ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

“ТЕХНОЛОГІЯ ВИЯВЛЕННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НА БАЗІ РІШЕННЯ DEFENDER”

на здобуття освітнього ступеня магістра
зі спеціальності 125Кібербезпека
(код, найменування спеціальності)
освітньо-професійної програми Інформаційна та кібернетична безпека
(назва)

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

Владислав ГРУША

Виконав: здобувач вищої освіти групи БСДМ-62
ГРУША Владислав
(ПРІЗВИЩЕ, Ім’я)

Керівник: ГАЙДУР Галина
д.т.н, професор (ПРІЗВИЩЕ, Ім’я)

Рецензент:
(ПРІЗВИЩЕ, Ім’я)

Київ 2024

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

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

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
“___”_____2023 року

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ

Груші Владиславу Григоровичу
(прізвище, ім’я, по батькові)

1. Тема кваліфікаційної роботи:
«Технологія виявлення шкідливого програмного забезпечення на базі рішення Defender»
керівник кваліфікаційної роботи: ГАЙДУР Галина, д.т.н., професор,
(ПРІЗВИЩЕ, Ім’я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «19» жовтня 2023р. №145.

2. Строк подання студентом кваліфікаційної роботи: 15.12.2023 р.

3. Вихідні дані до кваліфікаційної роботи:
- Рішення Microsoft Defender
- Наукова та технічна література
- Документація від вендора
- Інтернет-ресурси
- Документи та міжнародні стандарти

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1. Теоретичні аспекти шкідливого програмного забезпечення
2. Огляд архітектурів та методів виявлення ШПЗ на базі рішення Defender
3. Надання практичних рекомендацій застосування рішення для виявлення тазапобігання ШПЗ
4. Перелік ілюстративного матеріалу: Презентація PowerPoint
5. Дата видачі завдання 19.10.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Дослідження актуальності питання використання рішення Defender для виявлення ШПЗ	19.10.2023 р.	
2	Аналіз наукової та технічної літератури затемою кваліфікаційної роботи	22.10.2023 р.	
3	Аналіз способів використання рішення Defender для виявлення ШПЗ	27.10. 2023р.	
4	Дослідження методів та засобів виявлення ШПЗ	03.11.2023 р.	
5	Розроблення практичних прикладів виявлення ШПЗ	15.11.2023 р	
6	Оформлення результатів дослідження.Проходження плагіату	26.11.2023 р.	
7	Підготовка доповіді до захисту.	15.12.2023 р.	

Здобувач(ка) вищої освіти _____ Владислав ГРУША

(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Галина ГАЙДУР

(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувач Груша В.Г. до захисту кваліфікаційної роботи
(прізвище та ініціали)

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

на тему: «Технологія виявлення шкідливого програмного забезпечення на базі рішення Defender».

Кваліфікаційна робота і рецензія додаються.

Директор інституту _____ Віталій САВЧЕНКО
(*підпис*) (*Ім'я, ПРІЗВИЩЕ*)

Висновок керівника кваліфікаційної роботи

Здобувач ***ГРУША Владислав*** обрав тему роботи, метою якої було дослідити використання рішення Defender для виявлення та запобіганню шкідливого програмного забезпечення. Перелік використаних джерел свідчить про вміння здобувача розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання кваліфікаційної роботи ***ГРУША Владислав*** показав гарну 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 ***ГРУШІ Владислава*** на оцінку **«добре»** та присвоїти йому кваліфікацію магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Керівник кваліфікаційної роботи Галина ГАЙДУР
(підпис) *(Ім'я, ПРІЗВИЩЕ)*
"____" _____2023 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач ***ГРУША Владислав.*** допускається до захисту даної роботи в Державній екзаменаційній комісії.

Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

_____ Галина ГАЙДУР
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу

здобувача Груші Владислава
на тему: «Технологія виявлення шкідливого програмного забезпечення на базі рішення Defender ».

Актуальність:

З огляду на постійно зростаючі загрози кібербезпеки та швидкий розвиток технологій, дослідження ефективності та можливостей технологій виявлення шкідливого програмного забезпечення стає критично важливим. Актуальність роботи підкреслена в контексті поширення ШПЗ і його вдосконалення для обходусучасних засобів захисту.

Позитивні сторони:

1. Зміст роботи відповідає завданню. Дана робота відповідає високому рівню.
2. Чітко викладено матеріали щодо аналізу шкідливого програмного забезпечення.
3. Текст викладено з додержанням встановлених норм та правил. Висновки викладено чітко та змістовно. Науково-технічна література свідчить про вміння користуватись матеріалами за темою бакалаврської роботи.

Недоліки:

1. Недостатньо приділено уваги більш просунутому аналізу шкідливих файлів.
2. Надані рекомендації є загальними та потребують допрацювань.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку «**добре»**, а здобувач **ГРУША Владислав** - присвоєння кваліфікації магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Рецензент: _____ Віктор ВИШНІВСЬКИЙ
д.т.н., професор *підпис* *Ім'я, ПРІЗВИЩЕ*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 85 сторінок, 13 рисунків, 1 таблиця, 16 джерел.

Об'єкт дослідження – процес виявлення шкідливого програмного забезпечення, зосереджений на рішенні Defender виробника Microsoft.

Предмет дослідження – технологія захисту від шкідливих файлів на базі рішення Microsoft Defender.

Мета роботи – надати практичні приклади способів використання рішення Defender для виявлення ШПЗ.

Методи дослідження – опрацювання літератури за даною темою, аналіз доступних докуметацій, огляд процесу захисту від шкіливих файлів на базі рішення Microsoft Defender Також передбачається порівняння з іншими сучасними рішеннями з області кібербезпеки.

В роботі проведено аналіз проблеми виявлення ШПЗ, використовуючи рішення Defender. Надано практичні приклади способів використання рішення Defender для виявлення ШПЗ.

Досліджено методи та засоби захисту від шкідливих файлів на базі рішення Defender.

Запропоновано варіант практичного використання рішення Defender для виявлення ШПЗ.

Визначено призначення, основні функції та склад компонентів даної технології.

На основі проведених досліджень, в роботі вказано практичний приклад способів використання рішення Defender для виявлення ШПЗ.

Галузь використання – кібербезпека корпоративної мережі.

ШКІДЛИВЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, КІБЕРБЕЗПЕКА, DEFENDER, АРХІТЕКТУРА, МЕТОДИ ТА ЗАСОБИ, ФУНКЦІЇ, ADVANCED HUNTING

ABSTRACT

Text part of the master's qualification work: 85 pages, 13 figures, 1 table, 16 sources.

Object of research - is the process of malware detection ce ntered on the Microsoft Defender solution.

Subject of the research - is the technology of protection against malicious files based on the Microsoft Defender solution.

Purpose of the research - to provide practical examples of how to use the Defender solution to detect malware.

Research methods - studying the literature on this topic, analyzing available documents, reviewing the process of protecting against malicious files based on the Microsoft Defender solution.

The paper analyzes the problem of detecting malware files using the Defender solution. Practical examples of ways to use the Defender solution to detect malware are provided.

Methods and means of protection against malicious files based on the Defender solution are investigated.

A variant of practical use of the Defender solution for detecting malware is proposed.

The purpose, main functions and composition of the components of this technology are determined.

Based on the research, the paper provides a practical example of how to use the Defender solution to detect malware.

The field of application is the cybersecurity of a corporate network.

MALWARE, CYBERSECURITY, DEFENDER, ARCHITECTURE, METHODS AND TOOLS, FUNCTIONS, ADVANCED HUNTING

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

AD – Active Directory

SOC – Security Operation Center

FP – False Positives

ADS – Alternative Data Stream

LDAP – Lightweight Directory Access Protocl

ШПЗ - шкідливе програмне забезпечення

APT – Advanced Persistent Threat

KQL – Kusto Query Language

ВСТУП

Актуальність дослідження. Швидкий темп розвитку цифрових технологій у сучасному світі супроводжується зростанням кількості кіберзагроз, зокрема шкідливого програмного забезпечення, яке завдає значних збитків користувачам та підприємствам. Охорона інформаційної безпеки стає однією з ключових проблем, і виявлення ШПЗ визначається як невід'ємна складова стратегії кібербезпеки.

Однією з передових платформ для виявлення та протидії ШПЗ є рішення Microsoft Defender. Ця система використовує передові технології, такі як машинне навчання, аналіз поведінки та інші методи, щоб надати ефективний захист від різноманітних кіберзагроз.

Основною метою є глибоке розуміння функціоналу та можливостей рішення Microsoft Defender, а також визначення його переваг та обмежень у контексті виявлення ШПЗ.

Таким чином, сучасне шкідливе програмне забезпечення часто важче виявити, воно завдає більшої шкоди і його важче видалити, ніж попередні покоління шкідливого програмного забезпечення. І немає жодних ознак того, що ця еволюція закінчується. Коли найскладніші проблеми зі зловмисним програмним забезпеченням стануть рутинною справою, чекайте на появу нових викликів.

Об’єкт дослідження – процес виявлення шкідливого програмного забезпечення, зосереджений на рішенні Defender виробника Microsoft.

Предмет дослідження – технологія захисту від шкідливих файлів на базі рішення Microsoft Defender.

Мета роботи – надати практичні приклади способів використання рішення Defender для виявлення ШПЗ.

Наукові завдання:

- провести аналіз питання щодо можливості використання рішення

Defender для виявлення ШПЗ;

- проаналізувати основні методи та алгоритми для виявлення шкідливих файлів;
- протестувати рішення Defender та порівняти його з іншими рішеннями на ринку;
- навести практичні приклади використання технології Advanced Hunting та детально описати їх.

Методи дослідження – опрацювання літератури за даною темою, аналіз доступних докуметацій, огляд процесу захисту від шкіливих файлів на базі рішення Microsoft Defender Також передбачається порівняння з іншими сучасними рішеннями з області кібербезпеки.

Практичне значення одержаних результатів полягає в тому, що це дослідження може слугувати важливим внеском у підвищення рівня кібербезпеки та розробки більш ефективних заходів захисту в інформаційно-технологічному середовищі.

РОЗДІЛ 1
ШКІДЛИВЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ТА ЗАСОБИ ЗАХИСТУ: ТЕОРІЯ, ОСОБЛИВОСТІ ТА ЙОГО ВПЛИВ НА СУЧАСНІСТЬ

1.1 Визначення шкідливого програмного забезпечення (ШПЗ) та загальнаінформація

Шкідливе програмне забезпечення представляє собою зловмисну програму або код, які завдають шкоди кінцевим пристроям. Коли пристрій потрапляє під вплив шкідливого програмного забезпечення, може виникати несанкціонований доступ, пошкодження даних або блокування пристрою до тих пір, поки не буде сплачений викуп.

Особи, що поширюють шкідливе програмне забезпечення, або кіберзлочинці, мають фінансовий стимул і використовують уражені пристрої для запуску атак. Наприклад, вони можуть отримувати банківські облікові дані, збирати й продавати особисті дані, торгувати доступом до обчислювальних ресурсів або вимагати платіжну інформацію від потенційних жертв.

Шкідливе програмне забезпечення (ШПЗ), мабуть, є однією з найбільш значущих категорій загроз для комп'ютерних систем. NIST SP 800-83 (Посібник із запобігання інцидентам, пов'язаним зі зловмисним програмним забезпеченням для настільних комп'ютерів і ноутбуків, липень 2013 року) визначає шкідливе програмне забезпечення як "програму, яка вставляється в систему, зазвичай приховано, з наміром порушити конфіденційність, цілісність або доступність даних, додатків або операційної системи жертви, або в інший спосіб дратувати чи порушувати роботу жертви". Дуже важливо розуміти загрозу, яку шкідливе програмне забезпечення становить для прикладних програм, утиліт, таких як редактори та компілятори, а також для програм на рівні ядра. Занепокоєння викликає і використання ШПЗ на скомпрометованих або шкідливих веб-сайтах і серверах, або в спеціально створених спам-

розсилках чи інших повідомленнях, які мають на меті обманом змусити користувачів розкрити конфіденційну особисту інформацію [1].

Принцип дії шкідливого програмного забезпечення. Шкідливе програмне забезпечення використовує методи, що заважають нормальному функціонуванню пристроїв. Коли кіберзлочинці отримують доступ до пристрою, використовуючи різноманітні техніки, такі як фішингові електронні листи, заражені файли, вразливості систем або програмного забезпечення, заражені USB- носії або зловмисні веб-сайти, вони використовують цю можливість для проведення додаткових атак. Ці атаки можуть включати отримання доступу до облікових записів,збір та збут особистих даних, торгівлю доступом до обчислювальних ресурсів або вимагання викупу.

Будь-хто може стати жертвою атак шкідливого програмного забезпечення. Деякі користувачі можуть знаходити способи визначити, що зловмисники намагаються використовувати шкідливе програмне забезпечення, таке як фішингові електронні листи. Проте кібератаки є складними і постійно розвиваються, щоб уникнути технологічних заходів безпеки. Шкідливі атаки можуть виглядати та функціонувати по-різному, залежно від типу шкідливого програмного забезпечення. Наприклад, жертви атак руткіта можуть іноді навіть не підозрювати про їхню наявність, оскільки цей вид шкідливого програмного забезпечення створений так, щоб якомога триваліше залишатися непоміченим.

1.2. Види ШПЗ та їхні особливості

Багато дослідників намагаються класифікувати шкідливе програмне забезпечення. Хоча може бути використаний цілий ряд аспектів, один з корисних підходів класифікує шкідливе програмне забезпечення на дві широкі категорії, засновані спочатку на тому, як воно поширюється для досягнення бажаних цілей, а потім на діях або пейлоаді, який воно виконує, коли ціль досягнута.

Механізми поширення включають зараження існуючого виконуваного

або інтерпретованого контенту вірусами, які згодом поширюються на інші системи; використання вразливостей програмного забезпечення локально або через мережу черв'яками або завантажуваними файлами для реплікації шкідливого програмного забезпечення; атаки соціальної інженерії, які переконують користувачів обійти механізми захисту, щоб встановити троянські програми або відповісти на фішингові атаки.

У попередніх підходах до класифікації шкідливих програм розрізняли ті, що потребують програми-хоста, тобто паразитичні програми, такі як віруси, і ті, що є незалежними, самодостатніми програмами, які запускаються в системі, такі як хробаки, трояни і боти. Також розрізняють шкідливе програмне забезпечення, яке не розмножується, наприклад, трояни та спам, і шкідливе програмне забезпечення, яке розмножується, зокрема віруси та черв'яки.

Дії, які виконує шкідливе програмне забезпечення після того, як воно потрапляєв цільову систему, можуть включати пошкодження системних файлів або файлів даних; крадіжку сервісу з метою перетворення системи на зомбі-агента атаки в рамкахботнету; крадіжку інформації з системи, особливо логінів, паролів або інших персональних даних за допомогою програм-шпигунів або шпигунських програм; а також приховану роботу, коли шкідливе програмне забезпечення приховує свою присутність в системі від спроб виявити і заблокувати його[16].

Типи шкідливого програмного забезпечення. Безумовно існують різні типи шкідливого програмного забезпечення. Використаємо найпоширенішу класифікацію і опишемо їх:

- Фішингові атаки спрямовані на викрадення делікатної інформації, маскуючи електронну пошту, веб-сайти, текстові повідомлення або інші форми електронного спілкування під надійне джерело. Вони слугують механізмом для розповсюдження шкідливого програмного забезпечення. Під час таких атак зловмисники зазвичай викрадають імена користувачів, паролі, дані кредитних карток і банківську інформацію. У результаті може статися крадіжка ідентифікаційних даних або грошей безпосередньо з банківського рахунку або

кредитної картки особи.

Наприклад, кіберзлочинець може замаскуватися під відомий банк і надіслати електронний лист з оповіщенням про те, що обліковий запис особи заблоковано через підозрілі дії, закликаючи її перейти за посиланням для вирішення проблеми. Коли особа переходить за посиланням, інсталюється шкідливе програмне забезпечення.

- Шпигунські програми. Шпигунське програмне забезпечення інсталюється на пристрій без згоди користувачів або відповідного повідомлення. Після інсталяції воно може відстежувати поведінку користувачів в Інтернеті, збирати делікатну інформацію, змінювати параметри пристрою та зменшувати його продуктивність.
- Рекламне програмне забезпечення. Рекламне програмне забезпечення, подібно до шпигунського, інсталюється на пристрій без згоди користувача. Але воно призначене для показу агресивної реклами, зазвичай у формі спливаючих оголошень. Так зловмисник заробляє на їх кліках. Ці рекламні оголошення часто сповільнюють продуктивність пристроїв. Небезпечніші типи рекламного програмного забезпечення також передбачають інсталяцію додаткової програми та зміну параметрів браузера, що робить пристрій уразливим доінших зловмисних атак.
- Віруси. Віруси порушують нормальну роботу пристроїв, записуючи, пошкоджуючи або видаляючи дані на них. Зазвичай вони поширюються на інші пристрої після того, як введені в оману користувачі відкривають зловмисні файли.
- Експлойти та набори експлойтів. Експлойти обходять засоби захисту комп’ютера й уражають його, використовуючи вразливості програмного забезпечення. Кіберзлочинці сканують застарілі системи з критичними вразливостями, а потім використовують їх для розгортання шкідливого програмного забезпечення. Додавши код оболонки в експлойт, кіберзлочинці можуть завантажувати більше шкідливого програмного забезпечення, щоб уражати пристроїта проникати в системи організацій.

Набори експлойтів включають кілька експлойтів, які сканують різні типи вразливостей програмного забезпечення. Якщо такі виявлено, набори розгортають додаткове шкідливе програмне забезпечення. Вони можуть уражати таке програмне забезпечення, як Adobe Flash Player, Adobe Reader, браузери, Oracle Java та Sun Java. Angler/Axpergle, Hubtrino й Axtrino – це поширені типи наборів експлойтів.

Експлойти та набори експлойтів зазвичай потрапляють у мережу або на пристрої через зловмисні веб-сайти чи вкладення електронної пошти. Іноді вони також приховуються в рекламних оголошеннях на надійних веб-сайтах.

- Безфайлове шкідливе програмне забезпечення. Цей тип шкідливого програмного забезпечення, якому не потрібні файли, як-от уражене вкладення електронної пошти, щоб потрапити в мережу. Наприклад, воно може поширюватись у вигляді зловмисних мережевих пакетів, які інсталюють шкідливе програмне забезпечення виключно в пам’ять ядра, використовуючи вразливості системи. Безфайлові загрози надзвичайно важко виявляти та видаляти, оскільки більшість антивірусних програм не передбачають сканування мікропрограм.

- Шкідливе програмне забезпечення на базі макросів. Відомо, що макроси – способи швидкої автоматизації поширених завдань. Це шкідливе програмне забезпечення використовує макроси, щоб уражати вкладення електронної пошти та ZIP-файли. Щоб ввести користувачів в оману й змусити їх відкрити ці файли, кіберзлочинці часто маскують їх під рахунки, чеки або юридичну документацію. У минулому шкідливе програмне забезпечення на базі макросів використовувалося частіше, оскільки макроси запускались автоматично під час відкриття документа. Але в останніх версіях Microsoft Office макроси вимкнено за замовчуванням. Це означає, що зловмиснику, який уражає пристрій таким способом, потрібно переконати користувача ввімкнути макроси.

- Зловмисні програми з вимогою викупу. Зловмисні програми з вимогою викупу – це програми, створені зловмисниками, які погрожують

жертві знищити або заблокувати доступ до важливих даних, доки вона не сплатить викуп. Керовані зловмисні програми з вимогою викупу уражають організації за допомогою поширених неправильних конфігурацій систем і засобів захисту. Вони проникають у систему організації, переміщуються в корпоративній мережі й адаптуються до середовища та вразливостей. Щоб отримати доступ до корпоративної мережі та поширити зловмисну програму з вимогою викупу, кіберзлочинці часто крадуть облікові дані справжніх працівників, видають себе за нихі отримують доступ до їхніх облікових записів.

За допомогою керованих зловмисних програм із вимогою викупу злочинці уражають великі організації, оскільки ті можуть виплачувати більші викупи (часто мільйони доларів), ніж середньостатистичні користувачі. Через серйозні ризики, пов’язані з такими масштабними порушеннями, багато організацій сплачують викуп, щоб уникнути витоку делікатних даних або ризику подальших атак кіберзлочинців. Однак це не гарантує їм захисту від жодного із зазначених наслідків.

Що більше розвиваються керовані зловмисні програми з вимогою викупу, то організованішими стають кіберзлочинці. На практиці багато зловмисних програм із вимогою викупу тепер використовуються як модель служби. Це означає, що одна група кіберзлочинців самостійно створює зловмисні програми з вимогою викупу, а потім наймає інших афілійованих осіб, щоб зламати корпоративну мережу й інсталювати ці програми. Потім ці дві групи ділять прибуток відповідно до погодженої суми.

- Руткіти. Кіберзлочинці використовують руткіти, щоб якнайдовше приховувати шкідливе програмне забезпечення на пристрої (іноді навіть роками) і постійно викрадати інформацію та ресурси. Руткіт перехоплює контроль над стандартними процесами операційної системи та може змінювати інформацію на ваших пристроях. Наприклад, на ураженому руткітом пристрої може відображатися неточний список активних програм. За допомогою руткітів кіберзлочинці можуть отримати права адміністратора або розширені права, що дає їм змогу повністю контролювати пристрій і вчиняти потенційно зловмисні

дії, зокрема викрадати дані, шпигувати за жертвою й інсталювати додаткове шкідливе програмне забезпечення.

- Атаки на ланцюжки постачання. Цей тип шкідливого програмного забезпечення націлений на розробників і постачальників ПЗ та дає змогу отримати доступ до вихідних кодів, збірок або механізмів оновлення у звичайних програмах. Коли кіберзлочинці виявляють ненадійний мережевий протокол, незахищену інфраструктуру сервера або проблеми в програмуванні, вони проникають у мережу, змінюють вихідні коди та приховують шкідливе програмне забезпечення в збірках і пакетах оновлення.

- Шахрайство з технічною підтримкою. Шахрайство з технічною підтримкою – це поширена проблема в багатьох галузях. Зловмисники використовують тактику залякування, щоб змусити користувачів оплатити непотрібні послуги технічної підтримки, які пов’язані з усуненням вигаданих проблем із пристроями, платформами або програмним забезпеченням. Наприклад, кіберзлочинці можуть зателефонувати користувачеві, видаючи себе за працівника компанії з розробки програмного забезпечення. Завоювавши довіру потенційної жертви, вони спонукають її інсталювати програми або надати віддаленийдоступ до її пристроїв.

- Троянське програмне забезпечення. Принцип його дії: користувач ненавмисно завантажує його під виглядом надійних файлів або програм. Після завантаження може трапитися таке:

  - завантаження й інсталяція додаткового шкідливого програмного забезпечення,як-от вірусів або хробаків;
  - використання ураженого пристрою для шахрайства за допомогою повторюваних кліків;
  - запис натискання клавіш і відвіданих веб-сайтів;
  - надсилання зловмиснику інформації (наприклад, паролів, облікових даних і журналу браузера) про уражений пристрій;
  - установлення кіберзлочинцем контролю над ураженим пристроєм.

- Небажане програмне забезпечення. Якщо на пристрої є небажане програмне забезпечення, користувач може спостерігати зміни в користуванні браузером і керуванні завантаженнями й інсталяціями. Крім того, він може отримувати оманливі повідомлення та виявляти неавторизовані змінив параметрах пристрою. Деяке небажане програмне забезпечення входить у комплектпрограмного забезпечення, яке мають намір завантажити користувачі.
- Хробаки. Хробаки здебільшого містяться у вкладеннях електронної пошти, текстових повідомленнях, програмах для обміну файлами, соціальних мережах, мережевих папках і на знімних дисках, а також поширюються мережею, використовуючи вразливості та копіюючи себе. Залежно від типу хробака він може викрасти делікатну інформацію, змінити параметри безпеки або обмежити доступ до файлів.
- Криптомайнери. Зі зростанням популярності криптовалют зловмисники все частіше вдаються до криптомайнінгу. Криптомайнери використовують обчислювальні ресурси пристроїв для видобування криптовалют. Ураження цим типом шкідливого програмного забезпечення часто починається з вкладення електронної пошти або веб-сайту, який додає зловмисні програми до пристроїв, використовуючи вразливості в браузерах або можливості електронної обробки даних.

Криптомайнери використовують складні математичні обчислення та реєстр блокчейну, щоб викрадати обчислювальні ресурси, які дають їм змогу створювати нові монети. Криптомайнінг базується на можливостях електронної обробки значної кількості даних, однак дає змогу викрадати відносно невелику кількість криптовалют. Тому кіберзлочинці часто працюють у командах, щоб максимально збільшити та розділити прибуток.

Однак не всі криптомайнери – кіберзлочинці. Іноді як окремі користувачі, так іцілі організації купують апаратне забезпечення й електронні потужності та займаються законним криптомайнінгом. Процес стає незаконним, якщо кіберзлочинець таємно проникає в корпоративну мережу та використовує можливостіелектронної обробки даних для видобування криптовалют [2].

1.3. Історія та еволюція ШПЗ

Історія шкідливого коду. Хоча за останні кілька років ми стали свідками величезного зростання кількості атак на шкідливий код, шкідливе програмне забезпечення, безумовно, не є новим. Зловмисники десятиліттями створюють високоефективні шкідливі програми. Однак, завдяки постійному еволюційному вдосконаленню можливостей цих інструментів атаки та швидкому поширенню Інтернету в усі куточки нашої економіки, сьогоднішній шкідливий код має набагато більший вплив, ніж атаки минулих років. Розглянемо минуле, щоб отримати уявлення про коріння шкідливого коду і зрозуміти, в якому напрямку ці інструменти рухаються в майбутньому.

Рання історія комп'ютерних вірусів. Десь у 1962 році дослідники з Bell Labs Віктор Висоцький, Дуглас Макілрой та Роберт Морріс-старший придумали комп'ютерну гру, яку назвали "Дарвін". У цій грі гравці повинні були писати комп'ютерні програми, які боролися за домінування у визначеній області пам'яті. Як описано в журнальній статті 1972 року, метою гри було виживання; програми ("організми") мали можливість "вбивати" одна одну, а також могли створювати свої копії. Ця стаття є найбільш раннім опублікованим ресурсом, який ми можемо зустріти, що використовує термін "вірус" в контексті самовідтворюваного програмного забезпечення. Зокрема, в тексті згадується, що один з гравців "винайшов вірусний незнищенний організм", який зміг виграти кількаігор завдяки тому, як він захищався від атак ворожих програм.

Згадка про вірус у грі Дарвіна не зовсім відповідає нашому розумінню того, що таке традиційний вірус, але вона дає уявлення про походження ранніх програм, що самовідтворюються. Стаття, опублікована в 1984 році А. К. Дьюдні, популяризувала версію Дарвіна під назвою "Війна за ядро". У грі Дьюдні комп'ютерні програми "переслідують одна одну від адреси до адреси.... Іноді вони йдуть на розвідку ворога, іноді обрушують на нього шквал числових бомб, іноді копіюють себе, щоб уникнути небезпеки або зупиняються, щоб виправити пошкодження".

Як і сучасні віруси, програми в Core War і Darwin були розроблені з

урахуванням реплікації, хоча вони не мали паразитичних властивостей, які ми звикли асоціювати з типовими зразками вірусів сьогодні. Першою підтвердженою реалізацією коду, що самовідтворюється, який існував у природі як частина програми-хазяїна, був PERVADE, написаний Джоном Вокером у 1975 році. PERVADE був підпрограмою загального призначення, яку могла викликати будь-якапрограма, що потребувала можливості розмноження.

За словами Вокера, коли викликали PERVADE, "вона створювала незалежний процес, який, поки основна програма займалася своїми справами, перевіряв усі каталоги, доступні для її виклику. Якщо каталог не містив копії програми або містив стару версію, PERVADE копіював версію, що виконувалася, до цього каталогу".

Напевно, саме тому вони назвали його PERVADE; він проникає в систему, використовуючи цю техніку. Єдиною відомою програмою, яка містила PERVADE, була реалізація популярної гри ANIMALWalker, в якій комп'ютер намагається вгадати, яку тварину має на увазі гравець. Версія гри Вокера була значно кращою за багато інших версій, і люди продовжували просити у нього копії. Шукаючи інноваційний спосіб розповсюдження програмного забезпечення, він поєднав ANIMAL з програмою PERVADE. Отримана програма мала вірусні властивості, що дозволяло їй поширюватися з каталогу в каталог.

Більше того, коли користувачі обмінювалися касетами, що містили "заражені" копії гри, вона поширювалася на інші системи. Хоча в той час люди не використовували слово "вірус" для опису такого програмного забезпечення, зв'язок зцим терміном все ж таки існував: Вихідний код програми містив змінну на ім'я VIRUS, яка контролювала, чи слід активувати процедуру PERVADE.

Коротка історія хробаків. Хробаки - це неприємно, але вони точно не нові. Значна частина раннього Інтернету була виведена з ладу хробаком Морріса ще в листопаді 1988 року , але це був навіть не перший хробак. У 1971

році в компанії Bolt Beranek and Newman (BBN) дослідник на ім'я Боб Томас створив програму, яка могла переміщатися через мережу систем управління повітряним рухом - вражаючу мішень для такого раннього зразка. Так звана програма Томаса Creeper переходила від системи до системи, переміщуючисвій код між машинами, намагаючись допомогти авіадиспетчерам керувати своєю роботою.

Однак, на відміну від хробаків, Creeper не встановлював кілька своїх копій на кількох об'єктах; він просто мандрував мережею, намагаючись видалити себе з попередніх систем у міру свого подальшого поширення. Роками пізніше перший справжній хробак (тобто код, що самовідтворюється і поширюється мережею) був винайдений геніальними людьми з Xerox PARC. Так, ті самі люди, які створили лазерні принтери, графічний інтерфейс, мишу та багато інших комп'ютерних гаджетів, якими ми користуємося щодня, також створили першого відомого справжнього хробака. Однак вони не планували використовувати черв'яків як зловмисні інструменти. Двоє дослідників компанії Xerox на ім'я Джон Ф. Шох та Джон А. Хупп просто думали про хробаків як про напрочуд ефективний спосіб розповсюдження програмного забезпечення в системах. Звичайно, вони мали рацію. На жаль, на початку 1980-х років їхній перший дослідницький хробак випадково вирвався з полону і почав поширюватися мережею їхньої власної лабораторії Xerox, що стало зловісною ознакою прийдешніх черв'яків. Сьогодні зловмисники використовують ефективність черв'яків, щоб поширювати шкідливе програмне забезпечення далеко і широко.

Випуски черв'яків дійсно прискорилися наприкінці 1990-х років і протягом цього десятиліття. Атака Melissa у березні 1999 року та атакаLove Bug у травні 2000 року призвели до того, що багато компаній були повністю відключені від Інтернету на день чи два. Хоча більшість людей називають Melissa і Love Bug вірусами, насправді вони були набагато більше схожі на черв'яків, які нестримно поширювалися через Інтернет. Зовсім недавно ми бачили хробаків Code Red і Nimda, кожен з яких скомпрометував кілька сотень

тисяч комп'ютерів у 2001 році. До сьогодні зловмисники по всьому світу вигадують нові і більш хитромудрі рецепти черв'яків [3].

Характер сучасного шкідливого програмного забезпечення. Якщо ранні шкідливі програми, як правило, використовували один засіб поширення для доставки одного пейлоаду, то з розвитком ми спостерігаємо зростання кількості змішаних шкідливих програм, які включають в себе ряд механізмів поширення і пейлоадів, що збільшує їх здатність поширюватися, приховуватися і виконувати ряд дій на цілях. Змішана атака використовує кілька методів зараження або розповсюдження, щоб максимізувати швидкість зараження і серйозність атаки. Деякі шкідливі програми навіть підтримують механізм оновлення, який дозволяє їм змінювати діапазон розповсюдження і використовувані пейлоади після розгортання.

Набори для атак. Спочатку розробка та розгортання шкідливого програмного забезпечення вимагала від авторів значних технічних навичок. Ситуація змінилася з появою наборів інструментів для створення вірусів на початку 1990-х років, а пізніше - більш загальних наборів для атак у 2000-х роках.

Це значно полегшило розробку та розгортання шкідливого програмного забезпечення. Ці набори інструментів, часто відомі як кримінальні програми, тепер включають різноманітні механізми розповсюдження та модулі пейлоаду, які навіть новачки можуть комбінувати, вибирати та розгортати.

Їх також можна легко адаптувати до останніх виявлених вразливостей, щоб використати вікно можливостей між публікацією вразливості та широким розповсюдженням патчів для її закриття. Ці набори значно розширили коло зловмисників, здатних розгортати шкідливе програмне забезпечення. Хоча шкідливе програмне забезпечення, створене за допомогою таких наборів, як правило, менш складне, ніж розроблене з нуля, величезна кількість нових варіантів, які можуть бути створені зловмисниками, що використовують ці набори, створює значну проблему для тих, хто захищає системи від них.

Яскравим прикладом такого набору є інструментарій Zeus, який був

використаний для створення широкого спектру дуже ефективного, краденого шкідливого програмного забезпечення, що полегшує цілий ряд злочинних дій, зокрема, перехоплення та використання банківських облікових даних.

Набір експлойтів Angler, вперше помічений у 2013 році, був найактивнішим у 2015 році, часто розповсюджувався через шкідливу рекламу, яка використовувала вразливості Flash. Він є складним і технічно досконалим як у виконанні атак, так і в контрзаходах, що застосовуються для протидії виявленню.

Існує низка інших наборів для атак, які активно використовуються, хоча конкретні набори змінюються з року в рік, оскільки зловмисники продовжують розвивати та вдосконалювати їх.

Джерела атак. Ще однією значною зміною в розвитку шкідливого програмного забезпечення за останні кілька десятиліть став перехід від індивідуальних зловмисників, часто мотивованих продемонструвати свою технічну компетентність своїм колегам, до більш організованих і небезпечних джерел атак. До них відносяться політично мотивовані зловмисники, злочинці та організована злочинність; організації, які продають свої послуги компаніям і державам, а також національні урядові установи. Це суттєво змінило наявні ресурси та мотивацію для поширення шкідливого програмного забезпечення і призвело до розвитку великої підпільної економіки, пов'язаної з продажем наборів для атак, доступом до скомпрометованих комп'ютерів та викраденої інформації [4].

Характерною рисою сучасного шкідливого програмного забезпечення, яка найбільше відрізняє його від попередніх поколінь шкідливих програм, є ступінь йогокастомізації.

Для зловмисників стало тривіальною справою створення власного шкідливого програмного забезпечення шляхом придбання наборів інструментів, таких як Zeus, SpyEye та Poison Ivy, та налаштування шкідливого програмного забезпечення, створеного за допомогою цих наборів, відповідно до своїх індивідуальних потреб. Багато з цих інструментів доступні для

придбання, інші - з відкритим вихідним кодом,і більшість з них мають зручний інтерфейс, що дозволяє некваліфікованим зловмисникам легко створювати індивідуальні, високопродуктивні шкідливі програми.

Ось приклад того, що може зробити набір інструментів для створення шкідливого програмного забезпечення, проілюстрований тим, як працює отримана атака.

1. Інструментарій розсилає користувачам спам, намагаючись обманом змусити їхвідвідати певний веб-сайт.

2. Користувачі переходять на веб-сайт, який містить шкідливий вміст, наданийнабором.

3. Веб-сайт заражає комп'ютери користувачів троянськими програмами (наданими інструментарієм), використовуючи вразливості в операційних системах комп'ютерів.

4. Троянські коні встановлюють інструменти зловмисників, такі як реєстраторинатискання клавіш і руткіти (надаються в наборі).

Багато зловмисників додатково налаштовують своє шкідливе програмне забезпечення, підлаштовуючи кожен екземпляр шкідливого програмного забезпечення під конкретну людину або невелику групу людей.

Наприклад, багато зловмисників збирають інформацію через соціальні мережі, а потім використовують цю інформацію про приналежність і стосунки для створення досконаліших атак за допомогою соціальної інженерії. Іншими прикладами є часте використання фішингових атак типу "спис", тобто цільових фішингових атак, і вейлінг атак, тобто фішингових атак типу "спис", спрямованих на керівників та інших осіб, які мають доступ до інформації, що представляє особливий інтерес або цінність.

Кастомізація шкідливого програмного забезпечення створює значні проблеми для його виявлення, оскільки значно збільшує різноманітність шкідливих програм, які антивірусне програмне забезпечення та інші засоби контролю безпеки повинні виявляти і блокувати. Коли зловмисники здатні надсилати унікальну атаку кожній потенційній жертві, не дивно, що засоби

контролю безпеки, такі як антивірусне програмне забезпечення, не встигають за ними. Пом'якшення наслідків включає в себе підхід глибокого захисту з використанням декількох різних методів виявлення, щоб збільшити ймовірність того, що хоча б один з них зможе виявити зловмисну поведінку кастомізованого шкідливого програмного забезпечення.

Окрім кастомізації, ще однією важливою характеристикою сучасного шкідливого програмного забезпечення є його прихований характер. На відміну від більшості шкідливих програм кілька років тому, які, як правило, було легко помітити, більшість сучасних шкідливих програм спеціально розроблені для тихого, повільного поширення на інші комп'ютери, збираючи інформацію протягом тривалого періоду часу і, зрештою, призводячи до витоку конфіденційних даних та інших негативних наслідків[16].

Для позначення таких типів шкідливих програм зазвичай використовується термін "сучасні постійні загрози" (APT). Сценарій атаки, описаний у блоці вище, міг би бути прикладом просунутої постійної загрози, якби вона була прихованою. APT можуть вести спостереження тижнями, місяцями або навіть роками, потенційно завдаючи значної шкоди організації за допомогою лише однієї компрометації. Також APT-атаки, як відомо, важко видалити з комп'ютерів, часто вимагаючи перевстановлення операційної системи та додатків, а також відновлення всіх даних з відомих надійних резервних копій.

Таким чином, сучасне шкідливе програмне забезпечення часто важче виявити, воно завдає більшої шкоди і його важче видалити, ніж попередні покоління шкідливого програмного забезпечення. І немає жодних ознак того, що ця еволюція закінчується. Коли найскладніші проблеми зі зловмисним програмним забезпеченням стануть рутинною справою, чекайте на появу нових викликів [4].

1.4. Вплив ШПЗ: наслідки та потенційні загрози

Економічні та соціальні наслідки від шкідливого програмного забезпечення (ШПЗ) можуть бути значними і варіюватися залежно від конкретних ситуацій та обставин. Ось загальна інформація, але для конкретних деталей рекомендуєтьсявивчити актуальні джерела.

Економічні Наслідки:

- Фінансові Втрати: Поширення ШПЗ може призвести до великих фінансових втрат для компаній та індивідуальних користувачів, зокрема через втрату конфіденційної інформації, фінансових відомостей та доступу до банківських рахунків.
- Втрати Продуктивності: Атаки ШПЗ можуть призвести до витрат часу та зусиль на відновлення роботи інфраструктури, вирішення проблем безпеки та втрати продуктивності.
- Зниження Довіри: Великі атаки можуть призвести до зменшення довіри споживачів та партнерів до певних компаній чи сервісів.

Соціальні Наслідки:

- Втрати Приватності: ШПЗ може призвести до витоку особистих даних, порушення конфіденційності та втрати особистої приватності користувачів.
- Злочинні Дії: Використання ШПЗ для кіберзлочинів, таких як кібершантаж, крадіжка особистих даних або атаки на критичну інфраструктуру, може мати серйознісоціальні наслідки.
- Поширення Дезінформації: ШПЗ може використовуватися для поширення дезінформації через атаки на медіа, соціальні мережі та інші засоби комунікації [5].

Технології посилюватимуть нерівність, а ризики кібербезпеки залишатимутьсяпостійним предметом занепокоєння.

Для країн, які можуть собі це дозволити, новітні технології забезпечать часткове вирішення низки нових кризових ситуацій - від протидії новим

загрозам здоров'ю і дефіциту медичної допомоги до посилення продовольчої безпеки і пом'якшення наслідків зміни клімату.

Для тих, хто не зможе, нерівність і розбіжності зростатимуть. У всіх економіках ці технології також несуть ризики - від поширення дезінформації до некерованої швидкої плинності кадрів як серед "синіх", так і серед "білих комірців".

Однак швидкий розвиток і впровадження нових технологій, які часто супроводжуються обмеженими протоколами, що регулюють їх використання, створює свій власний набір ризиків.

Дедалі тісніше переплетення технологій з критично важливим функціонуванням суспільства наражає населення на прямі внутрішні загрози, в тому числі й ті, що мають на меті підірвати суспільне функціонування.

Поряд зі зростанням кіберзлочинності, спроби порушити роботу критично важливих технологічних ресурсів і послуг стануть більш поширеними: очікуються атаки на сільське і водне господарство, фінансові системи, громадську безпеку, транспорт, енергетику і побутову, космічну і підводну комунікаційну інфраструктуру.

Технологічні ризики не обмежуються лише діями зловмисників. Складний аналіз великих масивів даних дозволить зловживати персональною інформацією через законні правові механізми, послаблюючи індивідуальний цифровий суверенітет і право на недоторканність приватного життя навіть у добре регульованихдемократичних режимах.

На рисунку 1.1 ми можемо спостерігати топ 5 ризиків які проявляються в даний час, відсортовані в залежності від впливу на світ.

Кібератаки на критичну інфраструктуру займають п'яте місце в цьому списку.

Рис. 1.1. Найбільш розповсюджені ризики сьогодення

На рисунку 1.2 надана інформація про найвпливовіші ризики, які є прогнозованими на наступні 2 роки та 10 років.

Прогнозовано, кіберзлочини матимуть великий вплив як в найбільші 2 роки, так і в наступні 10 років.

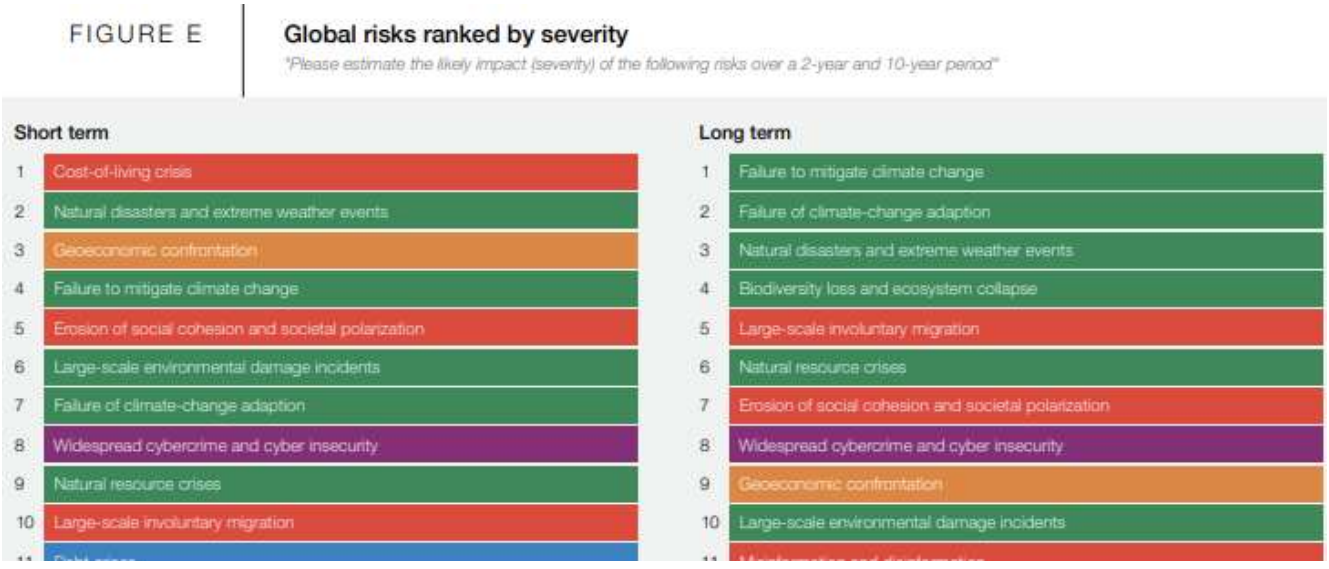


Рис. 1.2. Найвпливовіші ризики, які прогнозуються на наступні 2 та 10 років

Зростаючий компроміс між інноваціями та безпекою. Дані є важливим фактором виробництва, а їх збір і потоки необхідні длястимулювання інновацій для підвищення економічної продуктивності (включаючи автоматизацію), а також для суспільно корисного використання. Більш широке

та інноваційне застосування штучного інтелекту та інших новітніх технологій вимагатиме міжгалузевої та державно-приватної агрегації даних.

Централізація і консолідація деяких видів даних може надати конкурентну перевагу економіці, наприклад, завдяки поліпшенню стану здоров'я, пов'язаному з розвитком біотехнологій. Однак урядам також може бути дедалі важче знайти баланс між потенційною шкодою від втрати приватності і перевагами швидшого розвитку нових технологій. Водночас, щоб протистояти зростаючій концентрації даних у руках невеликої кількості приватних компаній, уряди можуть все більше наполягати на політиці відкритих даних з джерел як державного, так і приватного сектору, віддзеркалюючи нещодавні регуляторні кроки ЄС щодо просторів даних і ринків.

Така політика - як, наприклад, створення трастових фондів публічних даних длядослідницьких цілей - ймовірно, вплине як на національні компанії та галузі, так і на країни-союзники. Це може принести користь більш поширеним і дифузним інноваціям, але це також збільшить ризики, оскільки уможливить порушення приватності в набагато більших масштабах.

Конфіденційність буде сильно впливати на ці угоди: уряд США нещодавно взяв на себе зобов'язання посилити захист трансатлантичних потоків даних, в тому числі від розвідувальної діяльності США. Однак багато з цих наборів даних все ще можуть піддаватися загрозі повторної ідентифікації, навіть незважаючи на нещодавній розвиток технологій, що підвищують конфіденційність, таких як синтетичні дані, федеративне навчання і диференційована конфіденційність.

Дослідження показують, що чутливі бази даних і технології, такі як пули біологічних даних і секвенування ДНК, вже є вразливими до атак. Чутливі медичні дані регулюються непослідовно, а створення великих пулів персональних даних створює прибуткові цілі для кіберзлочинців, особливо з огляду на менш стабільне геополітичне середовище і обмеженість норм, що наразі регулюють кібервійну. Потенційні наслідки широкомасштабної крадіжки

біометричної або геномної інформації здебільшого невідомі, але можуть уможливити цілеспрямоване застосування біологічної зброї.

Дії сьогодні. На національному рівні клаптикова ковдра фрагментарних режимів політики щодо даних на місцевому або державному рівнях підвищує ризик випадкових і навмисних зловживань даними у спосіб, який не був передбачений первинною згодою особи. Гармонізація політики на національному рівні дозволить створити більш ефективні та менш складні механізми транскордонного обміну даними, що сприятимуть інноваціям, забезпечуючи при цьому належний захист осіб. Розробка більш узгодженої на глобальному рівні таксономії, стандартів даних і правового визначення персональної та чутливої інформації є ключовим фактором, що сприяє цьому.

Ці рамки повинні визнавати, що чутливість може зростати внаслідок висновків на основі даних, які стають можливими завдяки великим масивам даних, поширенню соціальних мереж в Інтернеті та розмиванню персональних і промислових даних під час розгортання Інтернету речей і впровадження "розумних" міст.

Наприклад, нещодавно одна компанія була оштрафована відповідно до Загального регламенту ЄС про захист даних (GDPR) за таргетовану рекламу, яка робила висновки про стан здоров'я (що вважається особливою категорією даних) на основі історії покупок. Історично суворі штрафи за втрату даних також допомагають змінити оцінку витрат і вигод, пов'язаних з інвестиціями в заходи кібербезпеки, але залишаються питання щодо індивідуальних прав на дії, відшкодування збитків і компенсації у разі порушення.

Організації будуть зобов'язані враховувати етику збору та використання даних, щоб звести до мінімуму репутаційні міркування, які виходять за рамки дотримання регуляторних вимог. Крім того, під впливом збільшення кількості кібератак і посилення законодавства про захист даних, добровільне видалення та знищення персональних даних може стати більш пріоритетним завданням - з потенційними екологічними супутніми вигодами від мінімізації потреб у зберіганні даних. Нарешті, урядам також потрібно буде розвивати потенціал

реагування на витоки даних і порушення права на приватність, щоб мінімізувати подальші наслідки [6].

Середня світова вартість витоку даних у 2023 році становила 4,45 млн доларів США, що на 15% більше, ніж за 3 роки.

51% організацій планують збільшити інвестиції в безпеку в результаті витоку даних, включаючи планування та тестування реагування на інциденти (IR), навчання співробітників, а також інструменти для виявлення загроз та реагування на них.

Середня економія для організацій, які широко використовують ШІ та автоматизацію безпеки, становить 1,76 млн доларів США порівняно з організаціями,які цього не роблять [7].

2022 рік переключив увагу світової спільноти з пандемії COVID-19 на вторгнення Росії в Україну, яке, серед іншого, поставило політичні розбіжності кіберзлочинного підпілля під збільшувальне скло. Дії правоохоронних органів, хактивізм та розбірки всередині злочинних угруповань розкрили відомі істини, підтвердили припущення та дали уявлення про внутрішню роботу бізнес-структур, а також про суб'єктів загроз, які ними керують.

Нестабільність у регіоні призвела до переміщення деяких кіберзлочинців, що діяли в цьому регіоні, створивши можливості для правоохоронних органів заарештувати високопоставлених суб'єктів загроз, які раніше були поза їхньою досяжністю. Наслідки геополітичної ситуації можна побачити у шквалі руйнівних кібератак, спрямованих не лише на українські та російські об'єкти, а й на об'єкти по всьому світу, особливо в ЄС.

Активізація цієї зловмисної діяльності, спрямованої проти держав-членів ЄС, здебільшого пов'язана зі значною кількістю розподілених атак типу "відмова в обслуговуванні" (DDoS), що впливають на національні та регіональні державні інституції. Ці атаки часто були політично вмотивовані та координувалися проросійськими хакерськими групами у відповідь на заяви або дії на підтримку України. Вторгнення в Україну також вкотре

продемонструвало адаптивність та опортунізм кіберзлочинців.

Онлайн-шахраї швидко відреагували на обставини і скористалися кризою, розробивши різноманітні наративи, пов'язані з нею. Вони обирали жертв по всьому ЄС під виглядом підтримки України чи українців. Були створені фальшиві веб- сторінки для збору коштів з використанням URL-адрес, які містили оманливі ключові слова. З шахрайських адрес надсилалися електронні листи з метою збору коштів на гуманітарну допомогу.

У деяких випадках шахраї видавали себе за знаменитостей, які очолювали або підтримували реальні кампанії, або підробляли домени гуманітарних організацій, пропонуючи жертвам робити пожертви у криптовалюті1 . Загроза сексуальної експлуатації дітей в Інтернеті, на яку не вплинули ці геополітичні події, продовжує зростати в кількісному та якісному відношенні. Злочинці з усіх сфер злочинності продовжують користуватися юридичними та кримінальними сервісами для маскування своїх дій та особистих даних, оскільки їхні знання про заходи протидії зростають.

1.5. Висновки до розділу

В першому розділі ми розглянули теоретичні основи шкідливого програмного забезпечення, отримавши комплексне розуміння його природи, визначення та його різноманітні види. Ми розглянули різні класифікації, серед яких були більш широкі(на способі поширенню, на діях які шкідливі файли виконують коли досягають своєї цілі), так і більш поширені та деталізоввані(включали доволі розгорнутий список з шпигунських програм, вірусів, експлойтівв, з використанням викупів, руткіти, трояни, хробаки, криптомайнери і так далі) Це можна вважати важливим для розуміння того, як різні загрози можуть впливати на системи та дані. Також нами було оглянуто історію та еволюцію ШПЗ, розкриваючи зміни його вигляду та методах атаки з плином часу. Ми дізналися про перші згадування шкідливих файлів і про те, якими вони були раніше, після чого перейшли до сучасності та розглянули

більш сучасні атаки. Важливими змінами, що ми помітили стало використання наборів для атак, зміна джерел атак з індивідуальних зловмисників до організованих та небезпечних угрупувань. Також змінився рівень кастомізації шкідливих файлів за цей час. Прослідкували тенденцію змін та звернули нашу увагу на використання нових більш просунутих технік. Це допомогло нам усвідомити розвиток загроз у кіберпросторі. Розгляд та висвітлення питання впливу та наслідків від ШПЗ показало нам яким великим ризиком для інформаційної безпеки є дане питання та дозволяє нам визначити для себе мотивацію у вивченні та розробці ефективних методів виявлення та захисту. Важливими питаннями, що розглядалися нами тут була централізація і консолідація даних з якої випливає зростаючий компроміс між інноваціями та безпекою Варто зазначити також, що кібератаки є одним із найбільш розповсюджених ризиків сьогодення. Розуміння всього цього дозволяє нам перейти до більш просунутого розгляду даного питання в наступних розділах.

РОЗДІЛ 2.
АНАЛІЗ АРХІТЕКТУРИ РІШЕННЯ DEFENDER, ОГЛЯД АЛГОРИТМІВ ТАМЕТОДІВ ВИЯВЛЕННЯ, ПОРІВНЯННЯ З ІНШИМИ РІШЕННЯМИ

2.1. Огляд архітектури Defender

Defender для кінцевих точок - це комплексне рішення для запобігання, захисту, виявлення та автоматизації розслідування й реагування на загрози на кінцевих точках. Це основна частина Microsoft 365 Defender, яка об'єднує й упорядковує можливості Defender для кінцевих точок, Defender для Office 365, Defender для ідентичності та Defender для хмарних додатків (рис 2.1.). Defender для кінцевих точок складається з кількох компонентів. Зловмисники частіше компрометують некеровані пристрої й тим самимзагрожують мережі.

Рис. 2.1. Ключові компоненти Microsoft 365

Defender для кінцевих точок допомогає виявити ці мережеві пристрої та кінцеві точки, щоб мати змогу оцінити та захистити їх. Для цього не потрібні додаткові пристрої або громіздкі зміни в процесах. Замість цього Defender для кінцевих точок використовує вже встановлені кінцеві точки для збору, дослідження або сканування мережі, щоб виявити некеровані пристрої. Після

виявлення цих некерованих пристроїв

Defender для кінцевих точок допомагає вам оцінити їхню вразливість і встановити на них захист. Виявлення активів є частиною управління загрозами та вразливостями: це місток, що змінює правила гри між командами IT-спеціалістів та службами безпеки.

Це підхід до виявлення, визначення пріоритетів та усунення вразливостей і неправильних конфігурацій кінцевих точок, що базується на оцінці ризиків. Управління загрозами та вразливостями допомагає організаціям виявляти їх в режимі реального часу на основі датчиків, без агентів або періодичних сканувань. Воно визначає пріоритети вразливостей на основі ландшафту загроз, виявлених у організації, конфіденційної інформації на пристроях та бізнес-контексту. Як результат, це допомагає значно зменшити загальну вразливість і підвищити рівень безпеки.

Наступною технологією запобігання є зменшення поверхні атаки. Зменшення поверхні атаки зменшує місця, де організація вразлива до атак, не обмежуючи продуктивність користувачів. Для цього вона надає багатий набір можливостей. Наприклад, контроль додатків дозволяє запускати лише довірені програми. Правила зменшення поверхні атаки допомагають обмежити певну поведінку програм, файлів або скриптів. А мережевий захист запобігає доступу програм до небезпечних місць на основі їхньої репутації.

У той час як управління загрозами й уразливостями та зменшення поверхні атаки допомагають нейтралізувати загрози ще до того, як вони встигнуть завдати шкоди вашим комп'ютерам, антивірус нового покоління здатний виявляти та блокувати атаки ще до того, як вони встигнуть завдати шкоди. Microsoft Defender Antivirus - це компонент захисту нового покоління Defender для кінцевих точок, який поєднує в собі машинне навчання, аналіз великих даних, поглиблене дослідження загроз і хмарну інфраструктуру Microsoft для захисту пристроїв. Він використовує моніторинг поведінки, евристики та захист від загроз у режимі реального часу для виявлення та блокування шкідливих файлових і безфайлових загроз. Завдяки хмарним

технологіям він майже миттєво виявляє та блокує нові загрози.

Далі, виявлення та реагування на кінцевих точках для пошуку загроз, які хочуть залишатися прихованими. Defender для кінцевих точок безперервно збирає дані про поведінку та методи зловмисників на кінцевих точках, щоб виявити підозрілу або зловмисну активність та попередити про неї. Він надає командам безпеки необхідні інструменти для візуального дослідження криміналістичних доказів, швидкого розуміння масштабу порушення та вжиття необхідних заходів. Наприклад, Defender для кінцевих точок пропонує потужні інструменти для пошуку загроз і реагування наних (рис 2.2.).

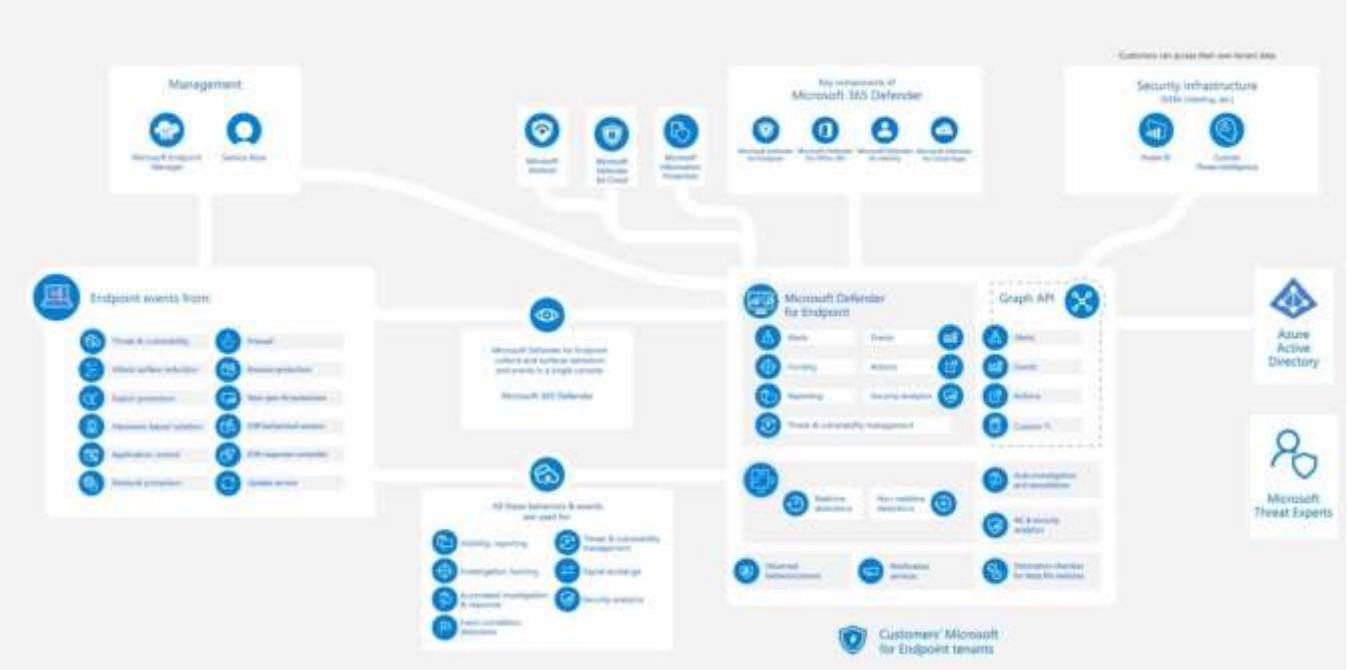


Рис. 2.2. Загальна архітектура тенату Microsoft Defender for Endpoint

Команди безпеки можуть досліджувати історичні дані за 6 місяців на всіх своїх кінцевих точках, писати гнучкі запити, зберігати їх і перетворювати на власні виявлення. Вбудована пісочниця дозволяє командам безпеки відправляти підозрілі файли на глибоку перевірку. Вона повертає повний звіт, який описує можливості файлу. Наступна функція - автоматизація, яка допомагає командам безпекипереходити від попередження до усунення загрози в масштабі. Штучний інтелект, вбудований в Microsoft Defender для кінцевих точок, використовує алгоритми перевірки та процеси, які аналітик застосовує для автоматичного розслідування та усунення загроз. Автоматизоване

розслідування та усунення загроз - це величезна перевага для команд безпеки.

Вони можуть перейти від тривоги до повномасштабного усунення загрози за лічені хвилини. Це значно зменшує кількість оповіщень, на які їм доводиться реагувати, і дозволяє зосередитися на більш складних загрозах або важливих діях. Defender для кінцевих точок надає командам безпеки необхідні інструменти, включаючи автоматизацію, щоб вони могли впоратися з більшістю загроз, з якими вони стикаються.

У тих випадках, коли їм потрібна допомога, вони можуть звернутися на експертів Microsoft Threat Experts. Крім того, Microsoft Threat Experts - це керована служба полювання на загрози, яка складається з двох компонентів. По-перше, цільовісповіщення про атаки надають спеціальну інформацію та аналіз, які допомагають швидко й точно виявляти та реагувати на найкритичніші загрози. Другий компонент

- це експерти на вимогу. Можна звернутися до експертів Microsoft Threat Experts, і вони нададуть технічну консультацію щодо відповідних виявлених загроз. Microsoft Defender для кінцевих точок є потужною платформою для захисту кінцевих точок. Можливість інтеграції з іншими рішеннями за допомогою API виводить її на новий рівень. Microsoft Defender для кінцевих точок - це інноваційна платформа безпеки, яка допоможе захистити вашу організацію від найсучасніших загроз.

Однак, середовища та структури клієнтів різняться, тому Microsoft надають інтерфейси API для забезпечення гнучкості. Клієнти можуть інтегрувати сервіс зі своїми існуючими інфраструктурами безпеки за допомогою багатого набору API.

Наприклад, вони можуть підключити до Defender для кінцевих точок свої SIEM- системи або системи продажу квитків, збагатити свої рішення даними Defender для кінцевих точок або увімкнути власні робочі процеси безпеки. Останній компонент - це управління. Цей компонент надає можливість використовувати Microsoft Endpoint Manager як центральне місце для налаштування базових та індивідуальних параметрівбезпеки кінцевих точок [8].

Портал Microsoft 365 Defender надає командам безпеки доступ до даних Defender для кінцевих точок і дозволяє їм взаємодіяти з кінцевими точками, розслідувати загрози, реагувати на порушення та вдосконалювати систему безпеки. Датчики кінцевих точок збирають події, пов'язані з безпекою, з вбудованих кінцевихточок і надсилають їх тенанту клієнтів.

Ці датчики також можуть виявляти некеровані пристрої в мережі, які можуть бути джерелом зловмисної активності. Платформа використовує поведінкові індикатори атак, алгоритми машинного навчання та виявлення аномалій для виявлення підозрілих подій та перетворення їх на дієві інсайти. Побудована на базі хмари Microsoft Azure, кожен клієнт має виділений тенант Defender for Endpoint, що забезпечує ізоляцію та безпеку даних.

Платформу можна інтегрувати з іншими службами безпеки Microsoft та існуючими інфраструктурами безпеки за допомогою API, що забезпечує гнучкість і налаштування (рис 2.3.).

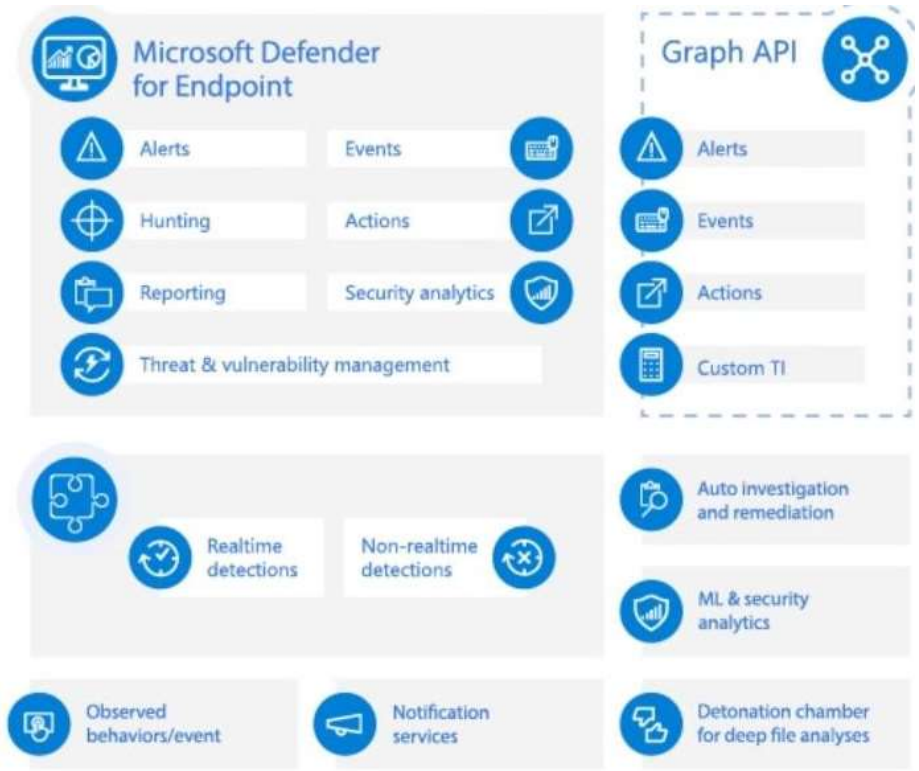


Рис. 2.3. Архітектура рішення Microsoft Defender for Endpoint

Microsoft Defender для кінцевих точок - це корпоративна платформа для

захисту кінцевих точок, призначена для запобігання, виявлення, розслідування та реагуванняна сучасні загрози в корпоративних мережах.

Defender для кінцевих точок використовує наступну комбінацію технологій, вбудованих в Windows 10, і надійну хмарну службу Microsoft:

- Датчики поведінки кінцевих точок: Ці датчики, вбудовані в Windows 10, збирають і обробляють поведінкові сигнали операційної системи та надсилають їх до вашого приватного, ізольованого, хмарного екземпляра Microsoft Defender для кінцевих точок.
- Хмарна аналітика безпеки: Завдяки використанню великих даних, навчанню пристроїв та унікальній оптиці Microsoft в екосистемі Windows, корпоративних хмарних продуктах (наприклад, Office 365) та онлайн-активах, поведінкові сигнали перетворюються на аналітику, виявлення та рекомендовані заходи реагування на сучасні загрози.
- Розвіддані про загрози: Аналітика загроз, яку збирають мисливці за загрозами Microsoft, команди безпеки та доповнюють дані, надані партнерами, дає змогу Defender для кінцевих точок виявляти інструменти, методи та процедури зловмисників і генерувати сповіщення, коли вони виявляються в зібраних даних датчиків.

На рисунку 2.4. ми можемо бачити компоненти Microsoft Defender for Endpoint.

Рис. 2.4. Компоненти Microsoft Defender for Endpoint

- Управління вразливостями Core Defender

Вбудовані функції керування вразливостями використовують сучасний

підхід, заснований на оцінці ризиків, для виявлення, оцінки, визначення пріоритетів та усунення вразливостей і неправильних конфігурацій кінцевих точок.

- Зменшення поверхні атаки

Набір засобів для зменшення поверхні атаки забезпечує першу лінію захисту встеку. Завдяки правильному налаштуванню параметрів конфігурації та застосуванню методів усунення вразливостей ці засоби протистоять атакам і використанню вразливостей. Цей набір засобів також включає мережевий захист і веб-захист, які регулюють доступ до зловмисних IP-адрес, доменів і URL-адрес.

- Захист наступного покоління

Щоб ще більше зміцнити периметр безпеки вашої мережі, Microsoft Defender для кінцевих точок використовує засоби захисту наступного покоління, призначені для виявлення всіх типів нових загроз.

Виявлення та реагування на загрози для кінцевих точокФункції виявлення та реагування на загрози на кінцевих точках призначені длявиявлення, розслідування та реагування на сучасні загрози, які могли пройти повз перші два компоненти захисту.

Розширений пошук - це інструмент пошуку загроз наоснові запитів, який дає змогу проактивно знаходити проломи та створювати користувацькі виявлення.

- Автоматизоване розслідування та усунення

Microsoft Defender для кінцевих точок не лише здатний швидко реагувати на складні атаки, але й пропонує функції автоматичного розслідування та усунення, які допомагають зменшити кількість сповіщень за лічені хвилини в масштабі.

- Microsoft Secure Score для пристроїв

До складу Defender для кінцевих точок входить Microsoft Secure Score for Devices, яка допомагає динамічно оцінювати стан безпеки корпоративної мережі, виявляти незахищені системи та вживати рекомендованих заходів для

підвищення загального рівня безпеки вашої організації.

- Експерти "Майкрософт" із захисту від загроз

Служба керованого пошуку загроз Microsoft Defender для кінцевих точок забезпечує проактивний пошук, визначення пріоритетів, а також додатковий контекст і розуміння, які надалі розширюють можливості операційних центрів безпеки (SOC) для швидкого і точного виявлення і реагування на загрози [9].

Microsoft Defender XDR, Defender для кінцевих точок і різні рішення длязахисту від Microsoft утворюють єдиний комплекс для захисту підприємства до та після порушень, який інтегрується з кінцевими точками, ідентичностями, електронною поштою та програмами для виявлення, запобігання, розслідування та автоматичного реагування на складні атаки [10].

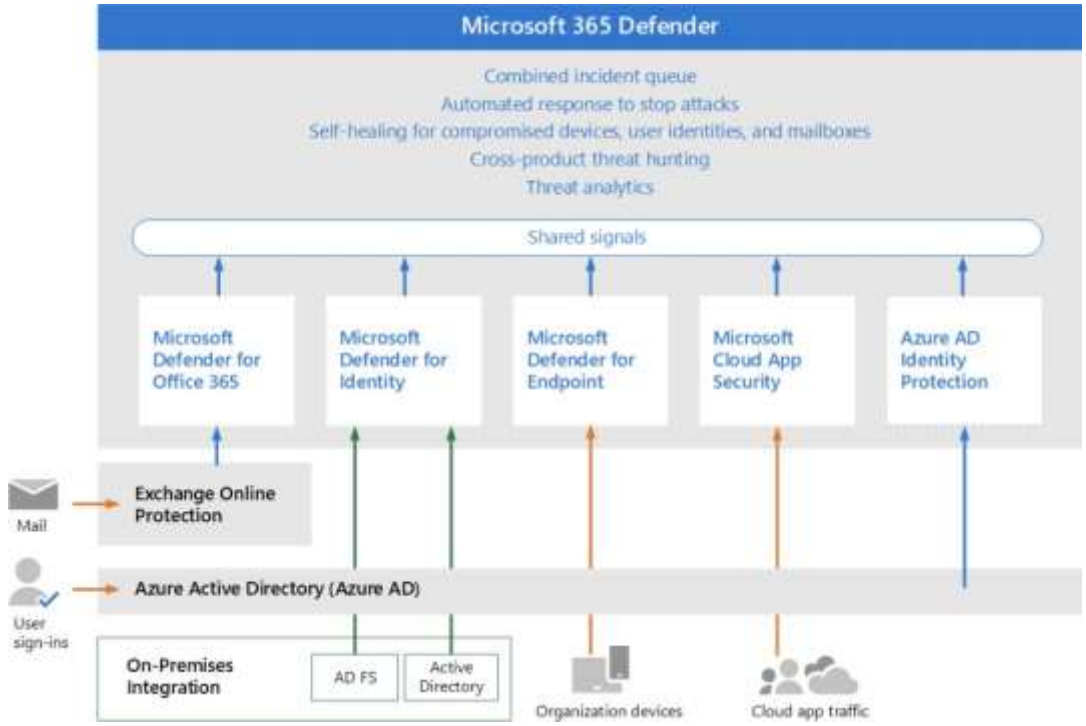


Рис. 2.5. Об’єднання сигналів від усіх компонентів Defender

На рисунку 2.5. Microsoft Defender XDR об'єднує сигнали від усіх компонентів Defender, щоб забезпечити розширене виявлення та реагування (XDR) в різних доменах. Сюди входить уніфікована черга інцидентів, автоматичне реагування для зупинення атак, самовідновлення (для скомпрометованих пристроїв, ідентифікаторів користувачів і поштових

скриньок), пошук перехресних загроз і аналітика загроз.

Microsoft Defender для Office 365 захищає вашу організацію від зловмисних загроз, що надходять через повідомлення електронної пошти, посилання (URL- адреси) та інструменти для співпраці. Він обмінюється сигналами, отриманими в результаті цих дій, з Microsoft Defender XDR. Інтегрований Exchange Online Protection (EOP) забезпечує наскрізний захист вхідної електронної пошти та вкладень.

Microsoft Defender для ідентичності збирає сигнали від серверів, на яких працюють служби Active Directory Federated Services (AD FS) і локальні служби доменів Active Directory (AD DS). Він використовує ці сигнали для захисту вашого гібридного середовища ідентичностей, зокрема для захисту від хакерів, які використовують скомпрометовані облікові записи для переміщення між робочими станціями в локальному середовищі.

Microsoft Defender для кінцевих точок збирає сигнали та захищає пристрої, щовикористовуються у організації.

Microsoft Defender для хмарних програм збирає сигнали про використання хмарних програм у організації та захищає дані, що передаються між середовищем і цими програмами, включно із санкціонованими та несанкціонованими хмарними програмами.

Microsoft Entra ID Protection оцінює дані про ризики, отримані під час мільярдів спроб входу, і використовує ці дані, щоб оцінити ризик кожного входу у ваше середовище. Ці дані використовуються Microsoft Entra ID, щоб дозволити або заборонити доступ до облікового запису, залежно від того, як налаштовані політики умовного доступу [11].

2.2. Алгоритми та методи для виявлення шкідливих файлів

Алгоритми та Методи виявлення Шкідливих Файлів в Microsoft Defender for Endpoint.

Microsoft Defender for Endpoint використовує ряд алгоритмів та методів

для ефективного виявлення шкідливих файлів. Основні підходи включають:

- Сигнатурне виявлення:

Цей підхід ґрунтується на визначенні унікальних підписів або характеристик вірусів, які включаються в базу даних відомих загроз. Коли Defender сканує файл, він порівнює його хеш-суму чи інші ідентифікатори з базою сигнатур, щоб визначити чи є файл шкідливим. Однак, цей методи не є дуже ефективним проти нових, раніше невідомих загроз.

- Виявлення аномалій та поведінковий аналіз:

Аналізує надзвичайні або несподівані взірці поведінки файлів, що може свідчити про шкідливу активність. Поведінковий аналіз і виявлення аномалій грають ключову роль у забезпеченні безпеки системи. Ці технології спрямовані на виявлення потенційно шкідливого програмного забезпечення, навіть якщо його сигнатура ще не входить до бази даних відомих загроз. Система визначає нормальну поведінку для файлів і потім працює на виявлення аномалій, коли програма чи процес не веде себе звично.

- Машинне навчання:

Використовує алгоритми машинного навчання для аналізу структурних та поведінкових ознак файлів. Цей підхід дозволяє створювати моделі, які можуть навчатися на основі великого обсягу даних та може виявляти шкідливі програми, враховуючи їх особливості та характеристики.

- Хмарні інтелектуальні служби:

За використанням хмарних інтелектуальних служб, таких як Intelligent Security Graph, для отримання додаткових даних та контексту. Такі служби можуть використовуввати хмарні обчислення та аналіз файлів на великій шкалі для надання більш точних та швидких результатів.

- Евристичні методи:

Використовує евристичні правила та методи для виявлення потенційно небезпечних або невідомих вірусів. Евристика використовує правила та принципи для виявлення загроз, базуючись на їх загальних характеристиках та

аспектах(наприклад, спостереження за використанням ресурсів системи).

Ці підходи працюють синергічно для створення надійного захисту від шкідливих файлів.

2.3. Методи тестування ефективності Defender

Microsoft Defender проходить через різноманітні методи тестування для забезпечення високої ефективності виявлення та захисту. Основні методи тестування включають:

- Тестування на власних лабораторіях:

Microsoft проводить внутрішнє тестування власних продуктів на великих лабораторних масштабах, щоб визначити їхню ефективність в умовах, які найкращевідображають реальні загрози.

- Участь у тестах незалежних лабораторій:

Microsoft Defender бере участь у тестах, проведених незалежними лабораторіями, такими як AV-TEST, AV-Comparatives, та інші. Ці тести дозволяютьотримати об'єктивну оцінку ефективності продукту.

- Тестування на реальних атаках (Red Team Testing):

Microsoft використовує методи тестування, що моделюють реальні атаки (Red Team Testing), щоб визначити, наскільки ефективно продукт протистоїть спробам вторгнення та компрометації систем.

- Співпраця зі спільнотою білого гатунку (White Hat Community Collaboration):

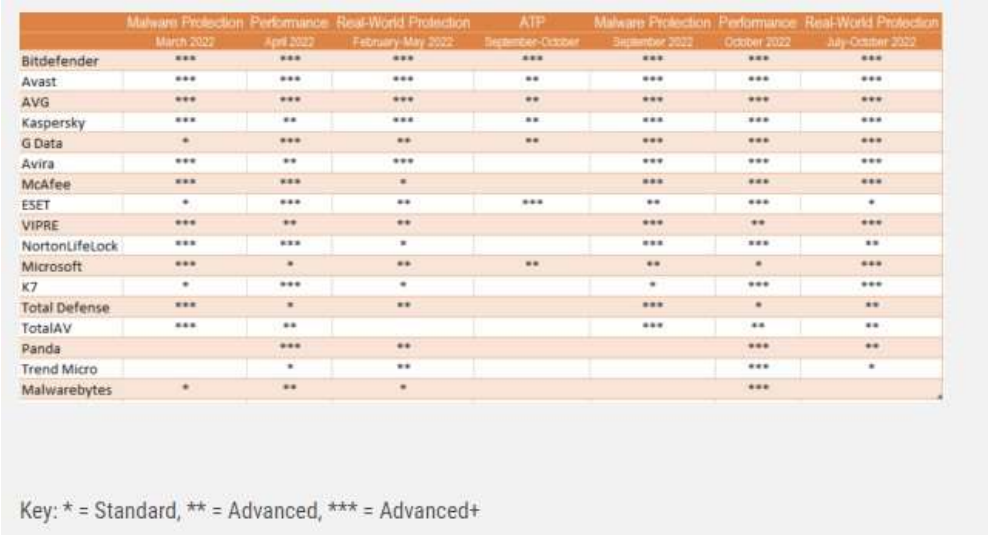
- Тестування з партнерами:

Microsoft співпрацює з партнерами, такими як інші компанії зі сфери безпеки,для спільного тестування та вдосконалення захисту [11].

AV-Comparatives. Microsoft отримала бронзову нагороду в тесті Advencer Threat Protection. Вона також отримала дві нагороди Advanced+ і три нагороди Advanced Awards у цьогорічних тестах. Продукт інтегрований в Windows 10 і має простий, ненав'язливий інтерфейс. Його чутливий захист при доступі

виявляє шкідливе програмне забезпечення на зовнішніх дисках і мережевих ресурсах, як тільки вони відкриваються.

На рисунку 2.6. ми можемо побачити результати антивірусного тестування за 2022 рік.



	Malware Protection March 2022	Performance April 2022	Real-World Protection February-May 2022	ATP September-October	Malware Protection September 2022	Performance October 2022	Real-World Protection July-October 2022
Bitdefender	***	***	***	***	***	***	***
Avast	***	***	***	**	***	***	***
AVG	***	***	***	**	***	***	***
Kaspersky	***	**	***	**	***	***	***
G Data	*	***	**	**	***	***	***
Avira	***	**	***		***	***	***
McAfee	***	***	*		***	***	***
ESET	*	***	**	***	**	***	*
VIPRE	***	**	**		***	**	***
NortonLifeLock	***	***	*		***	***	**
Microsoft	***	*	**	**	**	*	***
K7	*	***	*		*	***	***
Total Defense	***	*	**		***	*	**
TotalAV	***	**			***	**	**
Panda		***	**			***	**
Trend Micro		*	**			***	*
Malwarebytes	*	**	*			***	

Key: * = Standard, ** = Advanced, *** = Advanced+

Рис. 2.6. Результати антивірусного тестування за 2022 рік

Під час антивірусного тестування важливо вимірювати не лише можливості виявлення, але й надійність. Одним з аспектів надійності є здатність розпізнавати чисті файли як такі і не створювати хибних тривог (помилкових спрацьовувань). Жоден продукт не застрахований від хибних спрацьовувань, але деякі з них спрацьовують частіше, ніж інші. Тести на хибні спрацьовування визначають, які програми найкраще справляються з цим завданням, тобто відрізняють чисті файли від шкідливих, незважаючи на їхній контекст. Не існує повної колекції всіх існуючих легітимних файлів, тому неможливо провести "ідеальний" тест на хибнопозитивні спрацьовування [12].

Що можна зробити, і це розумно, так це створити і використовувати набір чистих файлів, який збирається незалежно. Якщо при використанні такого набору один продукт має, наприклад, 15 FP, а інший - лише 2, то цілком ймовірно, що перший продукт більш схильний до FP, ніж інший. Це не означає, що продукт, який має 2 ФП,не має більше 2 ФП в усьому світі, але важлива саме відносна кількість.

Процедура тестування.

Антивірусні продукти не повинні мати хибних спрацьовувань на будь-які чисті файли, незалежно від того, скільки користувачів наразі постраждало від них. Хоча деякі виробники антивірусних програм можуть применшувати ризик хибних спрацьовувань і збільшувати ризик шкідливого програмного забезпечення, ми не збираємося оцінювати продукти на основі передбачуваної поширеності хибних спрацьовувань.

Допустима певна кількість хибних спрацьовувань (наразі 10) у чистому наборі, припускається що продукти, які генерують більшу кількість хибних спрацьовувань, також з більшою ймовірністю генеруватимуть хибні спрацьовування з більшою кількістю поширених файлів (або в інших наборах чистих файлів).

Дані про поширеність чистих файлів ми наводимо лише з інформаційною метою. Зазначена поширеність може відрізнятися всередині звіту залежно від того, для якого файлу/версії сталася хибна тривога та/або скільки файлів одного типу було уражено.

Результати тестування. Кількість хибних спрацьовувань двох різних програм, які використовують один і той самий алгоритм (основний компонент виявлення), може відрізнятися. Наприклад, постачальник А може надати ліцензію на свій механізм виявлення постачальнику Б, але продукт постачальника А може мати більше або менше хибних спрацьовувань, ніж продукт постачальника Б. Це може бути пов'язано з такими факторами, як різні внутрішні налаштування, відмінності в інших компонентах і послугах, таких як додаткові або відмінні вторинні рушії/сигнатури/бази даних білих списків/хмарні сервіси/забезпечення якості, а також можлива затримка в часі між випуском оригінальних сигнатур і доступністю сигнатур для продуктів третіх сторін.

Хибнопозитивні спрацьовування (FP) є важливим показником якості антивірусної системи. Крім того, цей тест корисний і необхідний, щоб уникнути того, що виробники оптимізують продукти для отримання хороших результатів у тестах, дивлячись на контекст - ось чому хибні спрацьовування змішуються і

тестуються таксамо, як і тести зі шкідливим програмним забезпеченням.

Один звіт про FP від клієнта може призвести до великого обсягу інженерної та технічної роботи для вирішення проблеми. Іноді це може навіть призвести до втрати важливих даних або недоступності системи.

Навіть "несуттєві" FP (або FP у старих додатках) заслуговують на увагу, оскільки FP, швидше за все, є результатом виявлення принципових правил. Просто так сталося, що FP був у незначному файлі. Ймовірно, можливість FP все ще існує в продукті і потенційно може призвести до повторного виникнення FP на більш значущому файлі.

В таблиці 2.1. продемонстровано результати тестування, з сортуванням за кількістю хибних спрацювань від найменшого до найбільшого.

Таблиця 2.1.

Порівняння кількості хибних спрацювань

№	Назва рішення	К/ть	Хибні спрацювання
1.	TotalAV	0	very few FPs
2.	Avast, AVG, Avira, ESET	1	
3.	G DATA, Trend Micro	2	few FPs -
4.	Bitdefend er, Total Defense	4	
5.	Microsoft, Panda	5	
6.	Kaspersky	6	
7.	McAfee	10	
8.	Norton	12	many FPs
9.	**K7**	17	
10.	**F-Secure**	25	a lot of FPs

В рис .2.7. також наведемо позицію Microsoft в даному тестуванні де ми можемо бачити кількість хибних спрацювань в нашому рішенні і його місце поряд з іншими вендорами.

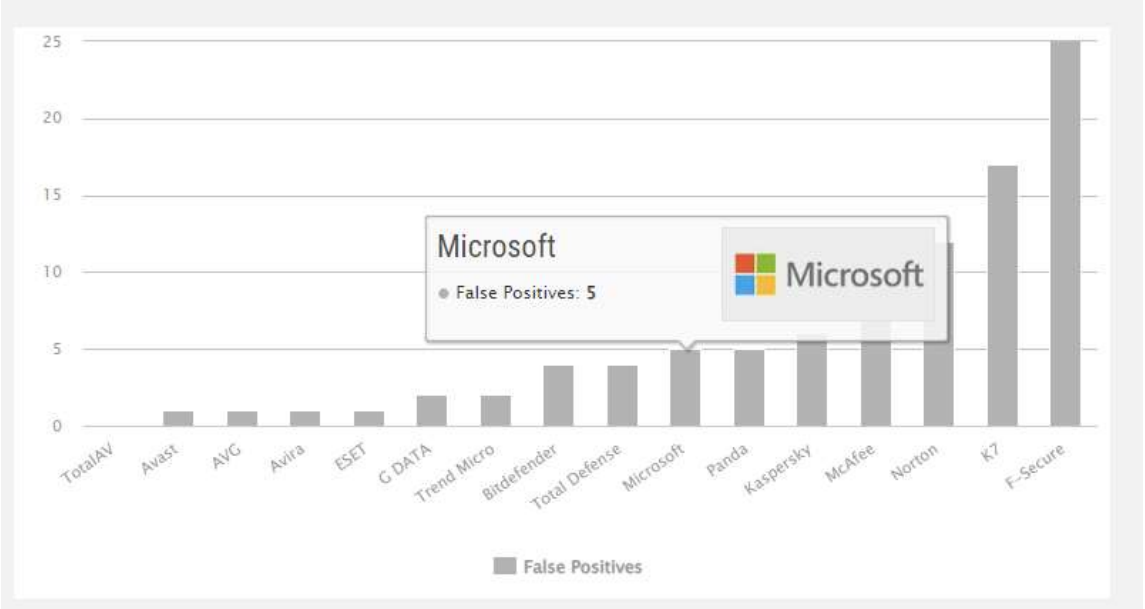


Рис. 2.7. Позиція Microsoft у тестуванні на к-ть FP

AV-TEST Award Best Advanced Protection 2022.

Вперше за 12-річну історію нагородження Інститут AV-TEST присуджує нагороди в категорії "ПРОСУНУТИЙ ЗАХИСТ". Для тестування в реальному часі в лабораторії потрібні споживчі користувацькі продукти під управлінням Windows, наприклад, для захисту від програм-вимагачів. Лабораторія крок за кроком оцінює атаку та її запобігання і виставляє оцінку захисту. За видатний розширений захист від шкідливого програмного забезпечення для споживчих продуктів AV-TEST присуджує нагороду "Найкращий розширений захист 2022" антивірусу MicrosoftDefender і додатку PC Matic Application Whitelist.

Рис. 2.8. Нагорода за найкращий просунутий захист для персонального використання

У новій номінації ADVANCED PROTECTION лабораторія AV-TEST відзначає найкращі рішення для захисту корпоративних користувачів, які поетапно оцінюються під час тестування. При цьому аналізується, чи виявлено, наприклад, програми-вимагачі, на якому етапі вони повністю або частково зупиняються, або не зупиняються взагалі. Серед продуктів для корпоративних користувачів із стабільно високими показниками захисту AV-TEST відзначає Microsoft Defender Antivirus нагородою AV-TEST Best Advanced Protection 2022.

Рис. 2.9. . Нагорода за найкращий просунутий захист для корпоративних користувачів

AV-TEST Award – for tested IT Security.

Всі продукти, що тестуються Інститутом AV-TEST, оцінюються відповідно до заздалегідь визначеної структури тесту. Це завжди прозоро для компаній і користувачів і завжди може бути логічно зрозуміло. Протягом одного року тестування продукти безпеки перевіряються та оцінюються кілька разів у таких сферах, як захист (функція захисту), продуктивність (швидкість) та зручність використання (зручність для користувача). Крім того, існують також тести Advanced Threat Protection, в яких перевіряється особлива ефективність продуктів у боротьбі з програмами-вимагачами, наприклад, у боротьбі з вірусами-здирниками. За успішне проходження тесту рішення для захисту отримує сертифікат про перевірений захист від IT-загроз. Продукти для Windows, які пройшли тест з результатами, що значно перевищують галузеві стандарти, відзначаються додатковою оцінкою "TOP PRODUCT". AV-TEST Award for Microsoft – more than just recognition

"Коли справа доходить до програм-вимагачів, Microsoft, схоже, розвинула особливу силу. Зовсім нові тести Advanced Threat Protection виходять далеко за рамки класичного виявлення. Не кожен провайдер зміг впоратися з розширеними атаками, переважно за допомогою програм-вимагачів, у тестах 2022 року. Ось чомуінститут AV-TEST був радий вручити дві важливі нагороди для споживчих користувачів і корпоративних користувачів за найкращий розширений захист 2022 року компанії Microsoft", - сказав Андреас Маркс, генеральний директор AV-TEST.

AV-TEST Product Review and Certification Report – Sep-Oct/2023

Протягом вересня та жовтня 2023 року AV-Test безперервно оцінювали 17 продуктів для захисту кінцевих точок, використовуючи налаштування, надані виробником. Для тестування завжди використовувалися найновіші загальнодоступні версії всіх продуктів. Вони могли оновлюватися в будь-який час і звертатися до хмарних сервісів. Ми зосередилися на реалістичних тестових сценаріях і перевіряли продукти на стійкість до реальних загроз. Продукти повинні були продемонструвати свої можливості з використанням

усіх компонентів і рівнів захисту.

Захист. Захист від зараження шкідливим програмним забезпеченням (таких як віруси, хробаки або троянські програми)

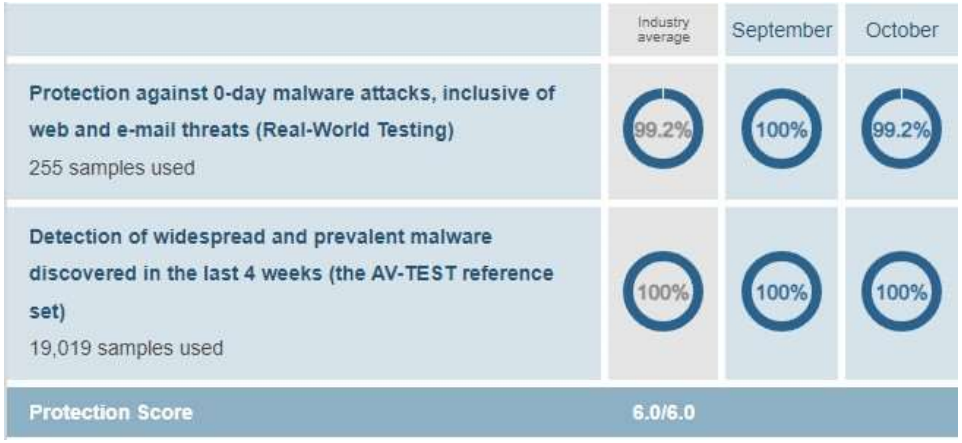


Рис. 2.10. Оцінка рівня захисту ввід зараження ШПЗ

Продуктивність. Середній вплив продукту на швидкість роботи комп'ютера при щоденномувикористанні.

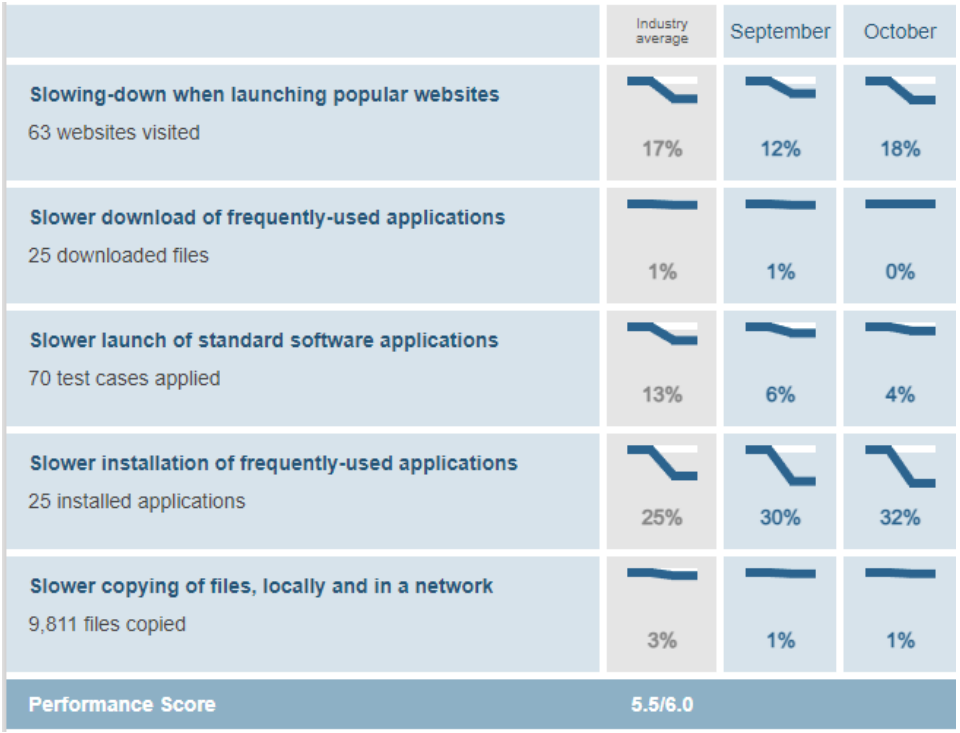
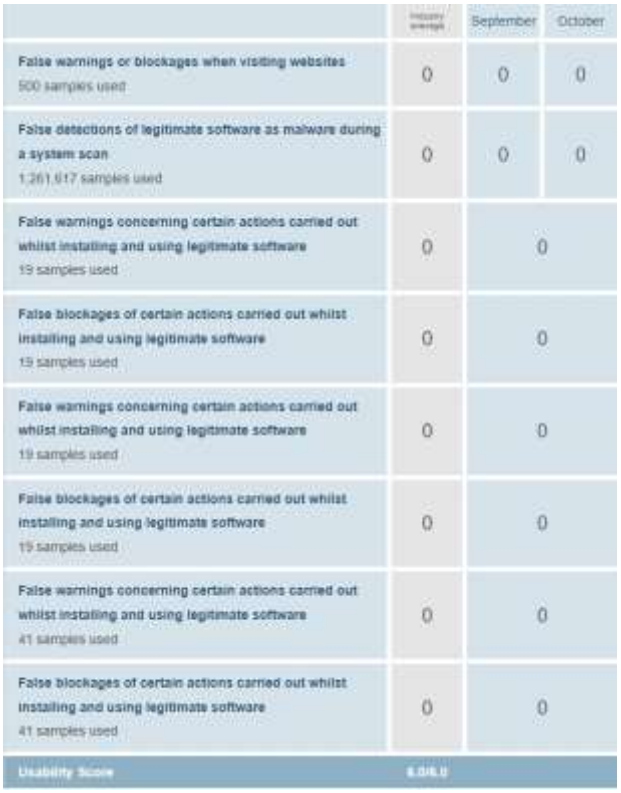


Рис.2.11. Оцінка продуктивності рішення Defender

Юзабіліті. Вплив програмного забезпечення для захисту на зручність використання всього комп'ютера (нижчі значення вказують на кращі

результати).



		September	October
False warnings or blockages when visiting websites 500 samples used	0	0	0
False detections of legitimate software as malware during a system scan 1,261,617 samples used	0	0	0
False warnings concerning certain actions carried out whilst installing and using legitimate software 19 samples used	0	0	
False blockages of certain actions carried out whilst installing and using legitimate software 19 samples used	0	0	
False warnings concerning certain actions carried out whilst installing and using legitimate software 19 samples used	0	0	
False blockages of certain actions carried out whilst installing and using legitimate software 19 samples used	0	0	
False warnings concerning certain actions carried out whilst installing and using legitimate software 41 samples used	0	0	
False blockages of certain actions carried out whilst installing and using legitimate software 41 samples used	0	0	
Usability Score			

Рис. 2.12. Оцінка зручності використання рішення Defender

Технологія Advanced Hunting та мова запитів KQL

Технологія Advanced Hunting є ключовим елементом системи безпеки Microsoft Defender. Ця технологія дозволяє користувачам використовувати запити для аналізу та виявлення потенційних загроз у реальному часі. Вона надає додаткові можливості для розширеного пошуку та аналізу великого обсягу данних у середовищі Microsoft Defender.

Основні характеристики технології Advanced Hunting включають:

- Запити на основі структурованої схеми даних: Використовуючи структуровану схему даних, користувачі можуть створювати запити для отримання інформації про події та дії в системі. Наприклад, це може бути корисно для виявлення аномальної активності акаунта чи інших надзвичайних ситуацій.
- Виявлення загроз та аномалій: Advanced Hunting дозволяє створювати запити, спрямовані на виявлення загроз та аномальної поведінки. Користувачі можуть аналізувати різноманітні підозрілі з'єднання, активності чи

дії, які можуть бути індикаторами атак.

- Розширені можливості аналізу даних: За допомогою Advanced Hunting можна проводити глибший аналіз даних, виявляти складні зв'язки та залежності між різними подіями, що дозволяє вчасно реагувати на потенційні загрози.
- Миттєвий доступ до даних: Технологія забезпечує можливість отримання інформації в реальному часі, що робить Advanced Hunting потужним інструментом для миттєвого виявлення та реагування на загрози.
- Використання Advanced Hunting дозволяє адміністраторам і аналітикам інформаційної безпеки більш гнучко та ефективно працювати з даними, спрощуючи процес виявлення та реагування на кіберзагрози.

Технологія Advanced Hunting у Microsoft Defender використовує спеціальну мову запитів для аналізу та взаємодії з даними. Ця мова називається Kusto Query Language (KQL). KQL є декларативною мовою, спроектованою для роботи з великими обсягами структурованих даних.

Деякі ключові аспекти Kusto Query Language:

- Декларативність: KQL дозволяє визначати, що саме ви хочете витягти з даних, а не як це робити крок за кроком. Це робить запити коротшими та більш зрозумілими.
- Подібність до SQL: Для багатьох, хто знайомий з SQL (Structured Query Language), вивчення KQL буде відносно простим. Вони мають подібний синтаксис та основні концепції.
- Підтримка структурованих даних: KQL працює з різноманітними типами даних та може опрацьовувати складні структури, що дозволяє аналізувати різні аспекти системи безпеки.
- Можливості фільтрації та агрегації: З KQL ви можете визначати умови фільтрації для виділення певних даних та використовувати функції агрегації для отримання підсумкової інформації.

Таким чином, мова KQL виступає як інструмент для створення потужних

запитів, які можна використовувати в технології Advanced Hunting для аналізу даних, виявлення загроз та вдосконалення системи безпеки [13].

2.4. Використання машинного навчання в алгоритмах Defender

Машинне навчання є ключовим рушієм постійного розвитку технологій безпеки в Microsoft. Машинне навчання дає змогу Microsoft 365 масштабувати можливості захисту нового покоління та вдосконалювати хмарне блокування нових і невідомих загроз у режимі реального часу.

Роль машинного навчання Люди-аналітики здатні створювати евристичні правила, які попереджають про порушення, спираючись на власний досвід. Однак при створенні евристичних правил аналітик може враховувати лише обмежений набір сигналів. Беручи до уваги тисячі сигналів, ML може більш точно проаналізувати дані, керуючись евристиками, створеними вручну. На основі аналізу реальних сповіщень технології ML щонайменше на 20% точніші, ніж евристики, створені вручну.

Технології машинного навчання також здатні працювати з більш загальними артефактами. Як результат, технології ML можуть узагальнювати різні відтінки даних, щоб виявити нові та раніше невидимі загрози. Моделі ML оптимізують використання величезних обсягів даних і обчислювальних ресурсів, доступних для Windows Defender ATP.

Корпорація Майкрософт удосконалила засоби захисту на основі штучного інтелекту в Microsoft Defender для кінцевих точок за допомогою різних спеціалізованих методів машинного навчання, які знаходять і швидко інкримінують - тобто визначають зловмисні наміри з високим ступенем достовірності - шкідливі файли, процеси або поведінку, що спостерігаються під час активних атак. Це було зроблено для того, щоб якомога раніше зупинити атаки програм-вимагачів, керованих людиною.

Комплексна стратегія пом'якшення наслідків, яка вимагає аналізу контексту атаки і пов'язаних з нею дій як на цільовому пристрої, так і в

організації, полягає в ранньому виявленні об'єктів, включаючи файли, облікові записи користувачів і пристрої. Щоб оцінити, чи пов'язаний об'єкт з поточною атакою програм-вимагачів, Defender для кінцевих точок інтегрує три рівні вхідних даних на основі штучного інтелекту, кожен з яких виводить оцінку ризику:

- Аналіз сповіщень у часі та статистиці для пошуку аномалій на рівні організації
- Агрегація підозрілих подій на всіх пристроях компанії з використанням структури графів для виявлення зловмисної поведінки на групі пристроїв
- Моніторинг на рівні пристроїв для впевненого виявлення підозрілої поведінки

Наприклад, Defender для кінцевих точок зміг виявити і викрити атаку зловмисників на ранній стадії процесу шифрування, коли зловмисники встигли зашифрувати файли лише на менш ніж чотирьох відсотках (4%) пристроїв організації, продемонструвавши поліпшену здатність зупинити атаку і захистити решту пристроїв організації. Цей інцидент є чудовим прикладом важливості швидкого засудження підозрюваних осіб і припинення операції з вимагання викупу, керованої людиною, на її шляху.

Ця подія демонструє, як можна зменшити кількість атак зловмисників в організації шляхом швидкого виявлення підозрілих файлів і процесів. Після отримання звинувачення на адресу цілі Microsoft Defender для кінцевих точок зупиняє атаку за допомогою блокування зі зворотним зв'язком, в якому використовується антивірус Microsoft Defender, щоб зупинити загрозу на кінцевих точках в межах підприємства. Потім Defender для кінцевих точок захищає інші компанії, використовуючи інформацію про загрози, отриману під час атаки з вимогою викупу.

Недоліки використання машинного навчання

Моделі машинного навчання здебільшого не здатні відрізнити зловмисні вхідні дані від доброякісних аномальних. Значним джерелом навчальних даних

є неконтрольовані, немодеровані, загальнодоступні набори даних, які відкриті для внесків третіх сторін. Зловмисникам не потрібно компрометувати набори даних, якщо вони можуть вільно вносити в них свої дані. З часом шкідливі дані з низьким рівнем довіри перетворюються на надійні дані з високим рівнем довіри, за умови, що структура/форматування даних залишається правильною.

Враховуючи велику кількість шарів прихованих класифікаторів/нейронів, які можуть бути використані в моделі глибокого навчання, занадто велика довіра покладається на результати процесів і алгоритмів прийняття рішень ШІ/ММ без критичного розуміння того, як ці рішення були досягнуті. Це призводить до неможливості "показати свою роботу" і ускладнює доказовий захист результатів ШІ/МН, коли їх ставлять під сумнів.

2.5. Висновки до розділу

В цьому розділі нами було проведено огляд архітектури Defender, де ми познайомилися з ключовими компонентами Microsoft 365, загальною архітектурою тенанту та доступними функціями (вбудована пісочниця, автоматизація, можливість взаємодії через API запити). Було розглянуто алгоритми та методи виявлення ШПЗ які використовуються в даному рішенні. Також ми порівняли наше рішення з іншими доступними рішеннями на ринку, розглянули використання машинного навчання та інших технік в алгоритмах Defender, а також оглянули технологію Advanced Hunting та мову запитів KQL. Як результат нашого огляду, ми можемо побачити, що система побудована з використанням потужних методів виявлення та реагування на загрози.

Вбудовані алгоритми в Defender є високоефективними та добре показали себе у виявленні шкідливого програмного забезпечення. Ми отримали важливі уявлення про те, яким чином використовується машинне навчання та інші техніки для покращення точності та швидкості виявлення загроз. Під час порівняння системи з іншими рішеннями, ми додали об’єктивності в оцінці ефективності даного рішення.

Це можна використати як важливий показник для організацій, які могли б розглядати вибір даного рішення. Огляд та введення в технологію Advanced Hunting та мову запитів KQL, яка використовується в цій технології стане нам в нагоді при роботі над третім розділом. Ми помітили важливість, зручність та гнучкість цієї технології для адміністраторів та дослідників в області кібербезпеки під час проведення аналізу.

РОЗДІЛ 3.
ПРАКТИЧНІ ПРИКЛАДИ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ ШПЗ ЗА ДОПОМОГОЮ ADVANCED HUNTING

В попередньому розділі ми вже розглянули що таке технологія Advanced Hunting, для чого ця технологія використовується та яка мова використовується для побудови запитів. Далі, можемо перейти до надання практичних прикладів запитів виявлення шкідливих файлів або підозрілої активності, надати детальний опис та аналіз цих запитів, щоб пояснити для чого та як їх можна використовувати. Для того, щоб якось класифікувати їх, можемо скористатися базою знань MITRE ATT&CK®.

MITRE ATT&CK® - це глобально доступна база знань про тактику і методи противника, заснована на реальних спостереженнях. База знань ATT&CK використовується як основа для розробки конкретних моделей і методологій протидії загрозам у приватному секторі, в уряді, а також у спільноті розробників продуктів і послуг у сфері кібербезпеки.

Створюючи ATT&CK, MITRE виконує свою місію - вирішувати проблеми заради безпечнішого світу, об'єднуючи спільноти для розробки більш ефективних засобів кібербезпеки. ATT&CK є відкритим і доступним для використання будь- якою особою чи організацією на безоплатній основі.

Розвідка.

Зловмисник намагається зібрати інформацію, яку він може використати дляпланування майбутніх операцій.

Розвідка складається з методів, за допомогою яких противник активно або пасивно збирає інформацію, яка може бути використана для підтримки вибору цілей. Така інформація може включати дані про організацію-жертву, її інфраструктуру або персонал/персонал. Ця інформація може бути використана противником для допомоги на інших етапах життєвого циклу противника, таких як використання зібраної інформації для планування і здійснення

початкового доступу, визначення обсягу і пріоритетності цілей після компрометації, або для управління подальшими розвідувальними зусиллями (Додаток А).

Цей запит складений для виявлення можливого сканування мережі з використаннямданих подій мережі на пристрої. Давайте докладніше розберемо його:

1. DeviceNetworkEvents: Використовує дані з подій мережі на пристрої.

2. where RemoteIP matches regex - Фільтрує події, вибираючи лише ті, що мають віддалену IP-адресу, яка відповідає певному регулярному виразу. В цьому випадку відбираються IP-адреси, які належать локальним мережевим підмережам(10.x.x.x, 172.x.x.x, 192.168.x.x).

3. and InitiatingProcessCreationTime > ago(1h): Додатковий фільтр, що обмежує час створення ініціюючих процесів, вибираючи лише ті, які створені в останню годину. Допомагає відфільтровувати хибні спрацювання.

4. where InitiatingProcessFileName !in ...: Виключення конкретних процесів (chrome.exe, Google Chrome Helper, firefox.exe, opera.exe, vivaldi.exe), які можуть бути причиною хибних результатів(FP).

5. where InitiatingProcessFolderPath !in (...): Ще одне виключення, яке використовується для визначення шляхів до виконуваних файлів, які повинні бутивиключені.

6. where not (DeviceName contains "Ourdevice" and InitiatingProcessFolderPath contains @""): Ще одне виключення, яке фільтрує події, які містять певні імена пристроїв та шляхи до виконуваних файлів.

7. summarize ... by DeviceName, DeviceId, InitiatingProcessFolderPath, InitiatingProcessFileName, InitiatingProcessId, InitiatingProcessCreationTime: Групує тапідсумовує дані за певними атрибутами.

8. where RemoteIPCount > 10: Обмежує результати, залишаючи лише ті, де кількість унікальних віддалених IP-адрес перевищує 10.Отже, запит виявляє пристрої, які можуть виконувати можливі сканування мережі, і

виключає з результатів деякі відомі процеси та шляхи (Додаток Б).

Ескалація привілеїв.

Зловмисник намагається отримати дозволи вищого рівня. Підвищення привілеїв складається з методів, які зловмисники використовують для отримання дозволів вищого рівня в системі або мережі. Зловмисники часто можуть увійти і досліджувати мережу з непривілейованим доступом, але потребують підвищених привілеїв, щоб досягти своїх цілей. Поширеними підходами є використання слабких місць системи, неправильних конфігурацій та вразливостей.Приклади підвищеного доступу включають

- системний/кореневий рівень;
- локальний адміністратор;
- обліковий запис користувача з правами адміністратора;
- облікові записи користувачів з доступом до певної системи або для виконанняпевних функцій.

Ці методи часто перетинаються з методами персистентності, оскільки функції операційної системи, які дозволяють зловмиснику продовжувати свою діяльність, можуть виконуватися в підвищеному контексті [14].

Керівник служби, доданий до ролі. Одним з показників компрометації кампанії Nobelium (раніше Solorigate) булоте, що до привілейованих ролей були додані несподівані керівники сервісів. Цей запит шукає замовників послуг, які були додані до будь-якої ролі (Додаток Б).

Цей запит призначений для отримання інформації про події в Cloud App (наприклад, Office 365), коли відбувається додавання користувача до ролі. Запит використовує дані відповідного заходу "Add member to role" та фільтрує їх за певними умовами.

Основні критерії вибірки:

Timestamp > ago(queryTime): Обмеження часу настання події, де queryTime -змінна, що представляє час в днях.

Application == "Office 365": Обмеження за додатком (в цьому випадку, Office365).

ActionType == "Add member to role.": Фільтрація за типом дії, конкретно "Add

member to role."

Розширення (extend) дані за допомогою полів, таких як EntityType, RoleName,RoleId, отриманих із RawEventData.

where EntityType == "ServicePrincipal": Обмеження за типом сутності, де ServicePrincipal - сервісний принципал.

Вивід (project) конкретних полів для подальшого використання.

Отже, результати запиту включають час події (Timestamp), тип дії (ActionType), інформацію про сервісний принципал (ServicePrincipalName, ServicePrincipalId) та роль (RoleName, RoleId), а також дані про актора (ActorId, ActorDisplayName).

Ухилення від оборони. Зловмисник намагається уникнути виявлення. Ухилення від захисту складається з методів, які зловмисники використовують, щоб уникнути виявлення протягом усього процесу компрометації. Методи, що використовуються для обходу захисту, включають видалення/відключення програмного забезпечення для забезпечення безпеки або приховування/шифрування даних і скриптів. Зловмисники також використовують і зловживають довіреними процесами, щоб приховати і замаскувати своє шкідливе програмне забезпечення .

Виявлення використання альтернативних потоків даних. Цей запит спочатку був опублікований у звіті з аналітики загроз "Програми- вимагачі продовжують вражати медичні та критичні служби". Існує також відповідний блог.

У квітні 2020 року дослідники безпеки помітили кілька кампаній зловмисників, які використовували один і той же набір методів.

Наступний запит виявляє підозріле використання альтернативних потоків даних (ADS), що може свідчити про спробу маскування шкідливої активності. Відомо, що такі кампанії розгортають програми-здирники в пам'яті та використовують ADS (Додаток В).

Цей запит призначений для виявлення використання альтернативних потоків даних (Alternate Data Streams) та виконання команд в системі. Давайте розглянемо основні кроки:

DeviceProcessEvents: Використання даних подій процесів на пристрої. Timestamp > ago(7d): Фільтрація подій, що сталися протягом останніх 7 днів.

ProcessCommandLine startswith "-q -s" and ProcessCommandLine hasprefix "-p": Фільтрація процесів за командним рядком, який починається з "-q -s" та має префікс"-p".

not(FolderPath has_any("visual studio", "ide")): Виключення процесів, пов'язаних з інтегрованими середовищами розробки (IDE), такими як "visual studio"та "ide".

summarize make_set(ProcessCommandLine), make_set(FolderPath), make_set(InitiatingProcessCommandLine) by DeviceId, bin(Timestamp, 1h): Зведення результатів за допомогою унікальних множин командних рядків процесів, шляхів папок та командних рядків ініціюючих процесів для кожного пристрою та години.

Отже, результати запиту міститимуть інформацію про використання альтернативних потоків даних та командні рядки, що використовуються в системі, з виключенням процесів, пов'язаних з інтегрованими середовищами розробки.

Доступ до облікових даних. Зловмисник намагається викрасти імена та паролі облікових записів. Доступ до облікових даних складається з методів викрадення облікових даних,таких як імена та паролі облікових записів.

Методи, що використовуються для отримання облікових даних, включають перехоплення клавіатури або дамп облікових даних. Використання законних облікових даних може надати зловмисникам доступ до систем, ускладнити їхнє виявлення та надати можливість створити більше облікових записів для досягнення своїх цілей [14].

Спроби входу після отримання шкідливого листа.

Цей запит знаходить 10 останніх спроб входу в систему, здійснених

отримувачами протягом 30 хвилин після того, як вони отримали відомий шкідливий лист. Ви можете використовувати цей запит, щоб перевірити, чи були скомпрометовані акаунти одержувачів.

Спроби входу після отримання шкідливого листа можуть свідчити про те, щоакаунт скомпрометований або знаходиться в процесі компрометації (Додаток Г).

Цей запит створений для пошуку входжень в систему, які сталися безпосередньо після того, як виявлено зловмисний електронний лист. Ось розшифровка кожного кроку:

let MaliciousEmail: Запитує всі електронні листи, в яких виявлено загрози, зокрема, вони мають позначку "Malware". Результати проектуються на поля, такі якчас (Timestamp), тема (Subject), адреса відправника (SenderFromAddress) та ім'я облікового запису (AccountName).

join (IdentityLogonEvents ...): Проводить з'єднання отриманих даних про зловмисні електронні листи з подіями входження в систему (IdentityLogonEvents). Два набори даних об'єднуються за іменем облікового запису.

| where (LogonTime - TimeEmail) between (0min.. 30min): Відбирає лише ті записи, де час входу в систему (LogonTime) стався відразу після виявлення зловмисного електронного листа (TimeEmail), протягом періоду 30 хвилин.

| take 10: Показує лише перші 10 результатів для спрощення виводу.

Отже, цей запит допомагає виявити входження в систему, які можуть бути пов'язані з отриманням зловмисного електронного листа, і виводить обмежену кількість (перші 10) таких входжень.

Виявлення.

Зловмисник намагається з'ясувати ваше середовище.

Виявлення складається з методів, які зловмисник може використовувати для отримання знань про систему та внутрішню мережу. Ці методи допомагають зловмисникам спостерігати за оточенням і зорієнтуватися, перш ніж вирішити, як діяти. Вони також дозволяють зловмисникам дослідити, що

вони можуть контролювати і що знаходиться навколо їхньої точки входу, щоб зрозуміти, як це може принести користь їхній поточній меті (Додаток Д).

Для збору інформації після компрометації часто використовуються вбудовані інструменти операційної системи .

Цей запит (детектор загрози) призначений для виявлення LDAP-запитів доActive Directory, які шукають чутливі об'єкти в організації

name: SensitiveLdaps: Це ім'я, яке присвоєно детектору загрози. Він може використовуватися для ідентифікації або звертання до цього детектора.

requiredDataConnectors: Вказує на необхідність конкретного конектора даних.

У цьому випадку, для використання цього детектора потрібний конектор данихMicrosoft Threat Protection.

connectorId: MicrosoftThreatProtection: Ідентифікатор конектора даних, якийвказує на використання Microsoft Threat Protection для збору даних.

dataTypes: IdentityQueryEvents: Зазначає типи даних, які необхідно використовувати. У цьому випадку, це IdentityQueryEvents, що, ймовірно, міститьінформацію про LDAP-запити.

query: Фактичний запит, який використовується для аналізу та виявлення чутливих LDAP-запитів. Використовуються умови, що перевіряють тип дії (ActionType), а також використовують parse для отримання деякої інформації з поляQuery .

Цей детектор загрози шукає LDAP-запити, які містять чутливі об'єкти чи фільтри в організації, такі як адміністратори, контролери доменів тощо. Цей LDAPзапит охоплює інструмент BloodHound (Додаток Е).

Цей запит на детектування використання торрент-програм або перегляд матеріалів, пов'язаних з торрентами, використовує дані з подій мережевої активностіпристрою. Основні етапи запиту наступні:

DeviceNetworkEvents: Використовує дані подій мережевої активності пристрою.

where Timestamp > ago(7d): Обмежує часовий діапазон подій -

враховуютьсялише ті, що відбулися протягом останніх 7 днів.

where RemoteUrl has "torrent" or RemoteUrl has "vuze" or RemoteUrl has "azureus" or RemoteUrl endswith ".tor": Обмежує події, де URL містить ключові слова, пов'язані з торрентами чи закінчується на ".tor".

or InitiatingProcessFileName has "torrent" or InitiatingProcessFileName has "vuze" or InitiatingProcessFileName contains "azureus": Додає умови для ім'я ініціюючого процесу - визначає події, де ім'я процесу містить ключові слова, пов'язані з торрентами.

project Timestamp, ReportId, DeviceId, DeviceName, InitiatingProcessFileName, RemoteUrl, RemoteIP, RemotePort: Вибирає конкретні поля для подальшого вивчення

- час події, ідентифікатор звіту, ідентифікатор пристрою, ім'я пристрою, ім'я ініціюючого процесу, URL віддаленої ресурсу, IP-адресу віддаленого сервера тапорт.

Отримані дані дозволяють виявляти активність, пов'язану з торрентами на пристроях в мережі (Додаток Ж).

Виявлення LDAP-запитів Active Directory, які намагаються знайти операційнісистеми, вразливі до певних уразливостей

Цей LDAP запит охоплює MetaSploit - інструмент enum_ad_computers let ComputerObject = "objectCategory=computer";, let ComputerClass =

"objectClass=computer";, let SamAccountComputer = "sAMAccountType=805306369";, let OperatingSystem = "operatingSystem=";: Визначає константи для рядків, які вказують на об'єкти комп'ютерів, їх клас, тип облікового запису та операційну систему. "sAMAccountType=805306369" - під час створення нових комп'ютерних об'єктів за допомогою з'єднувача Active Directory нові комп'ютери створюються з параметром sAMAccountType з 805306369, який є обліковим записом комп'ютера/акаунт хоста.

IdentityQueryEvents: Використовує дані подій запитів ідентичності. where ActionType == "LDAP query": Обмежується лише подіями LDAP-

запитів.

parse Query with * "Search Scope: " SearchScope ", Base Object:" BaseObject ", Search Filter: " SearchFilter: Використовує команду parse для розбору поля Query та виділення інформації про область пошуку, базовий об'єкт та фільтр пошуку.

where (SearchFilter contains ComputerObject or SearchFilter contains ComputerClass or SearchFilter contains SamAccountComputer) and SearchFilter contains OperatingSystem: Визначає умови, щоб визначити, чи містить фільтр пошуку інформацію про об'єкти комп'ютерів, їх клас, тип облікового запису та операційну систему.

Цей запит може допомогти виявити LDAP-запити, які стосуються об'єктів комп'ютерів і містять інформацію про їхню операційну систему, що може вказуватина можливі вразливості цих комп'ютерів .

Бойовий рух. Супротивник намагається переміститися через ваше середовище.

Латеральне переміщення складається з методів, які противник використовує для входу в віддалені системи в мережі та контролю над ними. Досягнення їхньої основної мети часто вимагає дослідження мережі, щоб знайти свою ціль і згодом отримати доступ до неї. Досягнення їхньої мети часто передбачає проходження через безліч систем і облікових записів, щоб отримати вигоду. Зловмисники можуть встановлювати власні інструменти віддаленого доступу для здійснення латерального переміщення або використовувати законні облікові дані за допомогою інструментів мережі та операційної системи, що може бути більш непомітним.

ImpersonatedUserFootprint.

Azure ATP сповіщає про підозрілі квитки Kerberos, вказуючи на потенційну атаку перебору хешу. Отримавши облікові дані користувача з вищими привілеями, зловмисники використовують їх для входу на інші пристрої та переміщення по мережі. Цей запит знаходить пов'язані події входу в систему після атаки перебору хешу, щоб відстежити слід користувача, який видає себе за іншого.

Зловмисники можуть "передати хеш", використовуючи викрадені хеші паролів, щоб переміщатися в середовищі в обхід звичайних системних засобів контролю доступу. Передача хешу (PtH) - це метод автентифікації користувача без доступу до його відкритого паролю. Цей метод обходить стандартні етапи автентифікації, які вимагають введення відкритого тексту пароля, переходячи безпосередньо до тієї частини автентифікації, яка використовує хеш-пароль.

При виконанні PtH дійсні хеші паролів для облікового запису, що використовується, перехоплюються за допомогою методу доступу за обліковими даними. Захоплені хеші використовуються у PtH для автентифікації від імені цього користувача. Після автентифікації PtH можна використовувати для виконання дій налокальних або віддалених системах (Додаток К).

Зловмисники також можуть використовувати викрадені хеші паролів, щоб "обійти хеш". Подібно до PtH, це передбачає використання хешу пароля для автентифікації в якості користувача, але також використовує хеш пароля для створення дійсного квитка Kerberos. Цей квиток може бути використаний для проведення атаки Pass the Ticket [15].

Цей запит призначений для виявлення підозрілих атак типу "overpass-the-hash"(Kerberos). Основні етапи запиту наступні:

AlertInfo | where ServiceSource == "Azure ATP" | where Title == "Suspected overpass-the-hash attack (Kerberos)": Фільтрує дані інформації про сповіщення, щоб включити лише ті, які пов'язані зі службою Azure ATP та мають заголовок "Suspected overpass-the-hash attack (Kerberos)".

| extend AlertTime = Timestamp: Розширює дані, додаючи новий стовпець AlertTime, що містить час сповіщення.

| join (AlertEvidence | where EntityType == "User") on AlertId: Об'єднує дані інформації про сповіщення з даними підтвердження, вибираючи лише ті записи, деEntityType є "User".

| distinct AlertTime, AccountSid: Залишає унікальні записи, визначаючи лишеAlertTime і AccountSid.

| join kind=leftouter (DeviceLogonEvents | where LogonType == "Network"

and ActionType == "LogonSuccess" | extend LogonTime = Timestamp) on AccountSid: об'єднання з даними подій автентифікації на пристрої, вибираючи лише ті записи, де LogonType - "Network" і ActionType - "LogonSuccess". Розширює дані, додаючи новий стовпець LogonTime.

| where LogonTime between (AlertTime .. (AlertTime + 2h)): Обмежує результати, залишаючи тільки ті, де час логону знаходиться від AlertTime до (AlertTime + 2 години).

| project DeviceId, AlertTime, AccountName, AccountSid: Вибирає необхідні стовпці для виведення результатів, такі як ідентифікатор пристрою, час сповіщення,ім'я облікового запису та ідентифікатор облікового запису.

Цей запит допомагає виявити підозрілі дії, пов'язані з атаками "overpass-the-hash" (Kerberos), використовуючи дані про сповіщення та підтвердження, а також події увімкнення пристрою.

Командування та управління.

Зловмисник намагається встановити зв'язок зі скомпрометованими системами,щоб контролювати їх.

Командування та управління складається з методів, які зловмисники можуть використовувати для зв'язку з підконтрольними їм системами в мережі-жертві[14].

Зловмисники зазвичай намагаються імітувати нормальний, очікуваний трафік, щоб уникнути виявлення. Існує багато способів, за допомогою яких зловмисник може встановити командування і контроль з різним рівнем прихованості, залежно від структури мережі жертви та її захисту .

Виявити rundll.exe, який використовується для розвідки та управління.

Цей запит був вперше опублікований у звіті з аналітики загроз Trickbot: Повсюдний і недооцінений.

Trickbot - це дуже поширене шкідливе програмне забезпечення з широким спектром шкідливих можливостей. Спочатку розроблений для крадіжки банківських облікових даних, він перетворився на модульного трояна, який може розгортати інші шкідливі програми, виводити з ладу програмне

забезпечення для захисту та виконувати командно-контрольні операції (C2).Відомо, що оператори Trickbot використовують легальний процес Windows rundll.exe для виконання шкідливих дій, таких як розвідка. Після зараження цілі оператор скидає пакетний файл, який виконує кілька команд і підключається до сервера C2 для подальших дій.

Наступний запит виявляє підозрілу активність rundll.exe, пов'язану з кампаніями Trickbot (Додаток Л).

DeviceNetworkEvents | where InitiatingProcessFileName =~ "rundll32.exe": Фільтрує дані подій мережі, обираючи тільки ті, які мають InitiatingProcessFileNamерівне "rundll32.exe".

| where InitiatingProcessCommandLine has "rundll32.exe" and InitiatingProcessCommandLine !contains " " and InitiatingProcessCommandLine != "": Додає додаткові умови фільтрації для InitiatingProcessCommandLine, включаючи тільки ті записи, де командний рядок містить "rundll32.exe", не містить пробілів тане є порожнім.

| summarize DestinationIPCount = dcount(RemoteIP), make_set(RemoteIP), make_set(RemoteUrl), make_set(RemotePort) by InitiatingProcessCommandLine, DeviceId, bin(Timestamp, 5m): Узагальнює результати, обчислюючи кількість унікальних RemoteIP, а також створюючи множини унікальних RemoteIP, RemoteUrl та RemotePort для кожного InitiatingProcessCommandLine та пристрою. Додає бінування часу до 5 хвилин для агрегації результатів.

Отже, результат цього запиту надає інформацію про те, скільки унікальних IP-адрес, URL та портів було використано для кожного rundll32.exe вказаного пристрою протягом 5-хвилинних інтервалів.

Це правило можна віднести відразу до декількох тактик, а саме Discovery, Collection, Command and control.

Advanced Hunting є ефективним інструментом для виявлення шкідливих файлів та аналізу підозрілої активності. Різноманітні типи запитів дозволяють глибоко аналізувати дані та виявляти потенційні загрози. Великою перевагою цієї технології є його гнучкість та адаптабельність.

Це проявляється в можливості створення різноманітних запитів, адаптувати аналіз до різних сценаріїв та типів атак, як і було показано нами. Було наведено приклади використання Advanced Hunting для ефективного виявлення ШПЗ та неочікуваних векторів атак. Поєднання використання цієї технології разом з використанням регулярних оновлень та розвитку запитів дозволяє отримати комплексний сильний захист у боротьбі із загрозами.

Наведені приклади створюють можливість виявлення та вивчення взаємозв'язків між подіями, що сприяє покращенню стратегій виявлення та реагування на загрози. Цей розділ надав нам можливість не лише теоретично ознайомитись із можливостями використання Advanced Hunting, але й показати практичні зразки, які можна застосувати в реальних умовах. Це зробило роботу більш практично корисною та потенційно застосовною для фахівців у галузі кібербезпеки.

Наведені вище запити є лише прикладами того, як можна використовувати цю технологію. Кожна окрема організація має самостійно визначати спосіб та методи використання в залежності від рівня знань аналітиків з інформаційної безпеки, інших інтегрованих рішень пов'язаних з системами безпеки та технологіями, що використовуються. Як підсумок, варто зазначити певні рекомендації для організацій, що стосуються використання технології Advanced Hunting:

- Advanced Hunting є дуже потужним інструментом, тому очікуваною рекомендацією є використання цієї технології для постійного моніторингу та аналізу подій та даних в мережі та системі.
- Важливо навчити персонал володінню мовою запитів KQL для можливості створення власних запитів, що є адаптованими для конкретних потреб організації
- Створення ефективних виключень - це постійний та важливий процес, оскільки він допомагає виокремлювати легітимні та відомі процеси та застосунки, щоб зменшити кількість отримуваних FP сповіщень та попереджень.

- Наявність запиту не є гарантією успішного реагування. Варто не забувати про написання документацій, планів реагування, відповідальностей та процедур дій у випадку виявлення шкідливої активності.
- Використовуйте рішення Advanced Hunting в інтеграції з іншими системами безпеки для комплексного підходу до захисту.

Висновки до розділу

Advanced Hunting є ефективним інструментом для виявлення шкідливих файлів та аналізу підозрілої активності. Різноманітні типи запитів дозволяють глибоко аналізувати дані та виявляти потенційні загрози. Великою перевагою цієї технології є її гнучкість та адаптабельність. Це проявляється в можливості створення різноманітних запитів, адаптування аналізів до різних сценаріїв та типів атак, як і було показано нами. Було наведено приклади використання Advanced Hunting для ефективного виявлення ШПЗ та неочікуваних векторів атак. Наявні приклади було обрано і описано відповідно до бази знань MITRE ATT&CK®. Поєднання використання цієї технології разом з використанням регулярних оновлень та розвитку запитів дозволяє отримати комплексний сильний захист у боротьбі із загрозами. Наведені приклади створюють можливість виявлення та вивчення взаємозв’язків між подіями, що сприяє покращенню стратегій виявлення та реагування на загрози. Цей розділ надав нам можливість не лише теоретично ознайомитись із можливостями використання Advanced Hunting, але й показати практичні зразки, які можна застосувати в реальних умовах. Це зробило роботу більш практично корисною та потенційно застосовною для фахівців у галузі кібербезпеки.

ВИСНОВКИ

Магістерська робота представляє собою важливий внесок у галузь кібербезпеки, розглядаючи сучасні методи та засоби боротьби з шкідливим програмним забезпеченням (ШПЗ).

Метою нашого першого розділу було отримання розуміння природи ШПЗ, усвідомлення впливу різних загроз на інформаційні системи та дані, розуміння того як змінювалися методи та вигляд атак з плином часу. Ми розглянули декілька класифікацій, серед яких є більш широкі(спосіб поширення, та дії які шкідливі файли виконують коли досягають своєї цілі), та більш поширені та спеціалізовані(включали доволі розгорнутий список з шпигунських програм, вірусів, експлойтівв, з використанням викупів, руткіти, трояни, хробаки, криптомайнери і так далі)

Ми розглянули історичні відомості про ШПЗ, його перші згадування, якими воно було раніше, після чого перейшли до сучасності та розглянули більш сучасні атаки. Ключовим етапом розвитку та вважливою зміною стало розповсюджене використання наборів для атак, зміна джерел атак з індивідуальних зловмисників до організованих та небезпечних угрупувань та рівень кастомізації шкідливих файлів.

Детальний аналіз архітектури рішення Defender у другому розділі висвітлює ефективні методи виявлення ШПЗ та використання машинного навчання для посилення алгоритмів захисту. Порівняння з іншими рішеннями та результати тестувань розкривають переваги та особливості Defender у сучасному кіберсередовищі.

Основна частина роботи присвячена використанню технології Advanced Hunting для виявлення ШПЗ. В ній ми приводимо конкретні приклади використання запитів, що спрощують виявлення шкідливих файлів та підозрілої активності. Такий практичний підхід надає високий

рівень адаптації до конкретних потреб організації в галузі кібербезпеки.

Магістерська робота не тільки глибоко досліджує актуальні питання кібербезпеки, але й надає практичні приклади та рекомендації для застосування у сфері захисту інформації. Це може стати важливою допомогою фахівцям у розробці ефективних стратегій протидії шкідливому програмному забезпеченню в сучасних умовах кіберзагроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. William S. COMPUTER SECURITY: PRINCIPLES AND PRACTICE [Електронний ресурс] / S. William, B. Lawrie // UNSW Canberra at the Australian Defence Force Academy. – 2017. – Режим доступу до ресурсу: https://www.mcu.edu.ng/home/wp-content/uploads/2023/11/Computer-Security-Principles-and-Practice-by-William-Stallings-Lawrie-Brown-z-lib.org_.pdf.

2. What is malware [Електронний ресурс] // Microsoft – Режим доступу до ресурсу: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-malware.

3. Ed Skoudis. Malware: Fighting Malicious Code / Ed Skoudis, Lenny Zeltser., 2003. – 672 с.

4. Murugiah Souppaya. Guide to Malware Incident Prevention and Handling for Desktops and Laptops / Murugiah Souppaya, Karen Scarfone., 2013.

5. The Global Risks Report – Geneva: World Economic Forum, 2023. – 97 с.

6. Cost of a Data Breach Report [Електронний ресурс] // IBM. – 2023. – Режим доступу до ресурсу: https://www.ibm.com/reports/data-breach.

7. Internet Organised Crime Threat Assessment [Електронний ресурс] // European Union Agency for Law Enforcement Cooperation. – 2023. – Режим доступу до ресурсу:https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA%202023%20-%20EN_0.pdf.

8. Heike Ritter. Become a Microsoft Defender for Endpoint Ninja [Електронний ресурс] / Heike Ritter // Micro. – 2020. – Режим доступу до ресурсу: https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/become-a-microsoft-defender-for-endpoint-ninja/ba-p/1515647.

9. Microsoft Defender for Endpoint [Електронний ресурс] // Microsoft 365. – 2023. – Режим доступу до ресурсу: https://learn.microsoft.com/en-

us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint?view=o365-worldwide.

10. Evaluate and pilot Microsoft Defender XDR [Електронний ресурс] // Microsoft 365. – 2023. – Режим доступу до ресурсу: https://learn.microsoft.com/en-us/microsoft-365/security/defender/eval-overview?view=o365-worldwide.

11. Review Microsoft Defender for Endpoint architecture requirements and key concepts [Електронний ресурс] // Microsoft 365. – 2023. – Режим доступу до ресурсу: https://learn.microsoft.com/en-us/microsoft-365/security/defender/eval-defender-endpoint-architecture?view=o365-worldwide.

12. Summary Report [Електронний ресурс] // AV-Comparatives. – 2022. – Режим доступу до ресурсу: https://www.av-comparatives.org/tests/summary-report-2022/#microsoft.

13. AV-TEST Product Review and Certification Report [Електронний ресурс] // The Independent IT-Security Institute. – 2023. – Режим доступу до ресурсу: https://www.av-test.org/en/antivirus/business-windows-client/windows-11/october-%202023/microsoft-defender-antivirus-enterprise-4.18-232514/.

14. Sample queries for Advanced hunting in Microsoft 365 Defender [Електронний ресурс] // Microsoft. – 2020. – Режим доступу до ресурсу: https://github.com/microsoft/Microsoft-365-Defender-Hunting-Queries.

15. Use Alternate Authentication Material: Pass the Hash [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://attack.mitre.org/techniques/T1550/002/.

16. Aycock, J. Computer Viruses and Malware. New York: Springer, 2006.

ДОДАТКИ

Додаток А

Possible IP scan

```
DeviceNetworkEvents
|where RemoteIP matches regex @"(^10\.[0-9]{1,3}|172\.(3[01]|2[0-
9]|1[6- 9])|192\.168)\.[0-9]{1,3}\.[0-9]{1,3}" and
InitiatingProcessCreationTime > ago(1h)
//EXCLUSIONS:
| where InitiatingProcessFileName !in ("chrome.exe", "Google
Chrome Helper","firefox.exe", "opera.exe", "vivaldi.exe"
| where InitiatingProcessFolderPath !in ()
| where not (DeviceName contains "" and InitiatingProcessFolderPath contains
@"")
//"END_EXCLUSIONS.
|summarize (Timestamp, ReportId)=arg_max(Timestamp,
ReportId), RemoteIPCount=dcount(RemoteIP) by DeviceName,
DeviceId, InitiatingProcessFolderPath, InitiatingProcessFileName,
InitiatingProcessId,InitiatingProcessCreationTime
|where RemoteIPCount > 20
```

Додаток Б

ServicePrincipalAddedToRole

```
let
queryTime = 1d;
CloudAppEvents
| where Timestamp > ago(queryTime)
| where Application == "Office 365"
| where ActionType == "Add member to role."
| extend EntityType = RawEventData.Target[2].ID,
RoleName =
RawEventData.ModifiedProperties[1].NewValue,
RoleId =
RawEventData.ModifiedProperties[2].NewValue
| where EntityType == "ServicePrincipal"
| project Timestamp , ActionType, ServicePrincipalName =
RawEventData.Target[3].ID,ServicePrincipalId = RawEventData.Target[1].ID,
RoleName, RoleId, ActorId = AccountObjectId , ActorDisplayName =
AccountDisplayName
```

Додаток В

Detect use of Alternate Data Streams

```
// Alternate Data Streams
executionDeviceProcessEvents
| where Timestamp > ago(7d)
// Command lines used
| where ProcessCommandLine startswith "-q -s" and ProcessCommandLine hasprefix
"-p"
// Removing IDE processes
and not(FolderPath has_any("visual studio", "ide"))
| summarize make_set(ProcessCommandLine), make_set(FolderPath),
make_set(InitiatingProcessCommandLine) by DeviceId, bin(Timestamp, 1h)
```

Додаток Г

Logon attempts after receive of malicious email

```
//Find logons that occurred right after malicious email
was receivedlet MaliciousEmail=EmailEvents
| where ThreatTypes has_cs "Malware"
| project TimeEmail = Timestamp, Subject, SenderFromAddress, AccountName =
tostring(split(RecipientEmailAddress, "@")[0]);
MaliciousEmail
| join (
IdentityLog
onEvents
| project LogonTime = Timestamp, AccountName, DeviceName
) on AccountName
| where (LogonTime - TimeEmail) between (0min.. 30min)
| take 10
```

Додаток Д

SensitiveLdaps

```
name:
SensitiveLdaps
requiredDataCo
nnectors:
- connectorId:
  MicrosoftThreatProtection
  dataTypes:
  -
IdentityQuery
Eventsquery: |
  let SensitiveObjects = "[\"Administrators\", \"Domain Controllers\",
\"DomainAdmins\", \"Account Operators\", \"Backup Operators\",
\"DnsAdmin\", \"Enterprise Admins\", \"Group Policy Creator Owners\"]";
  IdentityQueryEvents
  | where ActionType == "LDAP query"
  | parse Query with * "Search Scope: " SearchScope ", Base Object:"
BaseObject ",Search Filter: " SearchFilter
  | where SensitiveObjects contains QueryTarget or
SearchFilter contains"admincount=1"
```

Додаток Е

DetectTorrentUse

name:
DetectTorrentU
se
requiredDataCo
nnectors:
- connectorId:
  MicrosoftThreatProtection
  dataTypes:
  -
DeviceNetwork
Eventsquery: |
DeviceNetwork
Events
  | where Timestamp > ago(7d)

  | where RemoteUrl has "torrent" or RemoteUrl has "vuze" or RemoteUrl has "azureus" or RemoteUrl endswith ".tor" or InitiatingProcessFileName has "torrent" or InitiatingProcessFileName has "vuze" or InitiatingProcessFileName contains "azureus"

  | project Timestamp, ReportId, DeviceId, DeviceName, InitiatingProcessFileName,RemoteUrl , RemoteIP , RemotePort

Додаток Ж

VulnerableComputers

```
name:
 VulnComputers
 requiredDataCo
 nnectors:
- connectorId:
  MicrosoftThreatProtection
  dataTypes:
  -
IdentityQuery
Eventsquery: |
  let ComputerObject =
  "objectCategory=computer";let
  ComputerClass =
  "objectClass=computer";
  let SamAccountComputer =
  "sAMAccountType=805306369";let
  OperatingSystem = "operatingSystem=";
  IdentityQueryEvents
  | where ActionType == "LDAP query"
  | parse Query with * "Search Scope: " SearchScope ", Base Object:"
  BaseObject ",Search Filter: " SearchFilter
  | where (SearchFilter contains ComputerObject or
SearchFilter containsComputerClass or SearchFilter contains
SamAccountComputer) and
   SearchFilter contains OperatingSystem
```

Додаток К

ImpersonatedUserFootprint

```
        lertInfo
| where ServiceSource == "Azure ATP"
| where Title == "Suspected overpass-the-hash attack (Kerberos)"
| extend AlertTime = Timestamp
| join
(
      AlertEvidence
         | where EntityType == "User"
   )
   on AlertId
| distinct AlertTime,AccountSid
| join
kind=leftouter(
      DeviceLogonEvents
      | where LogonType == "Network" and ActionType == "LogonSuccess"
      | extend LogonTime = Timestamp
   )
   on AccountSid
| where LogonTime between (AlertTime .. (AlertTime + 2h))
| project DeviceId , AlertTime , AccountName , AccountSid
```

Додаток Л

Recon with rundll.exe

```
    DeviceNetworkEvents
| where InitiatingProcessFileName =~ "rundll32.exe"
// Empty command line
| where InitiatingProcessCommandLine has "rundll32.exe" and
InitiatingProcessCommandLine !contains " "
and InitiatingProcessCommandLine != ""
| summarize DestinationIPCount = dcount(RemoteIP), make_set(RemoteIP),
make_set(RemoteUrl),
make_set(RemotePort) by InitiatingProcessCommandLine, DeviceId, bin(Timestamp, 5m)
```