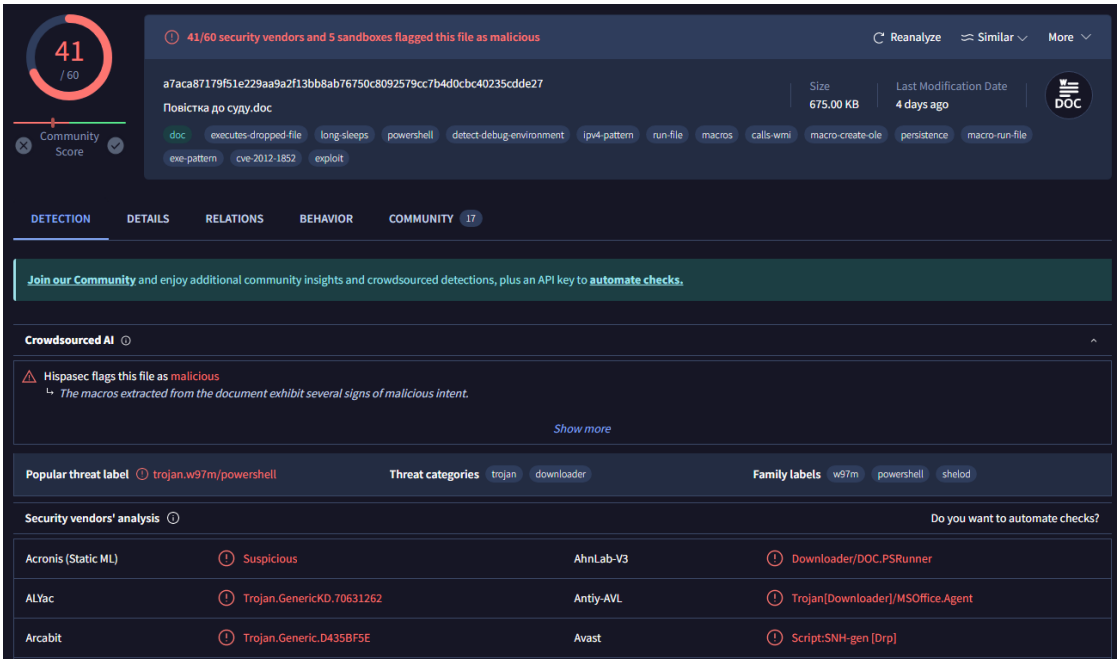


Рис. 2.15.1 Загальна інформація про завантажений зразок до Virus Total

При завантаженні зразка файлу “Повістка до суду .doc” до Sandbox Virus Total, спочатку можна побачити на рис. 2.15.1 загальну інформацію про файл, наприклад його назву та хеш-суму, додаткову інформацію про файл, а також рівень його репутації, яка ґрунтується на оцінці винесених вердиктів інших антивірусних баз даних різних виробників. З даного скріншоту можна побачити, що завантажений зразок файлу є шкідливим та має негативну репутацію за шкалою 41/60, також, серед додаткової інформації можна побачити, що згідно даних, які наявні в Virus Total, даний файл використовує “макроси”, “PowerShell”, може виконувати завантаження інших файлів та фігурує в інформації про вразливість “cve-2012-1852”.

У випадку, якщо завантажений зразок файлу з ШПЗ буде новий, тобто його сигнатури та індикатори раніше не фіксувались антивірусним захистом та не потрапили до їх баз даних, на даній сторінці буде відображено, що репутація завантаженого файлу – невідома.

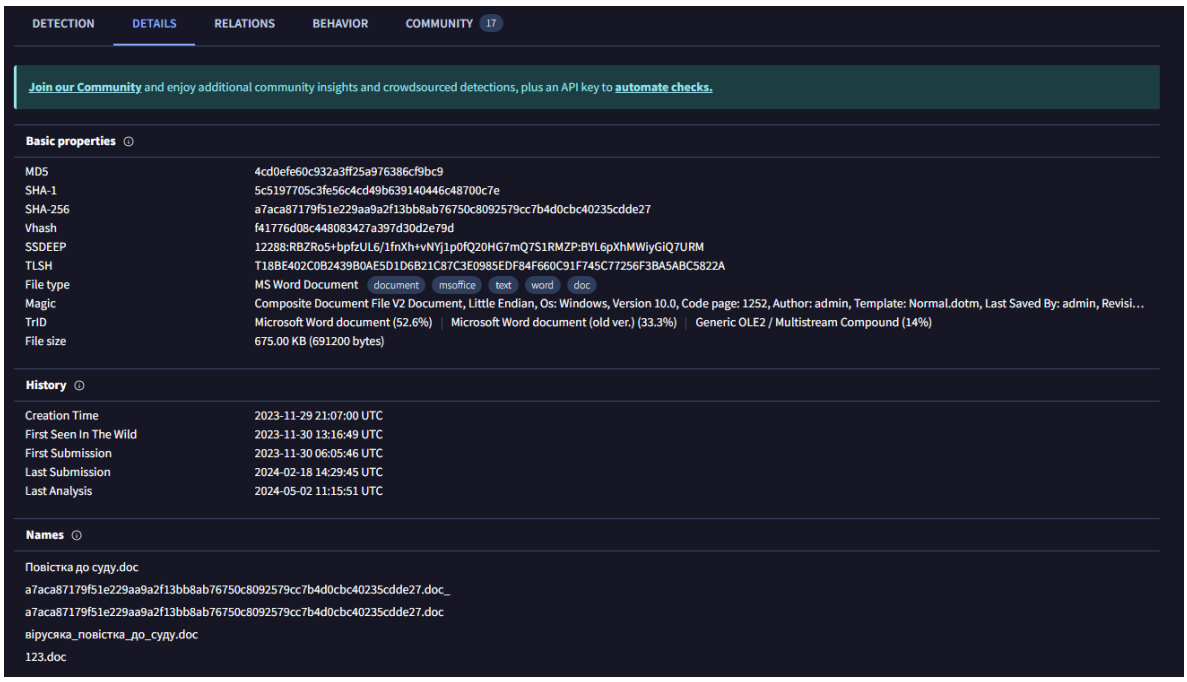


Рис. 2.15.2 Детальна інформація про завантажений зразок до Virus Total

При перегляді додаткової на рис. 2.15.2 інформації, можна побачити індикатори файлу такі як хеш-сума в різних форматах, інші зафіксовані назви даного зразка файлу, час створення файлу та час коли його завантажували вперше та останнє до пісочниці Virus Total.

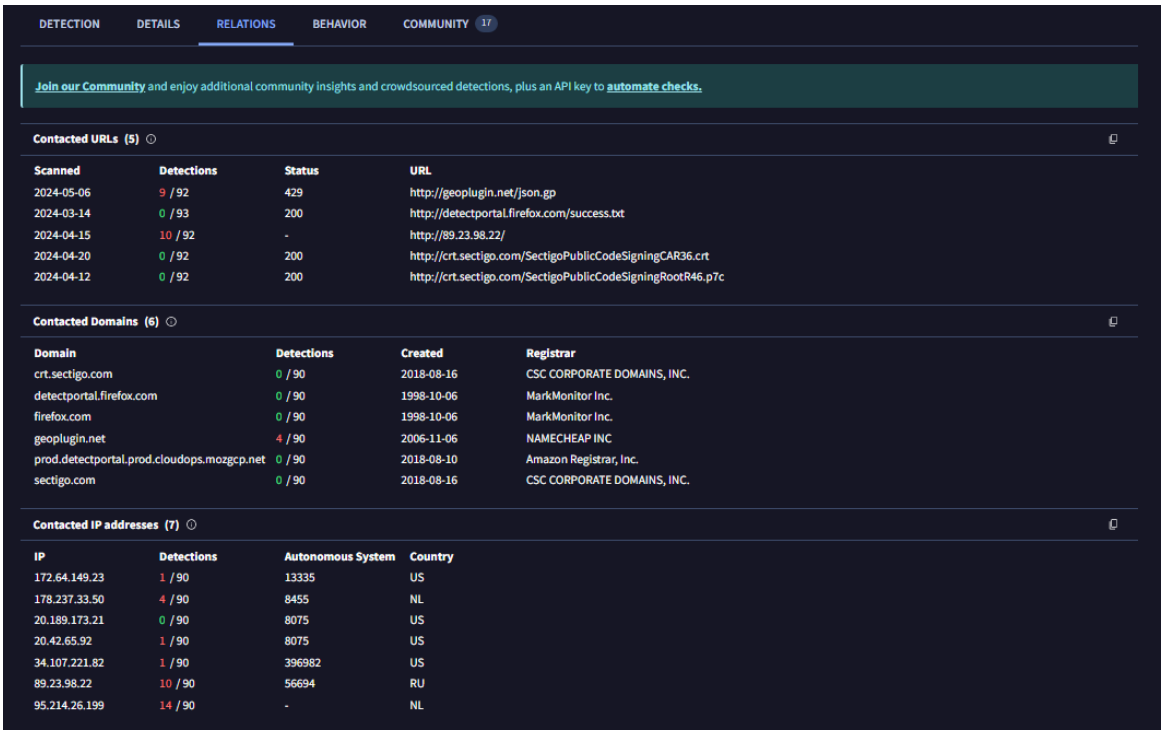


Рис. 2.15.3 Пов’язана інформація про завантажений зразок до Virus Total

У пов’язаній інформації про даний зразок на рис. 2.15.3 можна побачити посилання, домени та IP-адреси, які були задіяні при його поширенні, вони можуть бути як частиною алгоритму даного шкідливого програмного забезпечення так і сторонніми ресурсами за допомогою яких відбувалось поширення файлу.

Серед наведених індикаторів, які пов’язані з даним зразком присутня IP-адреса 89[.]23[.]98[.]22, яка була зафіксована при ручному аналізу коли відбувалась спроба комунікації по протоколу SMB з метою завантаження «scandoc.exe».

Аналіз за допомогою пісочниці Hybrid Analysis:

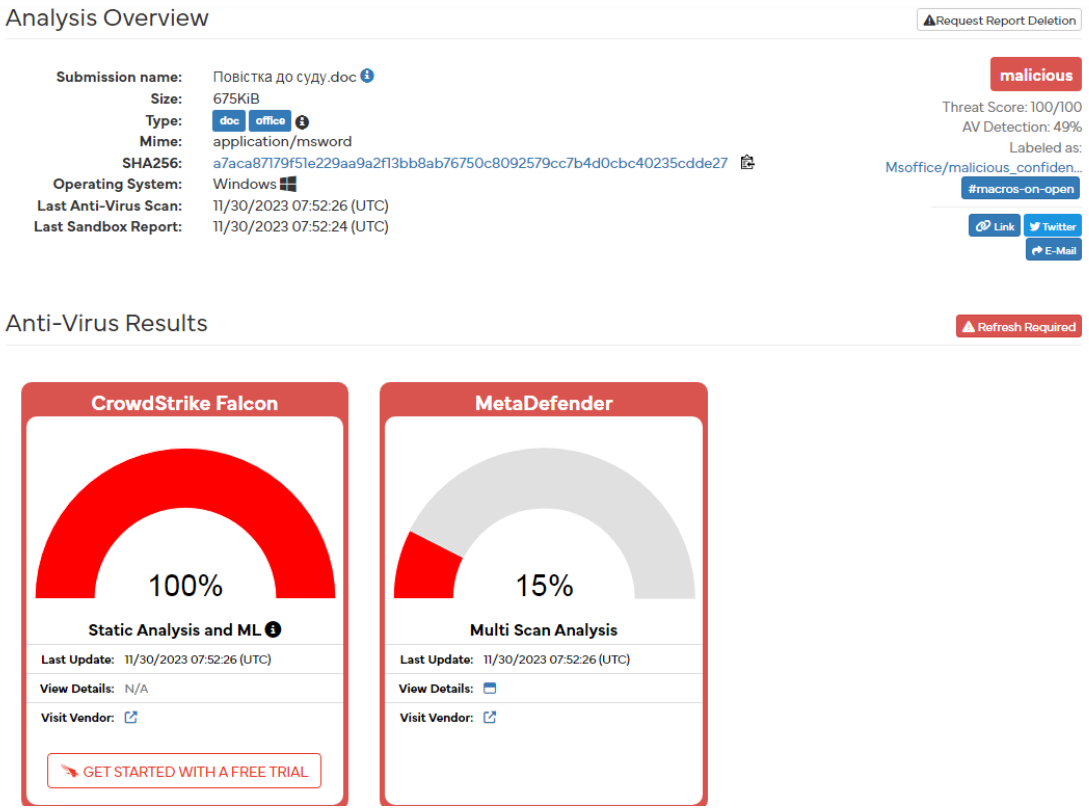


Рис. 2.16.1 Загальна інформація про завантажений зразок на Hybrid Analysis

У випадку загальної інформації про завантажений зразок файлу з ШПЗ можна побачити хеш-суму, тип файлу, його назву, коли вперше він була завантажений на аналіз до даної пісочниці, а також його вердикт, чи являється даний файл шкідливим, який ґрунтується на аналізі даної пісочниці, а також на вердикті наданим антивірусним захистом “CrowdStrice Falcon” та “MetaDefender”. Згідно наявної на рис. 2.16.1 інформації, Sandbox Hybrid Analysis вважає даний файл – шкідливим.

Рис. 2.16.2 Результат аналізу завантаженого зразок до Hybrid Analysis

Згідно рис. 2.16.2 можна побачити вердикт, що проаналізований файл – шкідливий за шкалою 100/100, серед зафіксованих індикаторів, згідно вердикту Sandbox Hybrid Analysis, було визначено дев’ять шкідливих індикаторів, які безпосередньо приймали участь при виконанні алгоритму даного ШПЗ, сім опосередкованих індикаторів, наприклад домени та п’ятдесят чотири легітимних індикаторів, які також були зафіксовані, але Hybrid Analysis вважає, що вони не мають прямого відношення до ШПЗ, наприклад індикатор, який належить Google DNS, а саме IP-адреса 8[.]8[.]8[.]8.

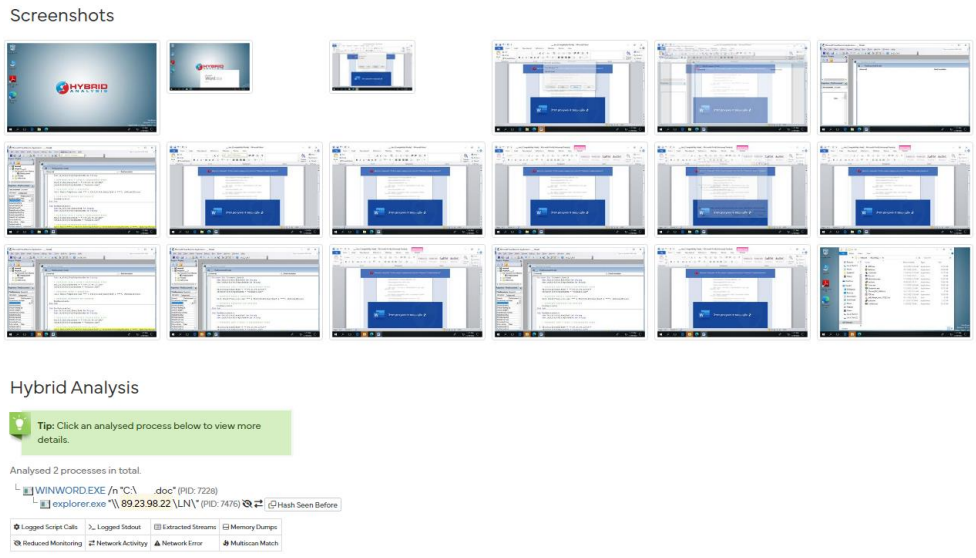


Рис. 2.16.3 Зроблені скріншоти під час аналізу завантаженого зразку до Hybrid Analysis, а також основний алгоритм дій даного ШПЗ

На рис. 2.16.3 наведено скріншоти, які зробила пісочниця Hybrid Analysis, а також наведена основний алгоритм дій даного ШПЗ, а саме спроба комунікації до IP-адреси 89[.]23[.]98[.]22.

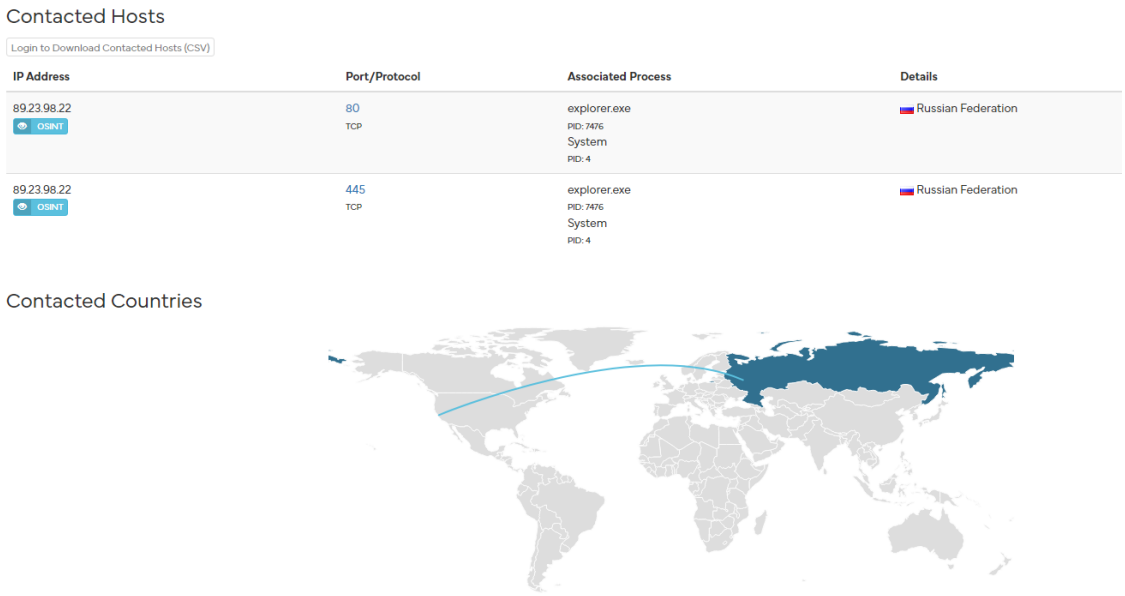


Рис. 2.16.4 Зафіксовані мережеві спроби комунікацій під час аналізу завантаженого зразку до Hybrid Analysis

Серед зафіксованих спроб мережевих комунікацій на рис. 3.2.4 можна побачити комунікацій по 80 (http) порту та 445 (SMB) порту до IP-адреси 89[.]23[.]98[.]22, яка згідно геолокації належить Russian Federation.

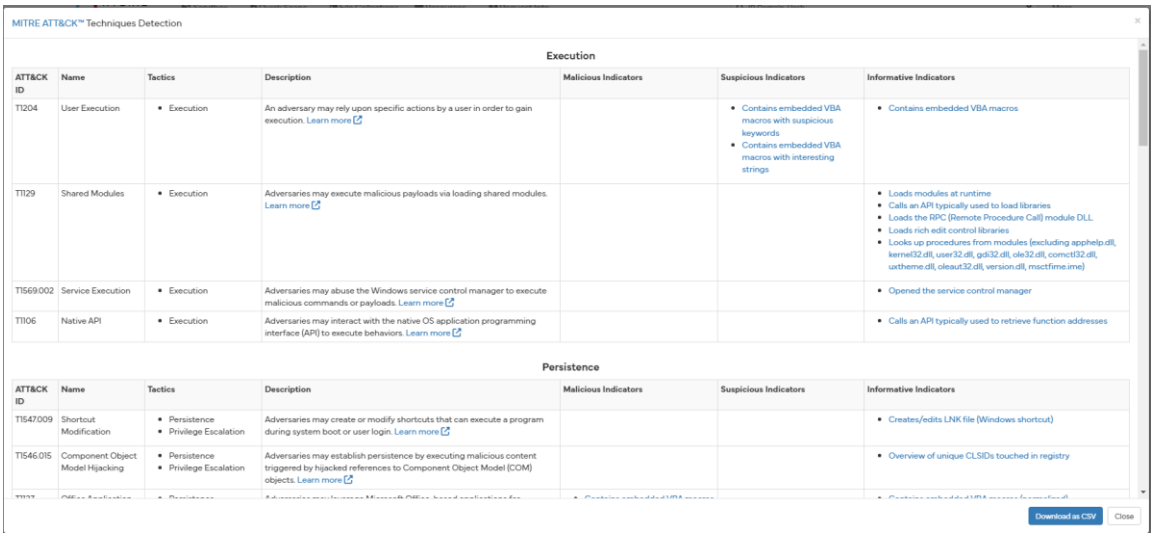


Рис. 2.16.5 Матриця тактик та технік, які застосовувались завантаженим зразком ШПЗ до Hybrid Analysis згідно “MITRE ATT&CK”

Згідно рис. 2.16.5 можна побачити усі зафіксовані тактики та техніки, які

використовувало дане ШПЗ згідно відомої матриці “MITRE ATT&CK”.

Аналіз за допомогою пісочниці Triage:

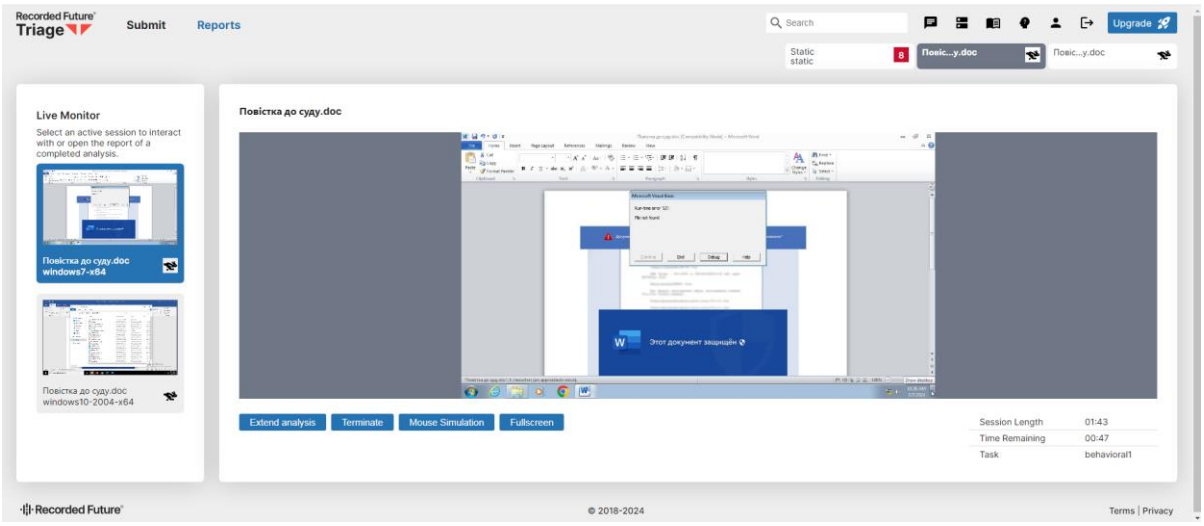


Рис. 2.17.1 Процес аналізу завантаженого зразку до Triage

На рис. 2.17.1 можна побачити процес аналізу завантаженого зразку з ШПЗ з яким під час аналізу можна взаємодіяти, наприклад відкривати або редагувати файл.

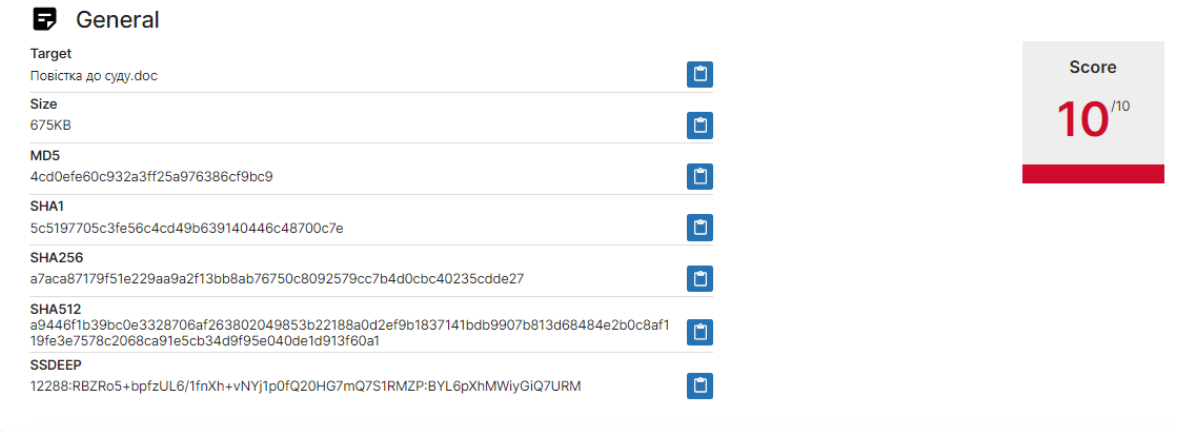


Рис. 2.17.2 Загальна інформація про завантажений зразок до Triage

Згідно загальної інформації на рис 2.17.2 про завантажений зразок до Sandbox Triage можна побачити індикатори файлу, а саме різні типи хеш-суми файлу, його назву, а також вердикт його зловмисності за шкалою 10/10.

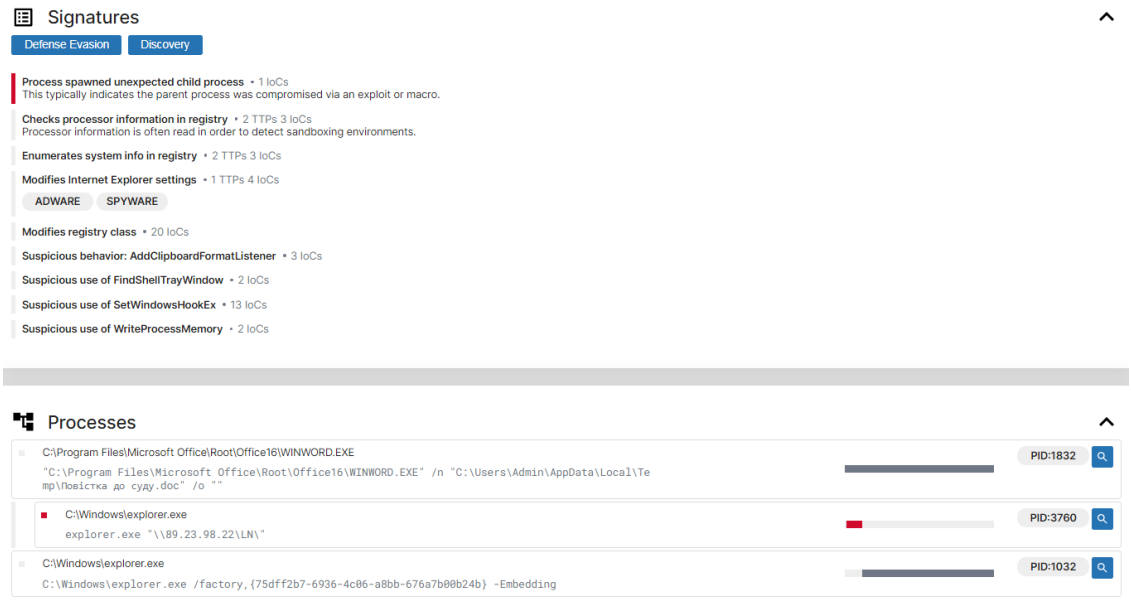


Рис. 2.17.3 Зафіксовані сигнатури та процеси під час аналізу завантаженого зразку з ШПЗ до Triage

Серед наявної інформації на рис. 2.17.3 можна побачити зафіксовані сигнатури зразка з ШПЗ з його імовірною класифікацією як “Adware” та “Spyware”, а також основні процеси, які виконував даний файл, серед яких можна побачити спробу комунікацій до IP-адреси.

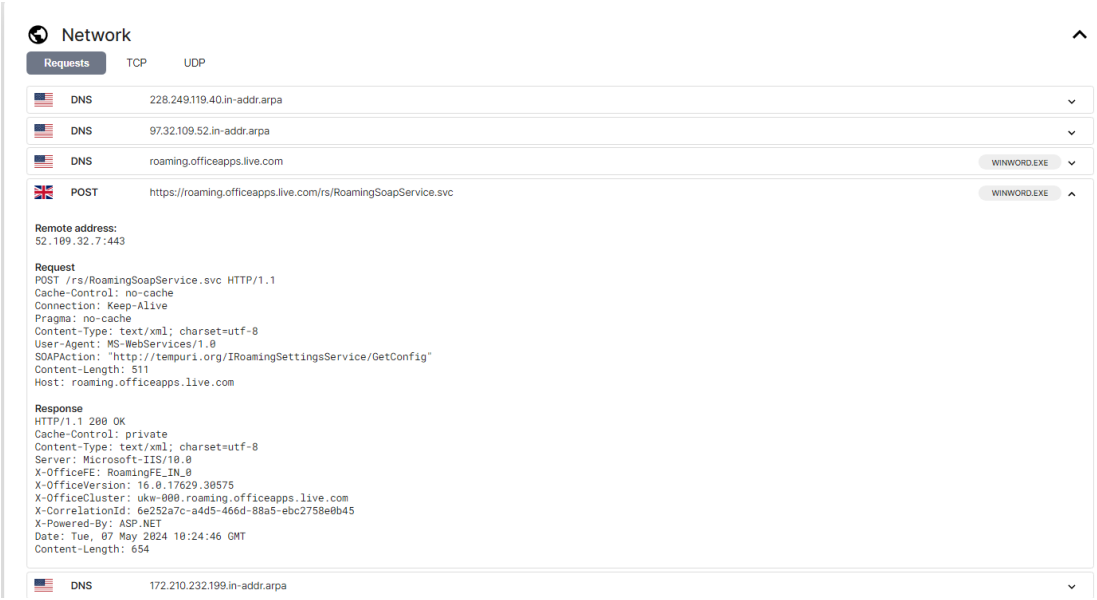


Рис. 2.17.4 Запити мережевих комунікацій, які були зафіксовані під час аналізу завантаженого зразку з ШПЗ до Triage

Серед наявних зафіксованих запитів на рис. 2.17.4 було виявлено лише

опосередковані запити до ресурсів, які напряму не стосуються зловмисної активності завантаженого зразку з ШПЗ.

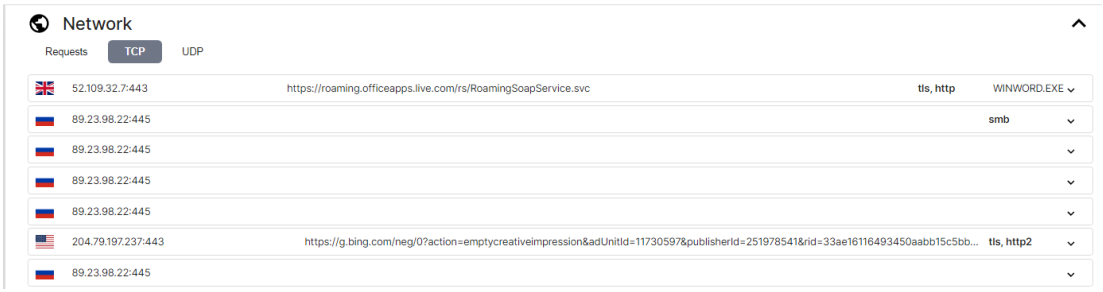


Рис. 2.17.5 Мережеві комунікації по TCP протоколу, які були зафіксовані під час аналізу завантаженого зразку з ШПЗ до Triage

Згідно зафіксованих під час аналізу завантаженого зразку з ШПЗ до Triage мережевих комунікацій по TCP протоколу, на рис 2.17.5 можна побачити комунікації по 445 (SMB) порту до IP-адреси 89[.]23[.]98[.]22.

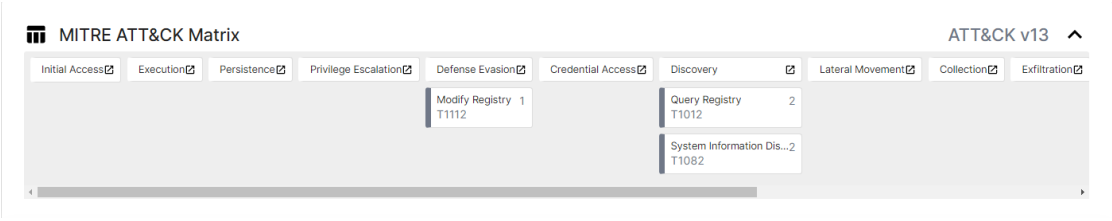


Рис. 2.17.6 Матриця тактик та технік, які застосовувались завантаженим зразком ШПЗ до Triage згідно “MITRE ATT&CK

Згідно рис. 2.17.6 можна побачити усі зафіксовані тактики та техніки, які використовувало дане ШПЗ згідно відомої матриці “MITRE ATT&CK”.

Аналіз за допомогою пісочниці Valkyrie:

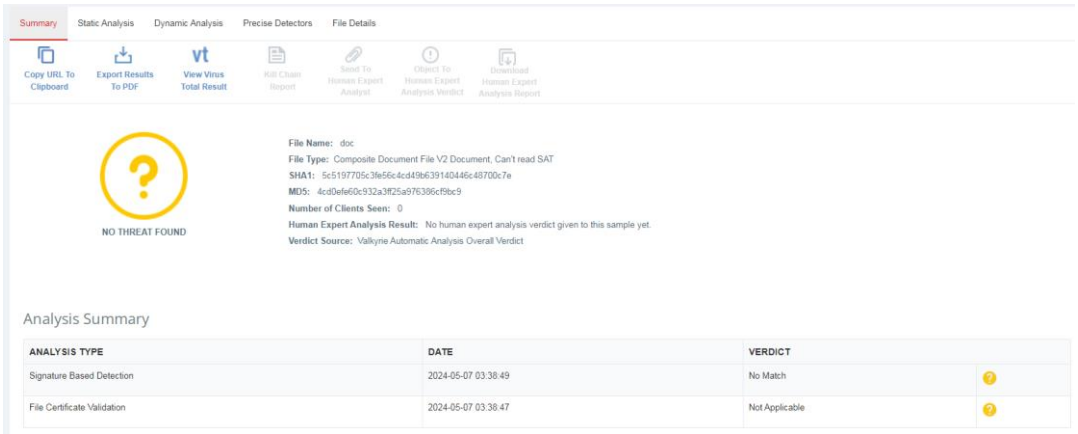


Рис. 2.18 Загальна інформація про завантажений зразок до Valkyrie

На рис. 2.18 можна побачити, що Sandbox Valkyrie не вдалось ідентифікувати завантажений зразок з ШПЗ як шкідливий файл, імовірно, це пов’язано з тим, що наразі ресурс для завантаження основного ШПЗ вже недоступний та даний зразок не завантажували до цієї пісочниці під час його доступності.

Отже, завершуючи аналіз даного шкідливого програмного забезпечення через який відбувся кіберінцидент "Повістка до суду" – CERT-UA#8150, можна зробити висновок, що зловмисники продовжують використовувати дедалі складніші методи для обходу захисних систем. Це підкреслює важливість постійного вдосконалення заходів безпеки та навчання працівників з основ кібергігієни. Важливим кроком для захисту від подібних атак є впровадження багаторівневих систем захисту, які здатні виявляти та блокувати шкідливі дії на різних етапах їх виконання.

Оскільки одним з головних рішень, які спроможні протидіяти подібним інцидентам є Firewall, розглянемо детальніше рішення типу NGFW від виробника Check Point в наступному розділі.

2.4 Огляд рішення Check Point NGFW

Check Point Next Generation Firewall (NGFW) - це інтегрована платформа забезпечення безпеки мережі, яка надає розширені функції захисту від загроз для корпоративних мереж.

Дане рішення має наступні характеристики та функції:

1) Захист від загроз: Check Point NGFW використовує мультілейбл-захист для виявлення та блокування різних видів загроз, включаючи віруси, шкідливі програми, атаки з метою перехоплення сесії та інші.

2) Апаратне та програмне забезпечення: Це рішення доступне у вигляді апаратного обладнання або програмного забезпечення, що дозволяє вибрати найбільш підходящий варіант для конкретних потреб вашої мережі.

3) Управління політикою безпеки: Check Point NGFW має потужні інструменти для налаштування та управління політикою безпеки, що дозволяє адміністраторам налаштовувати правила доступу та моніторити активність мережі.

4) Інтеграція з іншими продуктами: Check Point NGFW інтегрується з іншими рішеннями безпеки від Check Point та сторонніми постачальниками, що дозволяє створити комплексну систему захисту мережі.

5) Моніторинг та аналіз: Це рішення має вбудовані засоби моніторингу та аналізу мережевої активності, що допомагає виявляти аномалії та потенційні загрози. [7]

Управління шлюзами мережевого обладнання Check Point NGFW виконується за допомогою спеціального серверу керування Security Management Server (SMS), зазвичай схема підключення для налаштування політик NGFW зображено на рис. 2.19:

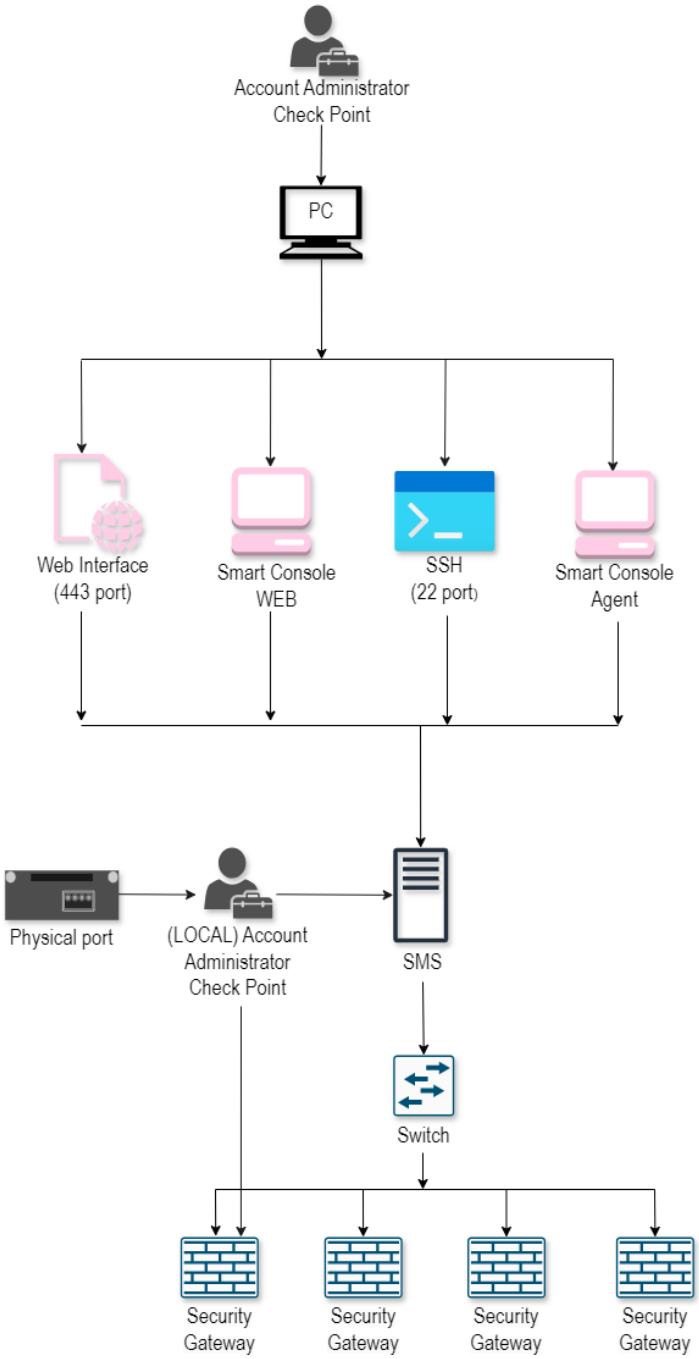


Рис. 2.19 – Загальна схема підключення для налаштування політик Check Point NGFW

З схеми підключення на рис. 2.19 можна побачити, що для налаштування політик шлюзів Check Point NGFW в даному випадку позначеними як “Security Gateway” потрібно або віддалено підключитись за допомогою спеціальних консолей, по веб-інтерфейсу та по SSH протоколу до керуючого серверу “SMS” або знаходячись фізично біля обладнання, в обох випадків повинно мати облікові дані від мережевого адміністратора Check Point.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАСТОСУВАННЯ РЕЗУЛЬТАТІВ АНАЛІЗУ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НА БАЗІ РІШЕННЯ CHECK POINT NGFW

3.1 Рекомендації щодо використання результатів аналізу шкідливого програмного забезпечення у контексті NGFW

Головним результатом аналізу шкідливого програмного забезпечення є отримання індикаторів таких як: IP-адрес, хеш-сума, URL, File Name, Domain, E-mail, E-mail Subject, тощо та розуміння основного алгоритму дій, які виконує відповідне ШПЗ.

У випадку результатів ручного та автоматизованого аналізу зразка файлу з ШПЗ, який стосується кіберінциденту "Повістка до суду" – CERT-UA#8150, в якості алгоритму дій можна відмітити:

1) Спроби комунікацій по 445 SMB порту до зовнішніх IP-адрес, які не належать безпосередньо організації з хоста якої були ініційованні дані спроби. Зробити окремий список з IP-адресами з якими дозволено створювати комунікації з внутрішньої мережі по SMB протоколу.

2) Спроби комунікацій до IP-адреси, яка згідно геолокації належить до країни з якою відсутні ділові зв’язки та з яких походять багато зловмисників згідно зафіксованих кіберінцидентів у відповідній країні, наприклад в нашому випадку є сенс обмежити доступ комунікацій по геолокації з наступними країнами: Росія, Китай, Білорусія, Іран, Сирія.

Також, в рамках рішення типу SEG/MSG варто розгляну політики щодо отримання електронних листів у вкладенні яких знаходиться архіви з паролем, а саме налаштувати відправку подібних листів до карантину з можливістю при необхідності дістати звідти дані електронні листи певними адміністраторами у випадку, якщо подібна активність не є нормою для даної організації.

В якості індикаторів для блокування можна визначити наступні IoC`s з

таблиці 1.1:

Таблиця 1.1

Зловмисні індикатори компрометації

Тип IoC`s	IoC`s для блокування
IP	89.23.98.22
Domain	\\89.23.98.22\LN
Hash SHA-256	73673d54d4618acf07725b94113fd978247f9238f594600614365dee2fb7cf9e
Hash SHA-256	26b4ccad487e76f40a5806c638589d3b2fb29bd799accc1cfaa6739e7ec437df
Hash SHA-256	a7aca87179f51e229aa9a2f13bb8ab76750c8092579cc7b4d0cbc40235cdde27
Hash SHA-256	0e87545022ff71033237566bafd531b504fcc973229810fab00267c6457bdde3
URL	\\89.23.98.22\LN\scandoc.exe
E-Mail Subject	Повістка в суд-вихідний : 8136927286 від 30.11.2023

Та в якості тимчасової міри до вирішення даного кіберінциденту, в даному випадку до моменту обмеження доступу зловмисникам до скомпрометованих облікових записів державного уряду з якого відбувалось поширення зловмисних електронних листів, можна заблокувати легітимні індикатори, а саме IoC`s, які наведено в таблиці 1.2:

Таблиця 1.2

Легітимні індикатори компрометації

E-mail	zal404@od.arbitr.gov.ua
E-mail IP	212.90.190.159
E-mail Domain	od.arbitr.gov.ua

3.2 Використання Check Point NGFW для протидії шкідливому програмному забезпеченню

Головною задачею Check Point NGFW є захист периметру мережі шляхом фільтрації трафіку, що проходить через шлюзи, які зазвичай є мостом між внутрішньою та зовнішньою мережею, отже протидіяти шкідливому програмному забезпеченню дане рішення може лише у випадках коли мережева активність яка пов’язана з ШПЗ намагається перетнути кордон через певний шлюз, незалежно від того звідки відбуваються дані спроби комунікацій, ззовні до внутрішнього хоста в мережі чи навпаки.

Отже, на прикладі результатів аналізу шкідливого програмного забезпечення який пов’язаний з кіберінцидентом "Повістка до суду" – CERT-UA#8150 розглянемо можливі дії, які будуть протидіяти появі аналогічного кіберінциденту в інфраструктурі організації або установи за допомогою рішення Check Point NGFW.

З результатів аналізу даного ШПЗ можна виконати 3 рішення для протидії даній активності, а саме:

1) Налаштування політики для блокування спроб комунікацій у випадку, коли хост з внутрішньої мережі ініціює спробу комунікації по 445 порту до IP-адреси, яка знаходиться у зовнішній мережі та не належить певному списку виключень для цього правила:

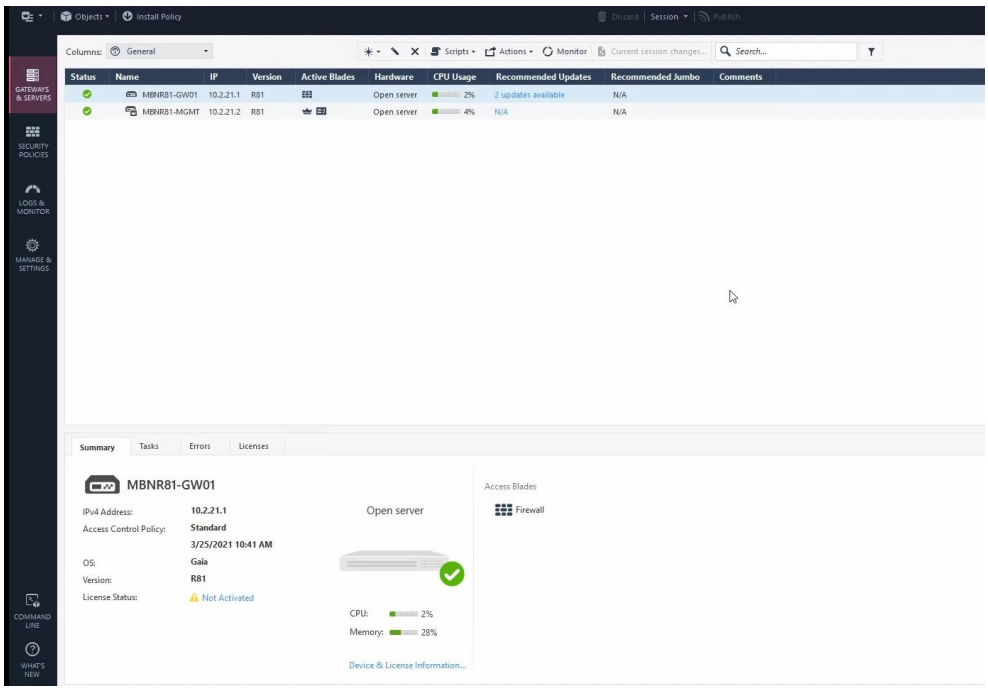


Рис. 3.1.1 – Інтерфейс Smart Console при підключенні до SMS для налаштування Check Point NGFW

Для того щоб виконати налаштування відповідного мережевого обладнання Check Point NGFW, в даному випадку це один шлюз “GW01”, необхідно за допомогою “Smart Console” підключитись до керуючого серверу “SMS” до якого підключене відповідний шлюз Check Point NGFW. Приклад відкритого Smart Console можна побачити на рис. 3.1.1.

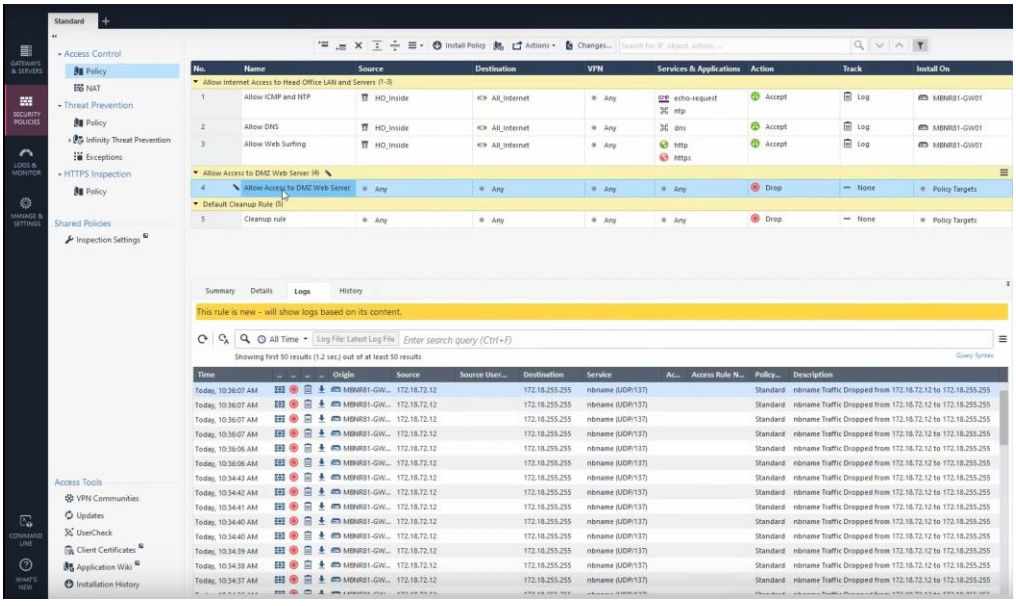


Рис. 3.1.2 – Налаштування політик та правил фільтрації трафіку Check Point NGFW

При переході до налаштувань політик необхідно створити та налаштувати правило, в нашому випадку це заборона комунікацій до зовнішніх IP-адрес по SMB протоколу, у випадку, коли дані IP-адреси не знаходяться у списку з виключеннями, яким дозволено подібні комунікації, в даному випадку це IP-адреси, які належать Microsoft. Приклад відкритої вкладки налаштування політик та правил можна побачити на рис. 3.1.2.

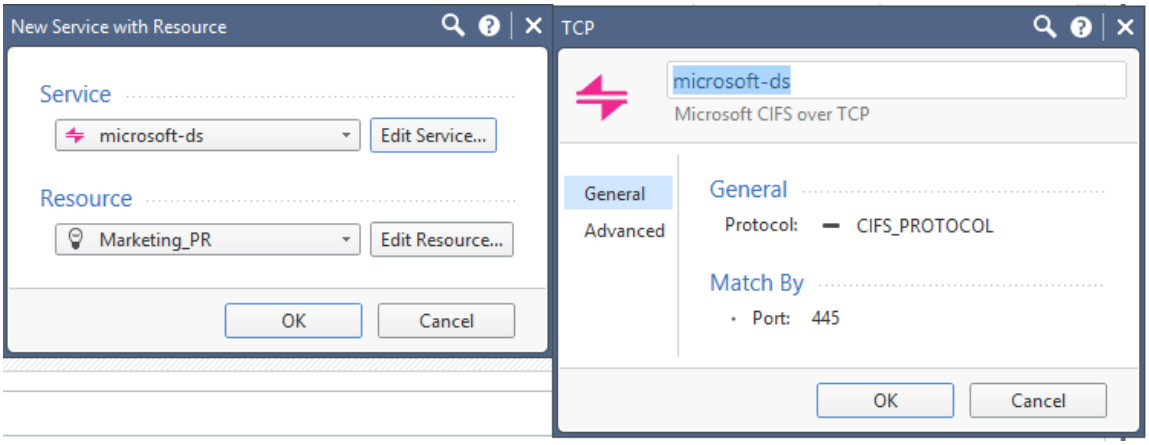


Рис. 3.1.3 – Створення правила та додавання виключень для легітимних комунікацій до зовнішньої мережі по протоколу SMB на Check Point NGFW

При створенні правила додаємо виключення до нього вже з готовим списком з IP-адресами, які належать компанії Microsoft та вказуємо 445 SMB порт по якому має працювати дане правило. Приклад налаштування наведено на рис. 3.1.3.

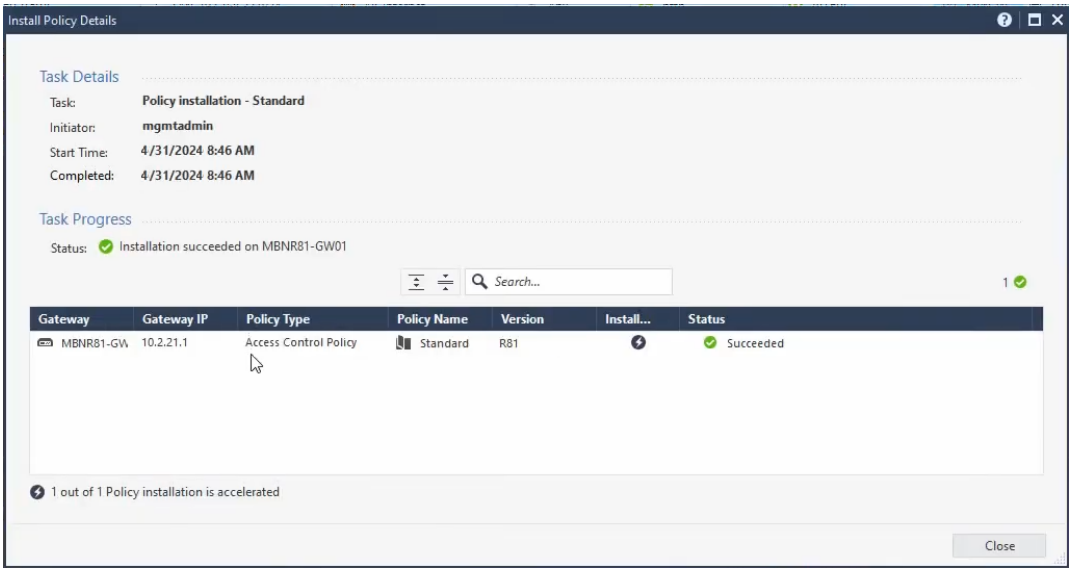


Рис. 3.1.4 – Встановлення налаштованих політик на Check Point NGFW

Після завершення налаштування політик, необхідно прийняти та відправити їх зміни до відповідного переліку обладнання, на яких має працювати дані політики, в нашому випадку це шлюз “GW01”. Приклад наведено на рис. 3.1.4.

2) Налаштування політики для блокування спроб комунікацій у випадку, коли комунікації відбуваються з IP-адресами, які належать певному переліку країн:

Оскільки IP-адреса 89[.]23[.]98[.]22, яка використовувалась для завантаження програми для віддаленого управління RemcosRAT згідно її геолокації належить до країни Russian Federation з якої постійно відбуваються кібератаки по відношенню до організацій та установ, які належать Україні, в даному випадку існує сенс заблокувати комунікації з даною країною.

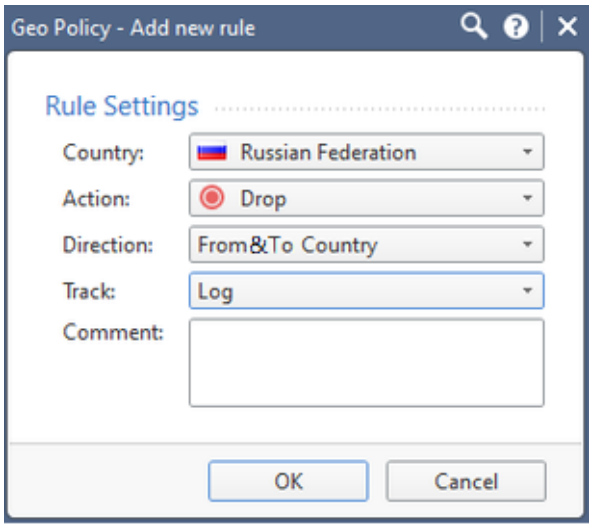


Рис. 3.2.1 – Створення нового правила для блокування трафіку з певною країною Check Point NGFW

На рис. 3.2.1 при створенні правила в “Country” обираємо відповідну країну, “Action” позначаємо як “Drop”, оскільки дані спроби комунікацій мають блокуватись, в “Direction” обираємо “From&To Country” для того щоб дане правило діяла у випадку спроб комунікацій з зовні до внутрішньої мережі та навпаки, а також в “Track” обираємо “Log” для того щоб в журнали подій потрапляла інформація про спроби вказаних в правилі комунікацій.

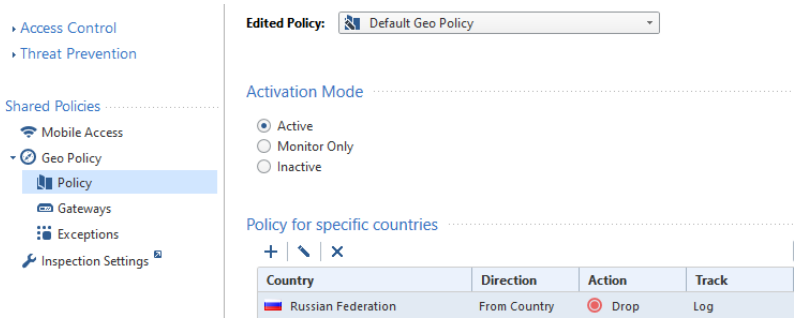


Рис. 3.2.2 – Увімкнення створеного правила для блокування трафіку з певною країною Check Point NGFW

На рис. 3.2.2 в налаштуваннях політик, обираємо дане правило та натискаємо в “Activation Mode” параметр “Active” для того, щоб дане правило почало виконуватись.

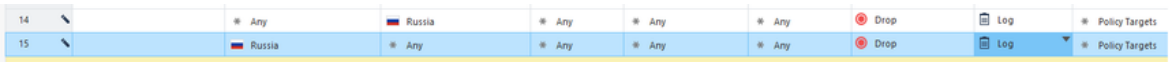


Рис. 3.2.3 – Перегляд створеного правила для блокування трафіку з певною країною Check Point NGFW

При перегляді створеного правила на рис. 3.2.3 можна побачити, що воно знаходиться в політиці Check Point NGFW та працює.

3) Занесення до чорного списку IoC`s видобутих з ШПЗ, який згідно налаштуванням на мережевому обладнанні Check Point NGFW блокує усі спроби комунікацій з даним списком:

В якості наглядного прикладу буде наведено процедуру зловмисної блокування IP-адреси 89[.]23[.]98[.]22:

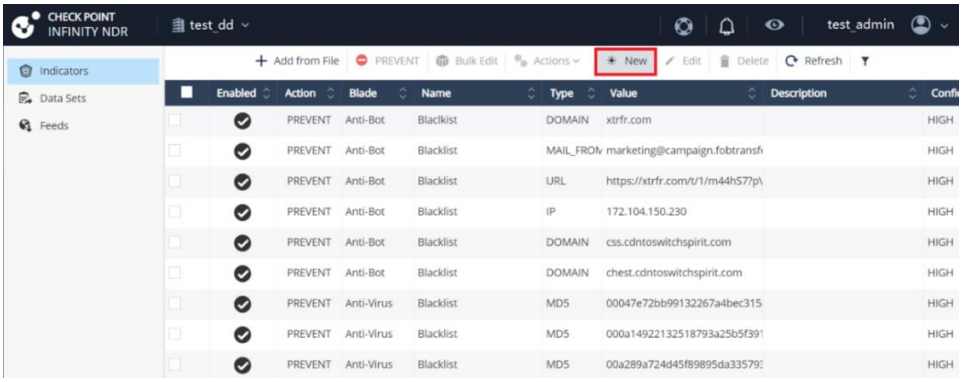


Рис. 3.3.1 – Внесення нового індикатору до чорного списку Check Point NGFW

Спочатку необхідно натиснути на клавішу “New”, приклад наведено на рис. 3.3.1, для того щоб відкрити форму заповнення внесення певного індикатора до певного списку.

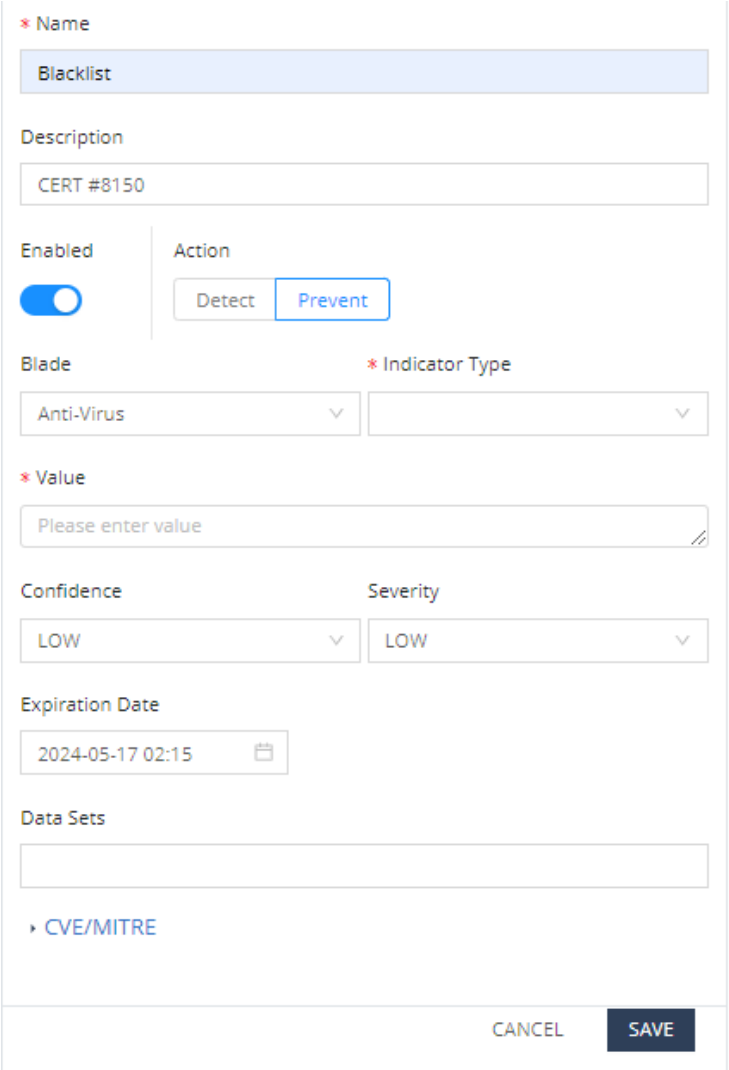


Рис. 3.3.2 – Огляд доступних налаштувань для внесення нового індикатору до чорного списку Check Point NGFW

В формі заповнення на рис 3.3.2 можна побачити, що для занесення певного індикатора до певного списку обов’язково необхідно заповнити поля “Name”, “Indicator Type” та “Value”, тобто необхідно ввести назву списку в даному випадку це назва чорного списку “Blacklist”, тип індикатору та сам індикатор. Також необхідно обрати тип дій “Detect” або “Prevent”, тобто як Check Point NGFW буде реагувати на виявлену спробу комунікації з даним індикатором, просто зафіксувати та при окремих налаштуваннях або інтеграцій з такими рішеннями як SIEM –

оповістити про виявлену комунікацію чи відразу заблокувати дану спробу комунікації, відповідно. Для того щоб дані дії виконувались необхідно включити дане правило за допомогою кнопки “Enabled”. Окрім цього в даній формі наявне поле “Description”, яке використовується для додавання опису, в даному випадку вказано номер кіберінциденту “CERT #8150”.

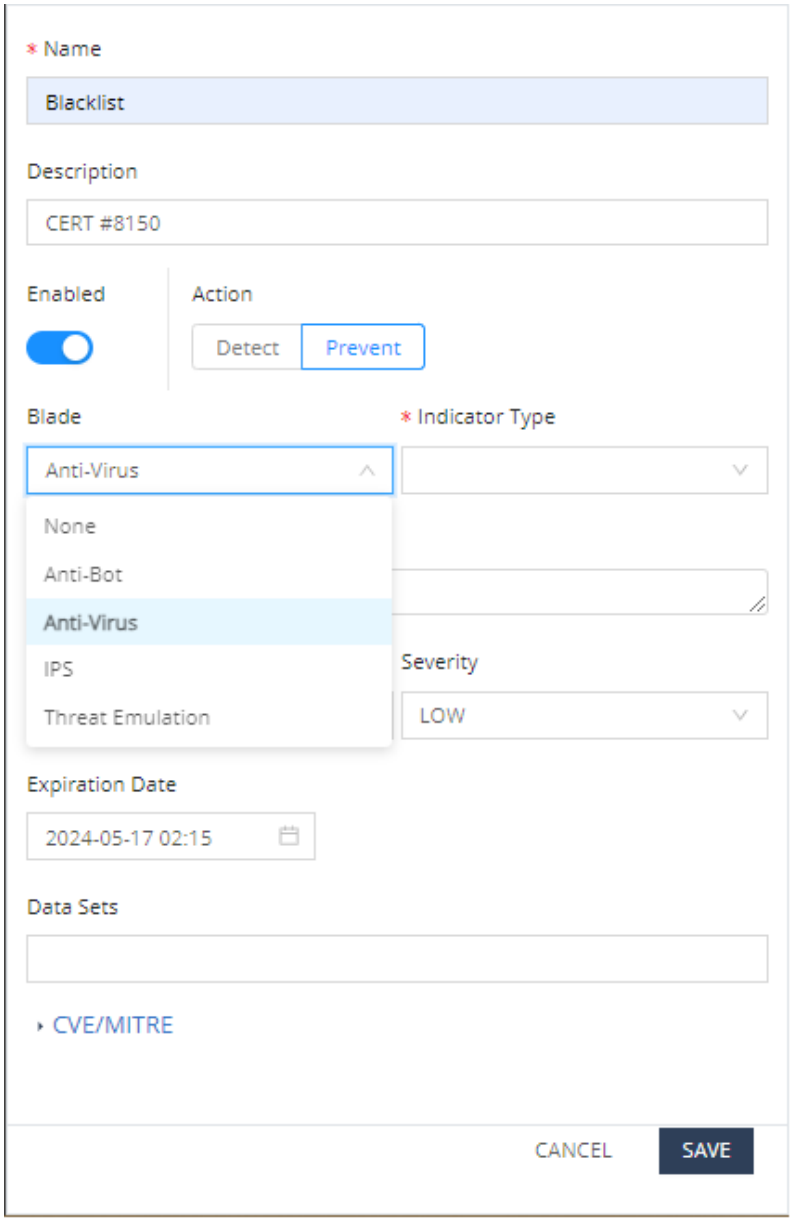


Рис. 3.3.3 – Заповнення “Blade” для внесення нового індикатору до чорного списку Check Point NGFW

При обиранні “Blade” на рис. 3.3.3 в даному випадку вказується “Anti-Virus”, оскільки джерело з якого добуте даний індикатор саме шкідливе програмне забезпечення.

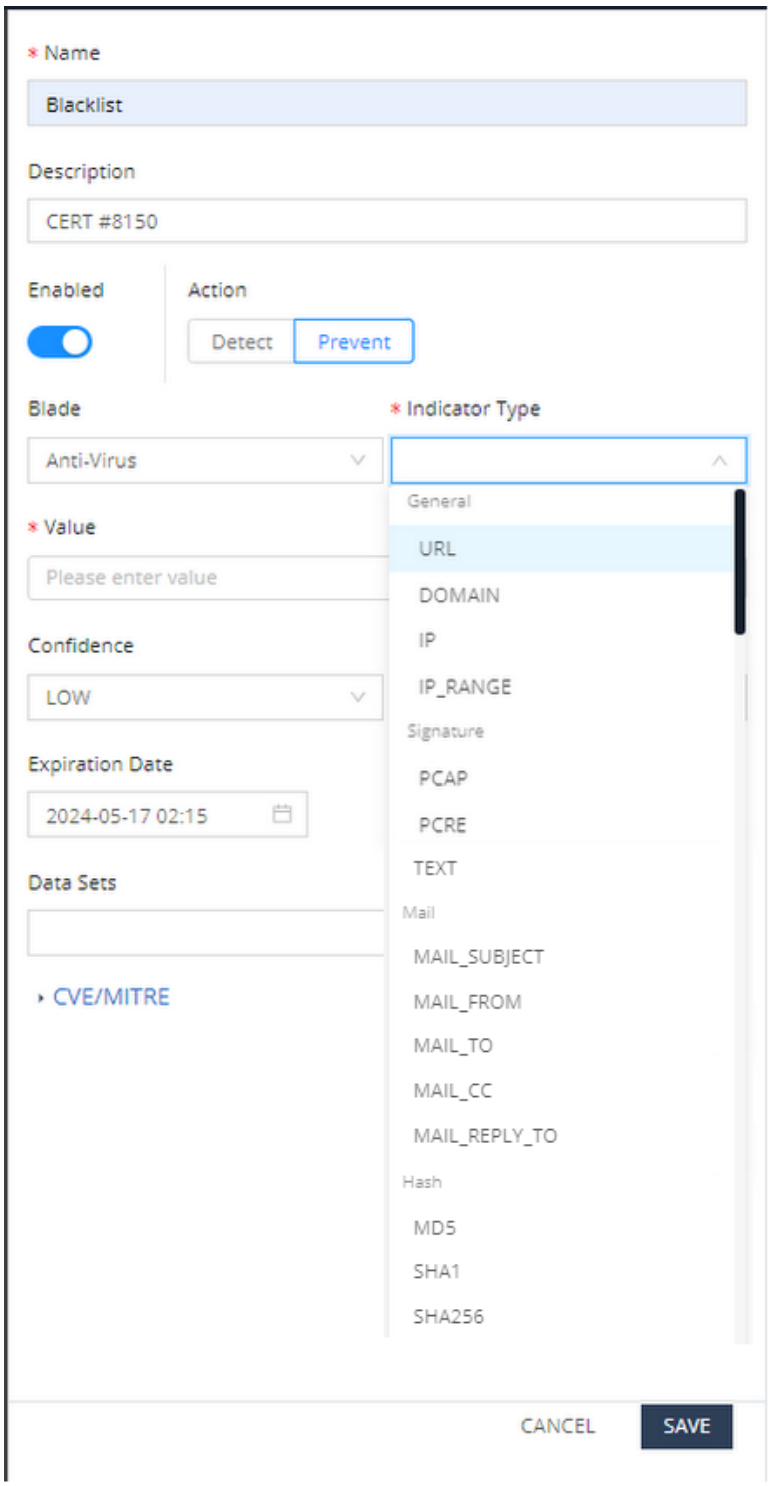


Рис. 3.3.4 – Заповнення “Indicator Type” для внесення нового індикатору до чорного списку Check Point NGFW

В якості “Indicator Type” на рис. 3.3.4 обирається “IP”, оскільки даний індикатор належить до типу IP-адрес.

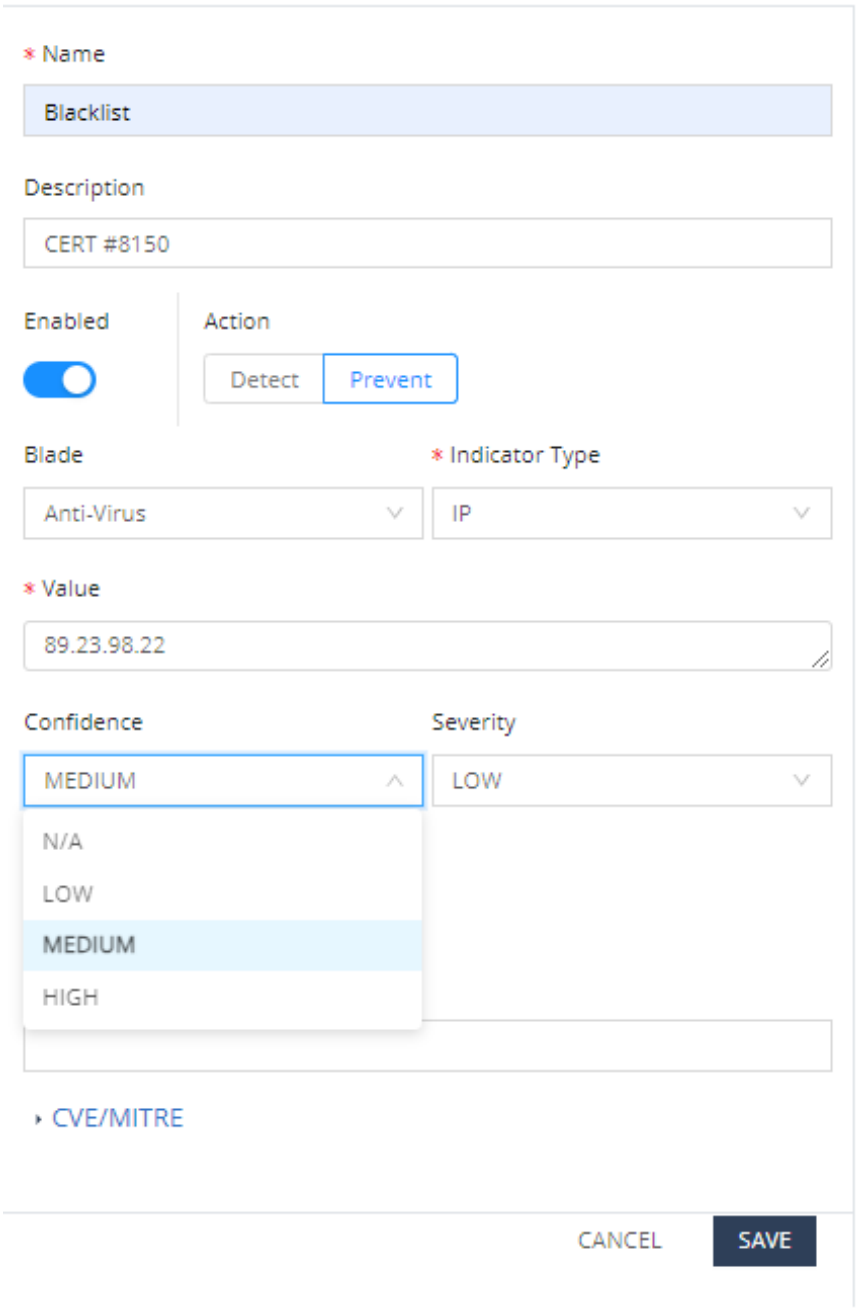


Рис. 3.3.5 – Заповнення “Value” та “Confidence” для внесення нового індикатору до чорного списку Check Point NGFW

В даному випадку в якості “Value” на рис. 3.3.5 вноситься індикатор, який буде блокуватись, а саме 89[.]23[.]98[.]22, в якості “Confidence” обирається “MEDIUM” оскільки є багаторазові підтвердження, що даний індикатор використовується для зловмисної активності даного ШПЗ.

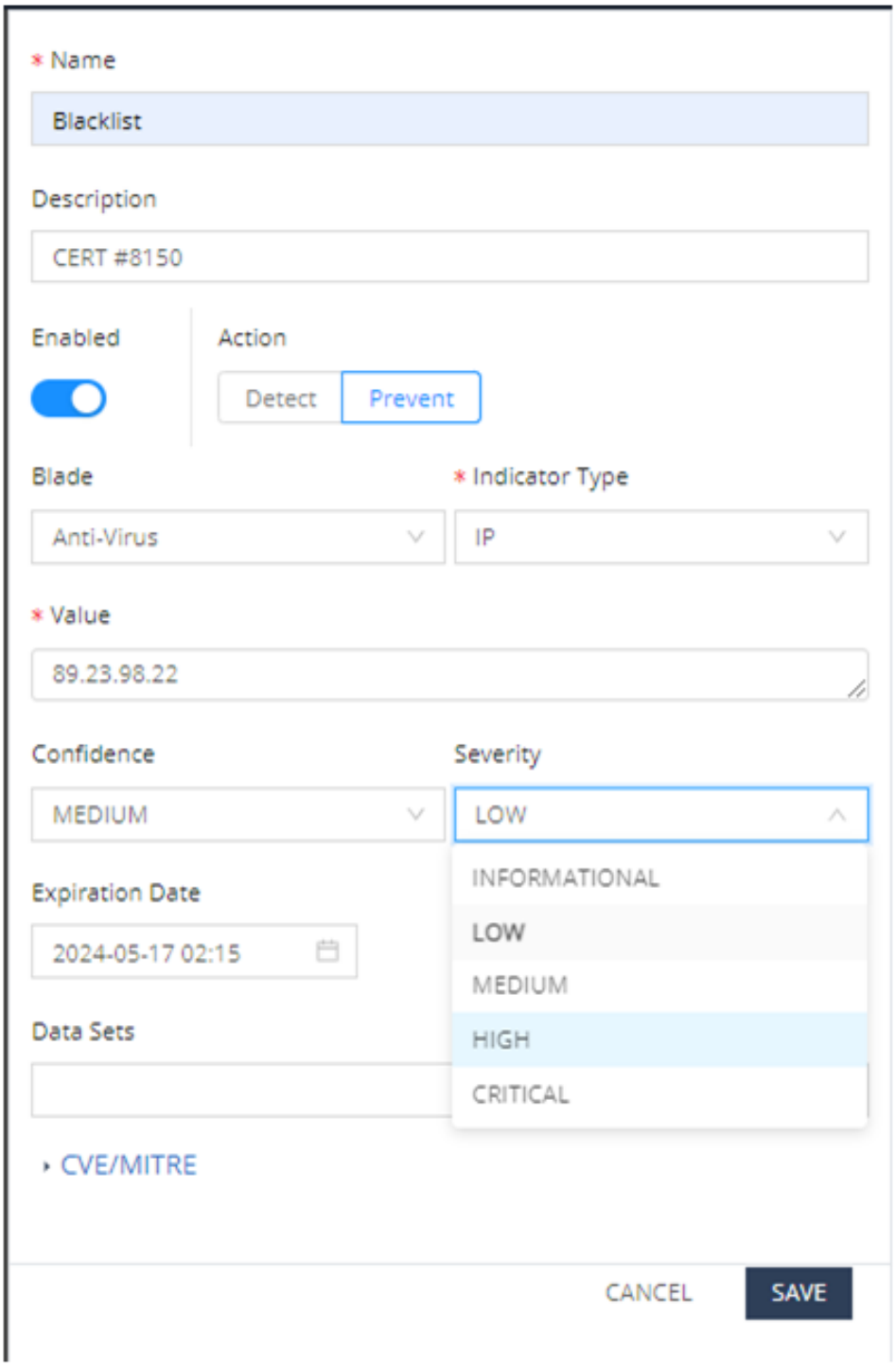


Рис. 3.3.6 – Заповнення “Severity” для внесення нового індикатору до чорного списку Check Point NGFW

У випадку “Severity” на рис. 3.3.6 обирається “HIGH”, оскільки загроза комунікації з даним індикатором несе в собі завантаження програми для віддаленого управління RemcosRAT.

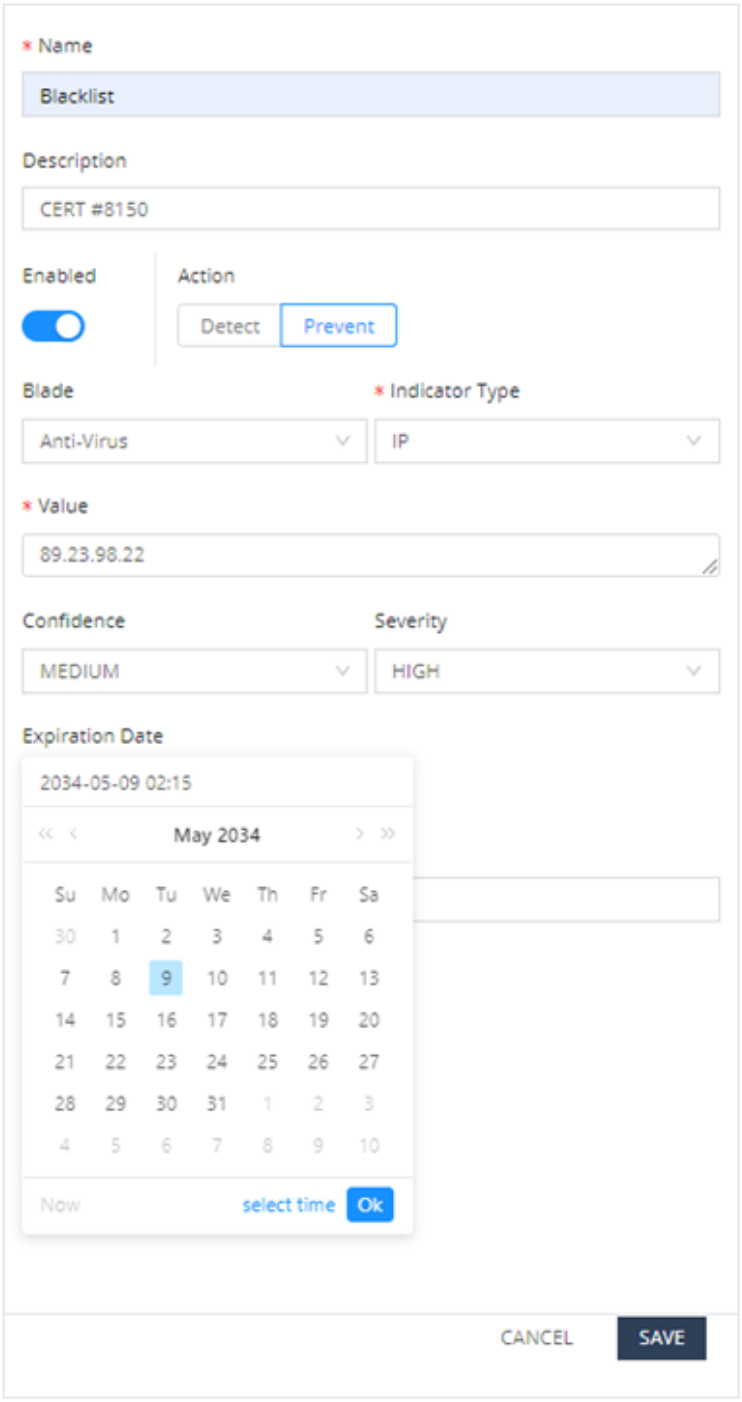


Рис. 3.3.7 – Заповнення “Expiration Date” для внесення нового індикатору до чорного списку Check Point NGFW

“Expiration Date” на рис. 3.3.7 це дата до якої буде діяти дане внесення, наприклад, якщо в якості дати вказати наступний день після внесення то після настання даної дати дане правило перестане функціонувати до ручного відновлення. В даному випадку я кості дати обирається 09.05.2034, оскільки вірогідність використання даного індикатора в легітимних цілях мало-імовірна.

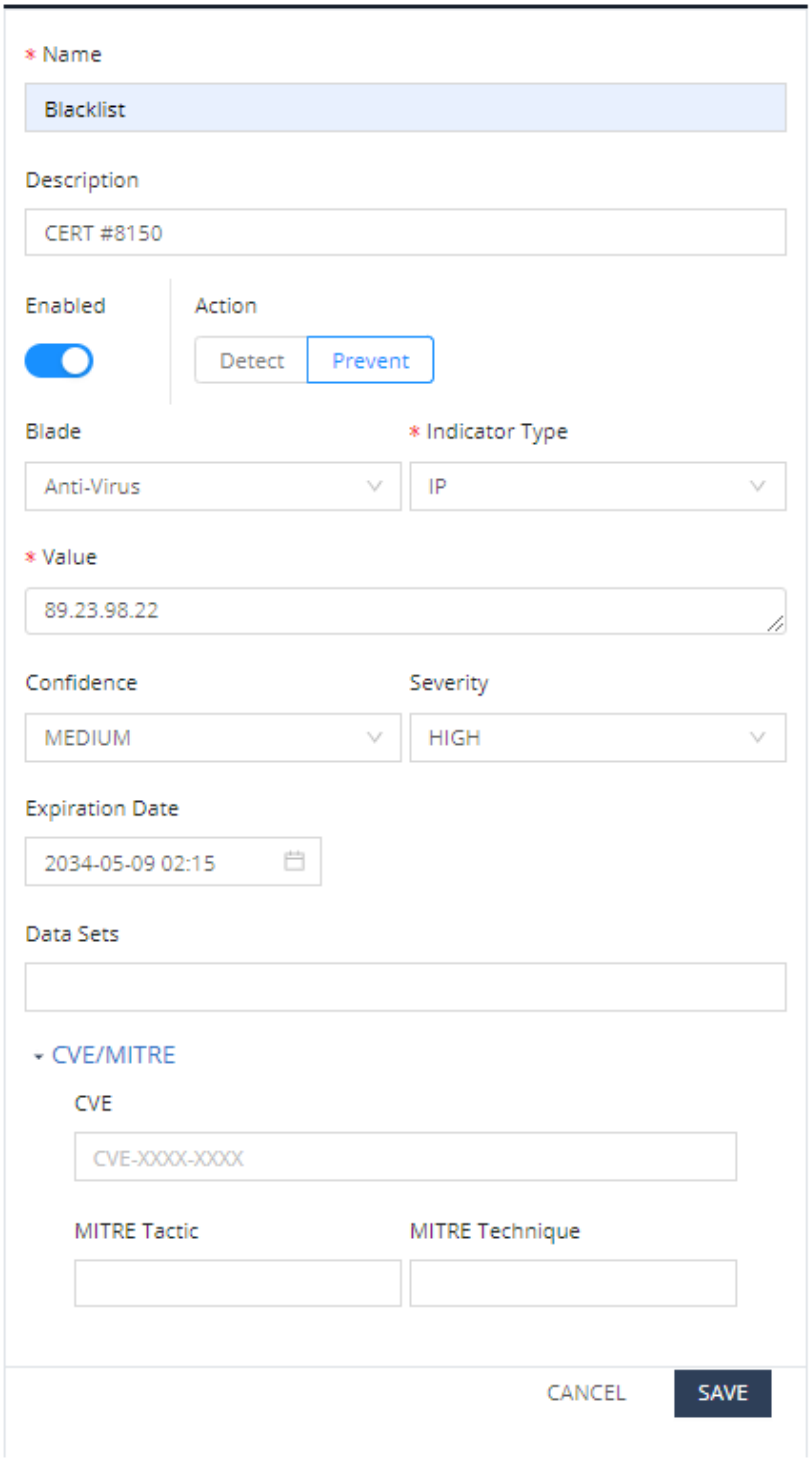


Рис. 3.3.8 – Огляд можливого заповнення “Data Sets” та “CVE/MITRE” для внесення нового індикатору до чорного списку Check Point NGFW

Також можливе внесення даних про вразливість “CVE” або тактики/техніки “MITRE” та “Data Sets”, що являє собою ще одним списком, але вже для побудови статистики, в обох варіантах в даному випадку відсутня необхідність занесення цих даних. Приклад наведено на рис. 3.3.8.

ВИСНОВКИ

В роботі проведено дослідження процесу аналізу шкідливого програмного забезпечення, визначено його мету та завдання. Сьогодні існують серйозні загрози, які несе в собі шкідливе програмне забезпечення, як великим організаціями та установам так і звичайним користувачам, з часом різноманітність даного ШПЗ збільшується, оскільки не завжди вдається вчасно виявити та заблокувати його активність через новизну або все більш витончені алгоритми дій, отже організаціям та установам потрібно покращувати засоби та методи захисту від нього. Також, спостерігається зростання ризиків для безпеки кінцевих точок організацій та установ, які посилюються недостатньою підготовленістю їх до протидії новим загрозам за допомогою існуючих платформ безпеки кінцевих точок, систем антивірусного захисту, тощо.

Було досліджено загальні типи шкідливого програмного забезпечення, а також наведено приклади з загрозами та видами збитку організаціям та установам, від зловмисної активності даних типів ШПЗ.

Проведено аналіз існуючих ручних та автоматизованих інструментів та рішень, за допомогою яких можливо виконати аналіз шкідливого програмного забезпечення з якого можливо видобути якісний результат в виді IoC`s та алгоритму дій відповідного ШПЗ, використання якого дає змогу протидіяти зловмисній активності вказаного ШПЗ. Але варто зазначити, що процедура аналізу шкідливого програмного забезпечення підходить більше для середніх та вище за розміром організацій та установ в яких наявний Security Operation Center (SOC), оскільки саме в такому випадку можливо найбільш ефективно скористатися результатами цього аналізу.

Оскільки рішення типу NGFW в більшості установ та організацій несе в собі ключову роль у захисті периметру відповідної мережі та відіграє значну роль у загальній системі забезпечення безпеки інформаційної системи організації, було проведено наглядний приклад дій по використанню процедури аналізу шкідливого

програмного забезпечення для протидії відповідного ШПЗ на прикладі кіберінциденту "Повістка до суду" – CERT-UA#8150 та рішенню Check Point NGFW.

Отже, виявлення та реагування на зловмисну активність шкідливого програмного забезпечення стало значним аспектом сучасної кібербезпеки, оскільки організації стикаються з дедалі складнішими кібератаками в яких задіяне ШПЗ. Check Point NGFW - це інтегроване рішення для захисту мережі, яке забезпечує захист від різноманітних кіберзагроз, виявляє потенційно шкідливі дії та реагує у реальному часі на них. Дане рішення також дає можливість цифрового розслідування для виявлення та аналізу потенційних загроз за допомогою Smart Console навіть без інтегрованої SIEM системи.

Таким чином, правильна реалізація процедури аналізу шкідливого програмного забезпечення та використання її результатів для рішення типу NGFW має сприяти ефективній протидії ШПЗ та захисту корпоративних інформаційних ресурсів у цілому.

ПЕРЕЛІК ПОСИЛАНЬ

1. Greenberg A. The untold story of notpetya, the most devastating cyberattack in history. *WIRED*. URL: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (date of access: 22.05.2024).

2. What is stuxnet?. *Malwarebytes*. URL: https://www.malwarebytes.com/stuxnet (date of access: 22.05.2024).

3. Newman L. H. What we know about friday's massive east coast internet outage. *WIRED*. URL: https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/ (date of access: 22.05.2024).

4. Fowler B. Google docs phishing scam: what you need to know. *Yahoo News*. URL: https://www.yahoo.com/news/google-docs-phishing-scam-know-222438992.html (date of access: 22.05.2024).

5. Greenberg A. NSA director confirms that russia really did hack the french election. *WIRED*. URL: https://www.wired.com/2017/05/nsa-director-confirms-russia-hacked-french-election-infrastructure/ (date of access: 22.05.2024).

6. "Повістка до суду": чергова цільова атака UAC-0050 з використанням RemcosRAT. Kyiv. URL: https://cert.gov.ua/article/6276567 (дата звернення: 09.05.2024).

7. What is a next generation firewall (NGFW)?. *Check Point*. URL: https://www.checkpoint.com/cyber-hub/network-security/what-is-next-generation-firewall-ngfw/ (date of access: 09.05.2024).

8. Advanced file analysis system valkyrie. *valkyrie comodo*. URL: https://valkyrie.comodo.com/ (date of access: 22.05.2024).

9. Free automated malware analysis service - powered by falcon sandbox. *Hybrid Analysis*. URL: https://www.hybrid-analysis.com/ (date of access: 22.05.2024).

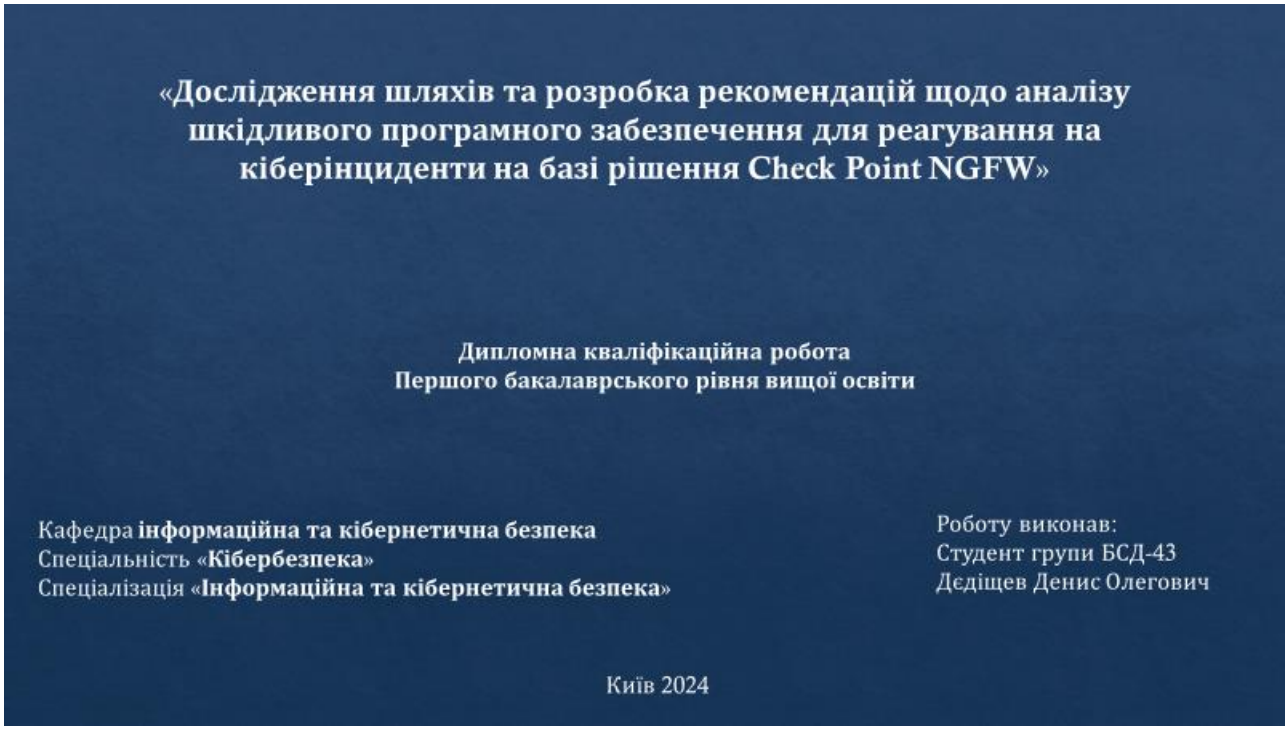
10. Lessons from the melissa virus. *ITPro Today*. URL: https://www.itprotoday.com/email-and-calendaring/lessons-melissa-virus (date of access: 22.05.2024).

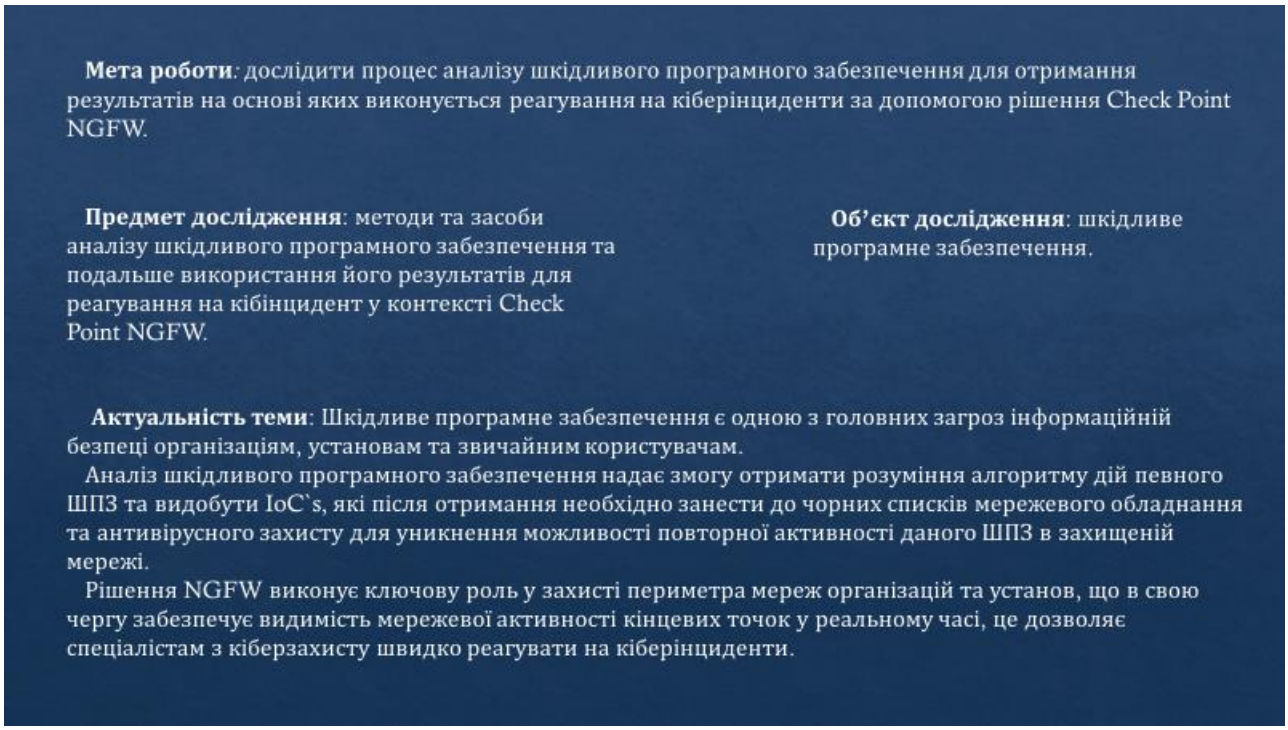
11. Sandbox triage. *Triage*. URL: https://tria.ge/ (date of access: 22.05.2024).

12. Sandbox virus total. *VirusTotal*. URL: https://www.virustotal.com/gui/home/upload (date of access: 22.05.2024).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)





Автоматизований аналіз шкідливого програмного забезпечення

Серед інструментів автоматичного аналізу шкідливого програмного забезпечення найбільш комплексним та зручним методом є використання спеціально створених для цього Sandbox`s.

Sandbox, як правило, буває у двох варіантах, тонкий клієнт та товстий клієнт, зазвичай, коли мова йде про тонкий клієнт мається на увазі веб-ресурси, які безкоштовно дають змогу завантажити файли до певного розміру до своїх Sandbox, у випадку товстого клієнту необхідно завантажити та встановити відповідне програмне забезпечення.

Triage

VALKYRIE COMODO

HYBRID ANALYSIS

VIRUSTOTAL

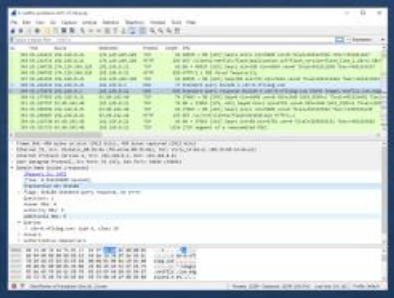
Sandbox (Пісочниця) - це ізольоване середовище з мінімальними привілеями та обмеженим доступом, зазвичай розгорнуто в віртуальному середовищі, яке використовують для виконання програм або процесів, з точки зору інформаційної безпеки, дане рішення використовують для аналізу шкідливого програмного забезпечення.

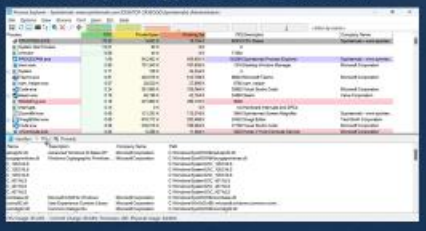
Ручний аналіз шкідливого програмного забезпечення

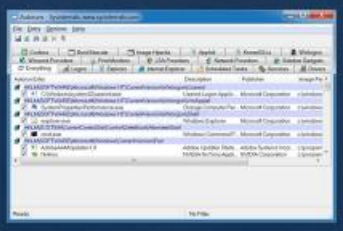
Wireshark – це програма для аналізу мережі, яка дозволяє перехоплювати та аналізувати мережевий трафік в реальному часі.

Sysinternals – це набір утиліт для адміністрування та діагностики операційних систем Windows, вони дозволяють виконувати різні завдання, такі як моніторинг системи, керування процесами та службами, аналіз файлової системи та реєстру, і багато іншого.

HashMyFiles – надає відомості про хеш-суму та інші парметри файлів.





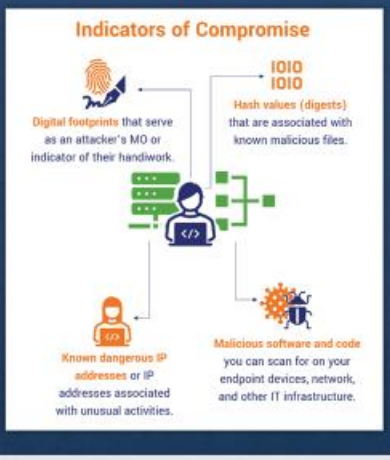


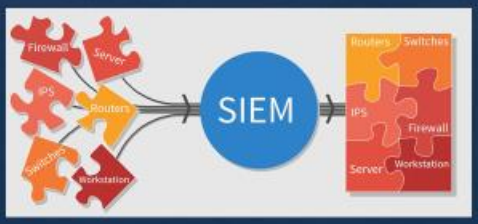
Рекомендації

Головною метою процесу аналізу шкідливого програмного забезпечення є отримання результатів у вигляді IoC`s для блокування та розуміння поведінки ШПЗ.

В залежності від інциденту, якщо воно пов'язане з ШПЗ та було проведено його аналіз, за допомогою блокування IoC`s на мережевому обладнанні, наприклад для рішень типу NGFW, а також при внесенні до антивірусних баз даних можна запобігти зловмисної активності в мережі після виконання відповідного блокування.
При розумінні поведінки ШПЗ можливо налаштувати відповідні політики для протидії його зловмисної активності.

Також, для того, щоб ефективно використати результати аналізу ШПЗ у вигляді IoC`s можливо виконати пошуки в системах типу SIEM для того щоб переконатись що зловмисна активність відсутня, або навпаки її виявити.





Висновки

Сьогодні існують серйозні загрози, які несе в собі шкідливе програмне забезпечення, як великим організаціями та установам так і звичайним користувачам, з часом різноманітність даного ШПЗ збільшується, оскільки не завжди вдається вчасно виявити та заблокувати його активність через новизну або все більш витончені алгоритми дій, отже організаціям та установам потрібно покращувати засоби та методи захисту від нього.

Також, спостерігається зростання ризиків для безпеки кінцевих точок організацій та установ, які посилюються недостатньою підготовленістю їх до протидії новим загрозам за допомогою існуючих платформ безпеки кінцевих точок, систем антивірусного захисту, тощо.

Отже, виявлення та реагування на зловмисну активність шкідливого програмного забезпечення стало значним аспектом сучасної кібербезпеки, оскільки організації стикаються з дедалі складнішими кібератаками в яких задіяне ШПЗ. Check Point NGFW - це інтегроване рішення для захисту мережі, яке забезпечує захист від різноманітних кіберзагроз, виявляє потенційно шкідливі дії та реагує у реальному часі на них. Дане рішення також дає можливість цифрового розслідування для виявлення та аналізу потенційних загроз за допомогою Smart Console навіть без інтегрованої SIEM системи.

Таким чином, правильна реалізація процедури аналізу шкідливого програмного забезпечення та використання її результатів для рішення типу NGFW має сприяти ефективній протидії ШПЗ та захисту корпоративних інформаційних ресурсів у цілому.