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

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Дослідження шляхів і розробка рекомендацій щодо зменшення часу реагування на APT атаки на робочих станціях на основі ESET Protect та Inspect»

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

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

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

_____ Артем МУРАВЙОВ
(підпис)

Виконав: здобувач вищої освіти групи БСД-42
МУРАВЙОВ Артем
(прізвище, ім'я)

Керівник д.ф. доцент, МАРЧЕНКО Віталій
(науковий ступінь, вчене звання, прізвище, ім'я)

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

Київ 2024

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

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

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

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Муравйова Артема Євгеновича
(прізвище, ім’я)

1. Тема кваліфікаційної роботи: «Дослідження шляхів та розробка рекомендацій щодо зменшення часу реагування на APT атаки на робочих станціях на основі ESET Protect та Inspect»

керівник кваліфікаційної роботи д.ф. доцент, МАРЧЕНКО Віталій.
(прізвище, ім’я, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від «_27_» _лютого_ 2024 року № __36__.

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

3. Вихідні дані до кваліфікаційної роботи
наукова та технічна література, дослідницькі статті, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Аналіз проблеми виявлення APT атак
2. Дослідження методів виявлення та пом’якшення протидії APT атакам
3. Розробка рекомендацій щодо зменшення часу реагування на APT атаки на робочих станціях

5. Перелік графічного матеріалу
Презентація PowerPoint.

6. Дата видачі завдання 15.04.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення актуальності проблеми виявлення APT атак	27.02.2024 р.	
2.	Аналіз наукової та технічної літератури з питань теми кваліфікаційної роботи.		
3.	Аналіз проблематики виявлення та пом’якшення протидії APT атакам		
4.	Аналіз наявних рішень методитик та підходів протидії APT атакам		
5.	Розробка рекомендацій щодо зменшення часу реагування на APT атаки на робочих станціях		
6.	Оформлення результатів дослідження.		
7.	Підготовка доповіді до захисту.	31.05.2024 р.	

Здобувач вищої освіти _____ Артем МУРАВЙОВ
(підпис) *(ім’я, прізвище)*

Керівник кваліфікаційної роботи _____ Віталій МАРЧЕНКО
(підпис) *(ім’я, прізвище)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу

здобувача МУРАВЙОВА Артема

на тему: «Дослідження шляхів і розробка рекомендацій щодо зменшення часу реагування на APT атаки на робочих станціях на основі ESET Protect та Inspect»

Актуальність: Дослідження шляхів і розробка рекомендацій щодо зменшення часу реагування на APT атаки на робочих станціях на основі ESET Protect та Inspect є актуальним через зростання складності та тривалості кіберзагроз, які можуть залишатися непоміченими протягом тривалого часу, завдаючи значних збитків. Використання сучасних технологій, таких як ESET Protect та Inspect, дозволяє автоматизувати процеси виявлення та реагування, забезпечуючи моніторинг у реальному часі та детальний аналіз загроз. Це значно скорочує час реакції на інциденти, мінімізує ризики поширення загроз та підвищує загальний рівень кібербезпеки організації, забезпечуючи надійний захист робочих станцій від передових персистентних загроз.

Актуальність теми дипломної роботи визначається сучасними тенденції розвитку міст та обробкою даних

Позитивні сторони:

1. Робота забезпечує детальне дослідження проблеми захисту ключових аспектів та процесів роботи розумних міст та дає високорівневий огляд на запропоновані рішення.
2. Методи і засоби розглянуті в кваліфікаційній роботі є актуальними та враховують сучасні кращі практики.
3. Представлено практичні рекомендації щодо підвищення рівня захищеності інформаційного середовища розумних міст.
4. Текст роботи чітко структурований, містить послідовне і грамотне викладення матеріалу. Висновки сформульовані змістовно і чітко.
5. Ефективність розроблених рекомендацій частково може бути підтверджена з допомогою аналізу подібних рішень в корпоративному середовищі.

Недоліки:

1. Аналіз та проведення реального випробування для тестування запропонованих рішень підвищив би рівень якості роботи.
2. У роботі могла б бути більш детально розроблена методика інтеграції запропонованих рішень, що дозволило б виявити потенційні перешкоди та визначити оптимальні підходи для різних типів проектів.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота заслуговує оцінку **“відмінно”**, а здобувач **МУРАВЙОВ Артем** – присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Інформаційна та кібернетична безпека

Рецензент:

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

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

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ

на здобуття освітнього ступеня бакалавра

Направляється здобувач МУРАВЙОВ Артем до захисту кваліфікаційної роботи
(прізвище, ім'я)

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

на тему: «Дослідження шляхів і розробка рекомендацій щодо зменшення часу реагування на APT атаки на робочих станціях на основі ESET Protect та Inspect».

Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач ***МУРАВЙОВ Артем*** обрав для своєї роботи тему, спрямовану на дослідження методів зменшення часу реагування на APT атаки на робочих станціях на основі ESET Protect та Inspect. Вибір і опрацювання наукових джерел свідчать про його глибоке розуміння теми та здатність адаптувати нові рішення в контекст вирішення питань безпеки інформаційного середовища розумних міст. Протягом всього процесу виконання дипломної роботи ***МУРАВЙОВ Артем*** проявив серйозний підхід, самостійність у розв'язанні складних питань і вчасно виконав всі заплановані завдання.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача ***МУРАВЙОВА Артема*** на оцінку **"відмінно"** та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Інформаційна та кібернетична безпека.

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

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач **МУРАВЙОВ Артем** допускається до захисту даної кваліфікаційної роботи в Екзаменаційній комісії.

Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

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

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 49 сторінок, 11 рисунки, 28 джерел.

Об'єкт дослідження – процес забезпечення зменшення часу реагування на APT атаки.

Предмет дослідження – методи та засоби зменшення часу реагування на APT атаки.

Мета роботи – розробити рекомендації щодо застосування новітніх практик та покращення існуючих механізмів реагування на APT атаки.

Методи дослідження – опрацювання технічної літератури та наукових джерел для з'ясування основних принципів сучасних методів реагування на APT атаки; порівняльний аналіз рішень для захисту кінцевих точок від APT атак; визначення ключових аспектів захисту; теоретичний розгляд нових методів захисту у контексті зменшення часу реагування на APT атаки.

Дослідження шляхів і розробка рекомендацій щодо зменшення часу реагування на APT атаки на робочих станціях на основі ESET Protect та Inspect є важливим завданням у контексті сучасного захисту організацій. Інформаційне середовище організацій включає різноманітні технології та системи, що взаємодіють для забезпечення ефективного управління ресурсами та безперебійної роботи. Разом із цим зростає необхідність у підвищенні рівня захисту цих систем від кіберзагроз.

У цьому дослідженні приділено особливу увагу сучасним методам захисту, які можуть бути застосовані для підвищення рівня безпеки в інформаційному середовищі організацій. Аналізовано технічну літературу та наукові джерела, проведено порівняльний аналіз різних рішень для захисту інформаційного середовища організацій. Визначено ключові аспекти захисту та теоретично розглянуто нові методи захисту у цьому контексті.

В результаті дослідження розроблено рекомендації щодо підвищення рівня захисту інформаційного середовища організацій. Практичне застосування результатів моєї роботи може знайти використання у різних проєктах, де критично

важливим є забезпечення надійності і безпеки інформаційних систем..

Галузь використання – кібербезпека інформаційних ресурсів організації.

КІБЕРБЕЗПЕКА, APT, XDR, EDR, SIEM, МОНІТОРИНГ БЕЗПЕКИ.

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

APT	—	просунута стійка загроза
EDR	—	виявлення та реагування на кінцевих точках
IDS	—	система виявлення вторгнень
IPS	—	система запобігання вторгнень
SIEM	—	управління інформацією та подіями безпеки
UBA	—	аналіз поведінки користувачів
UEBA	—	аналіз поведінки користувачів та об'єктів
XDR	—	розширене виявлення та реагування
IOC	—	індикатори компрометації

ВСТУП

Актуальність дослідження. Забезпечення безпеки інформаційного середовища організацій є критично важливим у сучасних умовах зростання кіберзагроз та підвищеної цифровізації. Інформаційне середовище організацій покладається на різноманітні технології, що взаємодіють для ефективного управління ресурсами та забезпечення стабільної роботи. Дослідження шляхів забезпечення безпеки та розробка рекомендацій дозволяє своєчасно виявляти потенційні загрози, мінімізувати ризики кіберінцидентів та забезпечити стабільну і безпечну роботу організаційної інфраструктури, підвищуючи загальний рівень безпеки та ефективності.

Проте, попри наявність сучасних інструментів та методик, питання інтеграції адаптивних підходів у процеси забезпечення безпеки інформаційного середовища організацій залишається недостатньо дослідженим. Це створює прогалини у захисних алгоритмах, особливо в умовах швидкого розвитку технологій та зростання кількості кіберзагроз. У цьому контексті, дослідження, спрямоване на аналіз та розробку рекомендацій щодо ефективного використання адаптивних підходів для підвищення безпеки інформаційного середовища організацій, стає актуальним.

Робота над цією темою дозволить не тільки систематизувати наявні знання та найкращі практики по забезпеченню захисту інформаційного середовища організацій, але й допоможе подальшим фахівцям кібербезпеки розвивати та досліджувати цю тему глибше.

Об'єкт дослідження – процес забезпечення зменшення часу реагування на APT атаки.

Предмет дослідження – методи та засоби зменшення часу реагування на APT атаки.

Мета роботи – розробити рекомендації щодо застосування новітніх практик та покращення існуючих механізмів реагування на APT атаки.

Наукові завдання:

Визначити ключові аспекти для захисту від APT атак.

Проаналізувати існуючі методології та рекомендації для захисту від сучасних APT загроз.

Визначити вимоги до рішень, які можуть використовуватись для захисту в інформаційному середовищі організацій.

Розробити рекомендації щодо підвищення рівня безпеки інформаційного середовища організацій та держустанов в контексті захисту від APT атак.

Методи дослідження – опрацювання тематичної літератури, інтернет-джерел, аналіз наукових досліджень, міжнародних стандартів та їх порівняння.

Практичне значення одержаних результатів: розроблено щодо зменшення часу реагування на APT атаки на робочих станціях на основі сучасних рішень. Методи реалізації сучасних стандартів та практик по підвищенню захисту інформаційного середовища організацій та держустанов.

1 АНАЛІЗ ПРОБЛЕМИ ВИЯВЛЕННЯ APT АТАК

1.1 Поняття APT атак та їх характеристики

Кібератака – це будь-яка спроба зловмисників отримати несанкціонований доступ до комп'ютерних систем, мереж або пристроїв з метою завдання шкоди, викрадення інформації або порушення нормального функціонування [1]. Такі атаки можуть бути спрямовані на приватні особи, компанії або державні установи та включати різноманітні методи, такі як фішинг, соціальна інженерія, експлуатація вразливостей програмного забезпечення та інші.

Захист від кібератак є критично важливим з кількох причин. По-перше, кібератаки можуть призвести до викрадення особистих даних, фінансової інформації, комерційних таємниць та іншої конфіденційної інформації, що може мати серйозні наслідки для приватності та безпеки. По-друге, атаки можуть спричинити значні фінансові втрати через викрадення коштів, витрати на відновлення систем та виплати штрафів за порушення законодавства про захист даних. По-третє, порушення безпеки може призвести до втрати довіри клієнтів, партнерів та громадськості, що негативно вплине на імідж організації. Крім того, кібератаки можуть спричинити збої в роботі критично важливих систем, що призведе до зупинки бізнес-процесів та зниження продуктивності. Для державних установ кібератаки можуть становити загрозу національній безпеці, особливо якщо вони спрямовані на критичну інфраструктуру. Таким чином, захист від кібератак є необхідним для забезпечення безпеки інформації, фінансової стабільності, підтримки репутації та безперервності діяльності організацій.

Одним з найнебезпечніших видів кібератак є APT атаки (Advanced Persistent Threats), або цільові атаки [2]. Ці атаки характеризуються високим рівнем складності та тривалим періодом активності, що дозволяє зловмисникам залишатися непоміченими протягом тривалого часу. Цільові атаки спрямовані на конкретні організації або навіть їх окремі підрозділи з метою викрадення конфіденційної інформації, саботажу або завдання інших видів шкоди. У

наступних розділах ми розглянемо поняття APT атак детальніше, а також їхні характеристики та основні методи, що використовуються для їх здійснення.

Цільова атака, вона ж APT атака, завжди спрямована на конкретну організацію чи навіть її ланку. Така атака ніколи не є масовою і завжди є несподіваною, що обходить захист від більшості стандартних атак. Такі атаки готуються тривалий термін, для їх підготовки залучаються значні ресурси APT організації чи її спонсора. Цілями такої атаки обираються великі організації, державні відомства. Менші цілі не є вигідними для такого рівня залучення ресурсів.

Зазвичай для конкретної атаки розробляється окремий інструментарій, що не зустрічався раніше. Такий інструментарій має на меті або дослідити інфраструктуру цілі атаки, або експлуатувати вразливості, що були знайдені APT угрупуванням. Зазвичай це вразливості нульового дня у інформаційних системах чи обладнанні.

Для проникнення всередину інфраструктури можуть використовуватись як більш класичні методи, орієнтовані на людський фактор, такі як фішинг у різних проявах чи соціальна інженерія, так і знайдені вразливості у тій частині інфраструктури цілі, що може бути експлуатована ззовні. Також для проникнення чи самої атаки може використовуватись напад на ланцюжок постачання.

Цільові атаки, або APT атаки, можна класифікувати за різними критеріями, зокрема за метою, джерелом фінансування та використовуваними методами. З точки зору мети, APT атаки можуть переслідувати кілька цілей: збір інформації, саботаж робочих процесів або фінансове збагачення. Шпигунські атаки зазвичай спрямовані на отримання конфіденційної інформації про діяльність організацій, урядових установ або військових об'єктів. Саботажні атаки мають на меті порушення роботи критичних систем та інфраструктури. Атаки, мотивовані фінансовими цілями, зосереджені на викраденні фінансових ресурсів або вимаганні викупу. Також цілей атаки може бути декілька, в залежності від мети APT угрупування. Так, наприклад у грудні 2015 року Україна зазнала цілеспрямованої APT атаки, спрямованої на саботаж роботи її енергетичної інфраструктури [3]. Група зловмисників, відома як Sandworm, здійснила координаційну атаку на

електромережу країни, що призвело до відключення електроенергії для близько 230 тисяч споживачів [4].

Крім того, APT атаки можуть класифікуватися за джерелом фінансування. Державні атаки підтримуються урядами з метою отримання стратегічної переваги та збору розвідувальної інформації. Прикладом такої атаки є атака на Демократичний національний комітет (DNC) у 2016 році, здійснена групою APT28, яку пов'язують з російською військовою розвідкою (ГРУ). Кримінальні угрупування фінансують атаки з метою отримання фінансової вигоди через викрадення даних, вимагання або інші злочинні дії. Активістські атаки, або хактивізм, здійснюються групами, які прагнуть досягнення політичних або соціальних цілей, часто за допомогою атак на корпоративні або урядові структури.

З точки зору технік і методів, що використовуються під час APT атак, зловмисники можуть застосовувати різні підходи. Фішинг та соціальна інженерія є одними з найпоширеніших методів для отримання початкового доступу до систем. Зловмисники використовують соціальну інженерію, щоб обманом змусити користувачів надати їм облікові дані або іншу конфіденційну інформацію, або запустити шкідливий файл, що був доставлений електронною поштою. Наприклад, під час атаки на українську електромережу у 2015 році, зловмисники використали фішингові листи, щоб отримати доступ до систем управління енергетичними підстанціями, що призвело до масштабних відключень електроенергії.

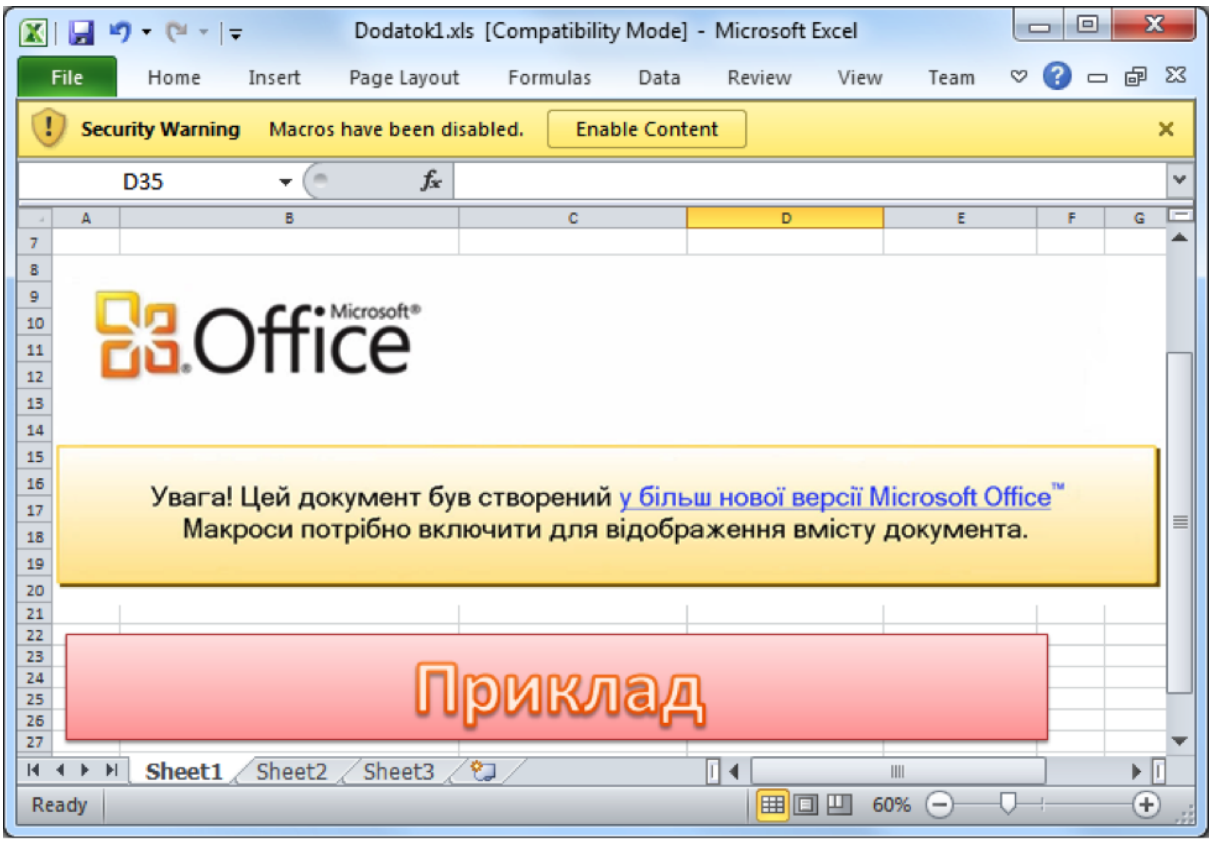

Рис. 1.1. Приклад зловмисного Excel файлу, що був використаний зловмисниками

Експлуатація вразливостей у програмному забезпеченні або обладнанні, особливо вразливостей нульового дня, є ще одним ефективним методом проникнення [5]. Зловмисники можуть використовувати невідомі раніше вразливості для проникнення в системи, перш ніж виробник випустить виправлення.

Крім того, атаки на ланцюжок постачання стають все більш поширеними, коли зловмисники проникають через вразливості у постачальників або партнерів. Одним із відомих прикладів є атака на українську компанію MeDoc у 2017 році. Зловмисники використали оновлення програмного забезпечення бухгалтерської системи MeDoc для розповсюдження шкідливого програмного забезпечення NotPetya, що призвело до значних фінансових збитків та порушення роботи багатьох компаній та урядових установ.

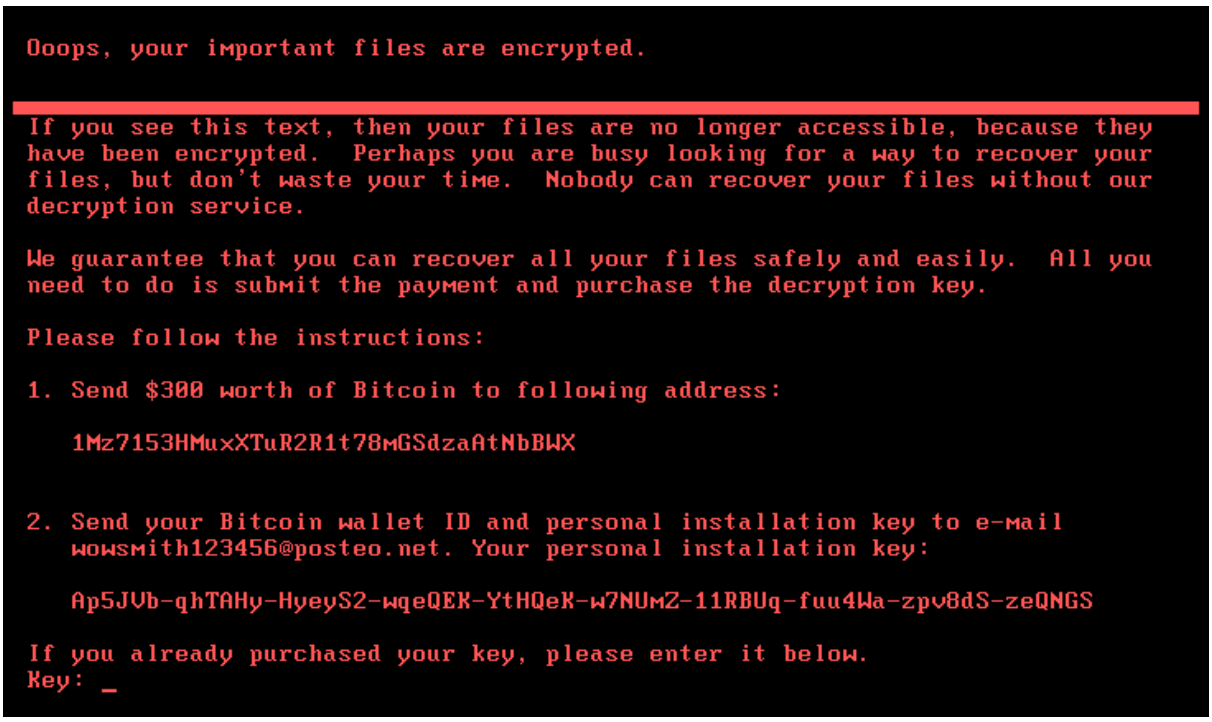

Рис. 1.2. Повідомлення, що виводилось Diskcoder.C на зашифрованих кінцевих точках

Таким чином, використання різних методів, таких як соціальна інженерія, експлуатація вразливостей нульового дня та атаки на ланцюжок постачання, демонструє високий рівень складності та небезпеку APT атак, що робить їх важким для виявлення та протидії.

1.2 Аналіз потенційних ризиків та шкідливих наслідків

Потенційними ризиками кібератак загалом і націлених атак, зокрема, є порушення бізнес-процесів, порушення цілісності або доступності конфіденційної інформації, фінансові та репутаційні збитки. У випадку націлених атак, таких як APT, ці ризики значно зростають через високий рівень складності та тривалий характер атак.

Порушення бізнес-процесів може включати збої в роботі критично важливих систем, що може призвести до втрати продуктивності, затримок у виконанні завдань та загального зниження ефективності компанії. Це, в свою чергу, може призвести до невиконання контрактних зобов'язань та втрати клієнтів.

Порушення цілісності або доступності конфіденційної інформації є особливо небезпечним, оскільки це може призвести до витоку важливих даних, таких як комерційні таємниці, особисті дані клієнтів та співробітників, фінансові звіти та інші критичні документи. Витік цієї інформації може бути використаний зловмисниками для шахрайства, шантажу або інших злочинних дій.

Фінансові збитки можуть виникнути через прямі витрати на відновлення систем, виплати компенсацій, штрафи за недотримання законодавства про захист даних та інші пов'язані витрати. Також можливі непрямі фінансові втрати, такі як зниження доходів через втрату клієнтів та інвесторів, які втратили довіру до компанії після інциденту.

Репутаційні збитки можуть бути ще серйознішими, оскільки вони впливають на довгострокову стійкість компанії на ринку. Втрата довіри клієнтів, партнерів та громадськості може призвести до тривалого зниження конкурентоспроможності та ринкової вартості компанії. Відновлення репутації після великого кіберінциденту може зайняти роки і вимагати значних ресурсів.

У листопаді 2014 року компанія Sony Pictures Entertainment зазнала масштабної APT атаки, яку здійснила хакерська група, відома як "Guardians of Peace" (GOP) [6]. Атака мала катастрофічні наслідки для компанії, зокрема репутаційні та фінансові збитки.

Зловмисники провели детальну розвідку, щоб зібрати інформацію про внутрішні системи компанії, співробітників та їх облікові дані. Використовуючи фішингові атаки та експлуатацію вразливостей, хакери отримали доступ до внутрішньої мережі Sony Pictures. Вони встановили бекдори та інші інструменти для збереження доступу до системи, навіть якщо первинний вектор атаки буде виявлений. Зловмисники розширили свої привілеї до адміністративного рівня, що дозволило їм отримати повний контроль над внутрішньою мережею компанії. Було зібрано величезну кількість конфіденційної інформації, включаючи особисті дані співробітників, фінансові звіти, комерційні таємниці, а також незапущені фільми. Зібрані дані були виведені з мережі компанії до серверів, контрольованих

зловмисниками. Хакери видалили або пошкодили внутрішні файли, щоб ускладнити розслідування атаки.

Наслідки атаки були руйнівними для Sony Pictures Entertainment. Репутаційні збитки були значними через витік особистих даних співробітників, включаючи їхні зарплати, соціальні номери та особисті листування. Це створило величезну негативну хвилю в медіа, що серйозно підірвало довіру до компанії. Крім того, витік планів щодо незапущених фільмів та іншої комерційної інформації призвів до зниження конкурентоспроможності компанії на ринку розваг.

Фінансові збитки були також суттєвими. Компанія зазнала значних прямих витрат на відновлення систем, проведення розслідувань, юридичні витрати та виплати компенсацій постраждалим. Зупинка бізнес-процесів та зниження продуктивності призвели до втрат доходів. Втрата довіри клієнтів та партнерів вплинула на фінансові показники компанії в довгостроковій перспективі.

Законодавчі наслідки теж мали місце. Компанія зіткнулася з численними перевірками з боку регулюючих органів, що додатково збільшило фінансові витрати та вплинуло на її репутацію. Співробітники та клієнти подали численні позови проти компанії через порушення конфіденційності їхніх даних, що створило додаткові юридичні проблеми та витрати.

Таким чином, потенційні ризики кібератак є багатогранними і можуть мати довгострокові наслідки для бізнесу. Це підкреслює важливість впровадження надійних засобів кіберзахисту та постійного вдосконалення систем безпеки для захисту від сучасних кіберзагроз.

1.3 Способи ініціації та поширення APT атак

Фішинг та соціальна інженерія є одними з найефективніших методів ініціації кібератак, оскільки вони спрямовані на найбільш вразливу ланку – людину [7].

Фішинг – це вид кібератаки, при якій зловмисники використовують підроблені повідомлення (зазвичай електронні листи або повідомлення в меседжерах), щоб змусити користувачів розкрити конфіденційну інформацію, таку

як облікові дані, фінансова інформація, інша чутлива інформація. Ці атаки часто виглядають як легітимні запити від надійних джерел. Фішинг може бути спрямований на конкретних осіб або групи, використовуючи інформацію добуту з відкритих джерел про них для створення більш переконливих повідомлень. Листи містять посилання на фальшиві веб-сайти, вкладення з шкідливим програмним забезпеченням, фальшиві інструкції. Коли користувачі виконують провоковану дію, вони можуть нанести .

Одним із найпоширеніших методів є фішинг та соціальна інженерія. Зловмисники використовують ці техніки для обману користувачів, щоб змусити їх розкрити конфіденційну інформацію або виконати шкідливі дії. Зазвичай це включає надсилання електронних листів, які виглядають як повідомлення від надійних джерел, але містять шкідливі посилання або вкладення. Наприклад, у 2016 році група зловмисників, відома як APT28 або Fancy Bear, використала фішингові листи для проникнення до мережі української Генеральної прокуратури. Це дозволило їм отримати доступ до конфіденційної інформації та викрасти важливі дані.

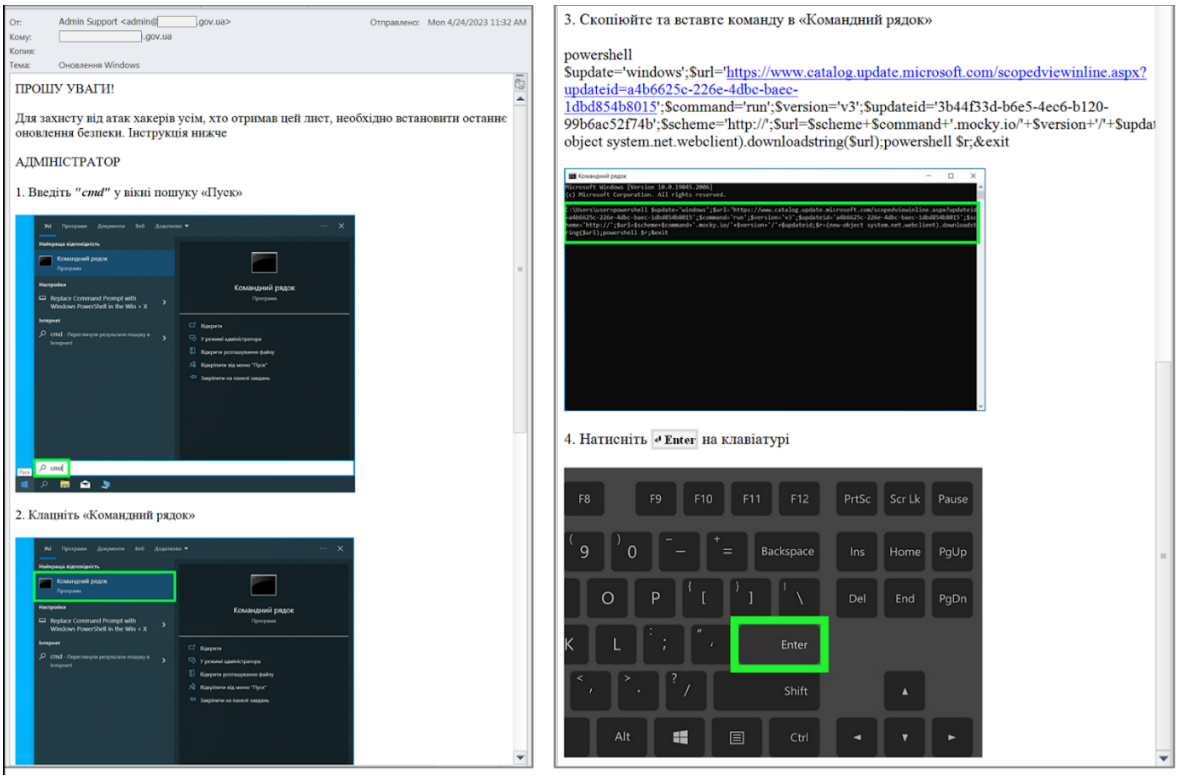

Рис. 1.3. Приклад використання фішингового повідомлення для виконання зловмисних команд користувачем

Іншим ефективним методом є експлуатація вразливостей у програмному забезпеченні або обладнанні. Вразливості – це помилки або слабкі місця в коді, які можуть бути використані зловмисниками для отримання несанкціонованого доступу до систем. Особливо небезпечними є вразливості нульового дня, які залишаються невідомими до моменту їх експлуатації, що дозволяє зловмисникам діяти без перешкод до випуску виправлення виробником. Зловмисники можуть використовувати автоматизовані сканери для пошуку вразливостей або цілеспрямовано шукати слабкі місця в програмному забезпеченні, яке використовується в організації.

Після виявлення вразливості вони розробляють експлоїти – спеціальні програми, які дозволяють використовувати ці вразливості для проникнення в систему, отримання підвищених привілеїв або виконання шкідливого коду. Експлуатація вразливостей є потужним інструментом, оскільки дозволяє зловмисникам проникати в системи без взаємодії з користувачами, часто залишаючись непоміченими до моменту нанесення значної шкоди.

Експлуатація вразливостей у програмному забезпеченні або обладнанні, особливо вразливостей нульового дня, є ще одним ефективним методом атаки. Зловмисники можуть використовувати невідомі раніше вразливості для проникнення в системи, перш ніж виробник випустить виправлення.

Наприклад, у 2017 році було зафіксовано атаку на українські держоргани, зокрема на Міністерство фінансів та Державне казначейство України, здійснену групою TeleBots. Зловмисники скористалися вразливостями у програмному забезпеченні, щоб отримати доступ до внутрішніх систем цих організацій. Вони встановили шкідливе програмне забезпечення, яке дозволило їм викрадати конфіденційну інформацію та порушувати роботу фінансових систем держави.

Рис. 1.4. Зображення, яке демонструвала шкідлива програма KillDisk під час атак

Крім того, атаки на ланцюжок постачання стають все більш поширеними. Зловмисники проникають через вразливості у постачальників або партнерів, що є частиною ланцюжка постачання. Такий підхід дозволяє зловмисникам проникнути в цільові системи через менш захищені точки доступу. Наприклад, у 2020 році було зафіксовано атаку на українську IT-компанію, що обслуговувала державні установи. Група зловмисників, відома як Gamaredon, використала оновлення програмного забезпечення для управління документами цієї компанії для розповсюдження шкідливого програмного забезпечення, що призвело до значних збоїв у роботі багатьох урядових організацій.

Рис. 1.5. Ланцюжок зараження Gamaredon

Використання компрометованих облікових даних є ще одним методом ініціації APT атак. Зловмисники можуть придбати ці дані на чорному ринку або отримати їх шляхом фішингу чи інших методів соціальної інженерії. Наприклад, у 2015 році група зловмисників, відома як APT29 або Cozy Bear, отримала доступ до систем Міністерства фінансів України, використовуючи компрометовані облікові дані. Це дозволило їм отримати доступ до конфіденційної інформації та викрасти важливі документи, що мало серйозні наслідки для національної безпеки.

У деяких випадках зловмисники можуть отримати фізичний доступ до цільових систем. Це може бути досягнуто через підкуп співробітників або інфільтрацію в організацію. Наприклад, у 2017 році група зловмисників отримала фізичний доступ до серверного приміщення однієї з українських енергетичних компаній. Вони встановили шкідливе обладнання для перехоплення даних та віддаленого управління системами, що дозволило їм здійснювати подальші атаки безпосередньо зсередини.

Таким чином, способи ініціації APT атак можуть бути різноманітними і складними, що робить їх важкими для виявлення та протидії. Використання методів, таких як фішинг, експлуатація вразливостей нульового дня, атаки на ланцюжок постачання, компрометовані облікові дані та фізичний доступ, демонструє високий рівень підготовки зловмисників та їх здатність обходити стандартні засоби захисту.

Висновки першого розділу

APT атаки є складними, цілеспрямованими та тривалими кібератаками, які використовують методи фішингу, соціальної інженерії та експлуатації вразливостей для проникнення в системи організацій. Ці атаки можуть завдати

значної шкоди, включаючи викрадення конфіденційних даних, фінансові втрати та порушення нормальної діяльності. Для ефективного захисту від APT атак необхідно застосовувати комплексний підхід, який включає як технічні засоби, так і організаційні заходи, щоб вчасно виявляти і нейтралізувати загрози.

2 ДОСЛІДЖЕННЯ МЕТОДІВ ВИЯВЛЕННЯ ТА ПОМ'ЯКШЕННЯ ПРОТИДІЇ APT АТАКАМ

2.1 Аналіз методів та інструментів виявлення та протидії APT атакам

Виявлення та протидія APT атакам є складним та багатогранним процесом, що вимагає застосування різноманітних методів і інструментів. Серед традиційних рішень для захисту від APT атак виділяються системи виявлення вторгнень (IDS) та системи управління подіями безпеки (SIEM). Проте сучасні технології, такі як Extended Detection and Response (XDR), пропонують інтегровані рішення, які можуть закрити потреби, які раніше покривали окремі IDS та SIEM системи.

Системи виявлення вторгнень (IDS)

IDS є одним із ключових інструментів у боротьбі з APT атаками. Вони можуть бути налаштовані для моніторингу мережевого трафіку та аналізу подій у реальному часі з метою виявлення підозрілої активності. Існує два основних типи IDS: мережеві (NIDS) та хостові (HIDS). NIDS моніторять трафік, що проходить через мережу, в той час як HIDS зосереджені на подіях, що відбуваються на окремих пристроях. IDS використовують підписні бази та алгоритми виявлення аномалій для ідентифікації потенційних загроз. Проте IDS мають обмежену здатність до виявлення нових та невідомих загроз і можуть генерувати велику кількість хибнопозитивних спрацьовувань, що ускладнює роботу персоналу.

Системи управління подіями безпеки (SIEM)

SIEM забезпечують централізоване збирання, аналіз та кореляцію подій безпеки з різних джерел у реальному часі. Вони дозволяють виявляти складні атаки, що можуть залишатися непоміченими при використанні окремих інструментів. SIEM використовують правила кореляції, що базуються на підписах та поведінковому аналізі, для ідентифікації підозрілих активностей та інцидентів безпеки. Проте, впровадження та обслуговування SIEM є дорогими і потребують значних ресурсів для аналізу та зберігання великих обсягів даних. Це може стати

викликом для багатьох організацій, особливо для тих, які мають обмежені бюджети або недостатньо кваліфікований персонал.

Extended Detection and Response (XDR) від ESET

Рішення ESET Inspect у складі ESET PROTECT представляє сучасний підхід до виявлення та реагування на загрози, який поєднує в собі переваги IDS та SIEM, забезпечуючи при цьому додаткові можливості. ESET Inspect інтегрує дані з різних джерел, включаючи кінцеві точки та мережеві пристрої, для комплексного виявлення загроз. Це дозволяє отримати повну картину стану безпеки організації та швидко реагувати на інциденти. Завдяки вбудованій у продукт безпеки обмеженій функціональності IDS, ESET Inspect може виявляти підозрілу активність на мережевому рівні, що значно підвищує рівень захисту. Хоча SIEM систему повністю замінити неможливо, ESET Inspect частково замінює її функціональність завдяки єдиним консолям керування EDR та XDR, які дозволяють централізовано збирати, аналізувати та корелювати події безпеки.

ESET Inspect забезпечує централізований збір і аналіз даних з кінцевих точок, мережевих пристроїв та інших систем, що дозволяє виявляти складні загрози, які можуть залишатися непоміченими при використанні окремих IDS або SIEM. Завдяки автоматизованим процесам аналізу та реагування, ESET Inspect значно скорочує час реакції на інциденти та знижує навантаження на персонал. Це досягається завдяки використанню розширених алгоритмів аналізу поведінки та кореляції подій, що дозволяє зменшити кількість хибнопозитивних спрацьовувань і підвищити ефективність роботи фахівців з безпеки.

Додатковою перевагою ESET Inspect є його масштабованість та гнучкість. Рішення легко масштабується відповідно до потреб організації та може бути інтегроване з іншими інструментами безпеки для забезпечення багаторівневого захисту. Використання ESET Inspect дозволяє зменшити витрати на впровадження та обслуговування окремих IDS та SIEM систем, оскільки всі необхідні функції інтегровані в єдину платформу. Це забезпечує економію коштів і спрощує процес управління безпекою, що є важливим фактором для організацій різного масштабу.

Таким чином, ESET Inspect у складі ESET PROTECT є ефективним рішенням для виявлення та протидії APT атакам, яке поєднує переваги традиційних IDS та SIEM систем, забезпечуючи при цьому додаткові можливості для захисту інфраструктури компаній. Це дозволяє організаціям не лише покращити свій рівень захисту, але й оптимізувати витрати на безпеку, зробивши процеси більш ефективними та керованими.

Інтрузивне виявлення (IDS)

Системи виявлення вторгнень (IDS) є одним з ключових інструментів у боротьбі з APT атаками [8]. Вони можуть бути налаштовані для моніторингу мережевого трафіку та аналізу подій у реальному часі з метою виявлення підозрілої активності.

Існує два основних типи IDS: мережеві (NIDS) та хостові (HIDS). Мережеві IDS моніторять трафік, що проходить через мережу, в той час як хостові IDS зосереджені на подіях, що відбуваються на окремих пристроях. IDS використовують підписні бази та алгоритми виявлення аномалій для ідентифікації потенційних загроз.

Поведінковий аналіз (UBA/UEBA)

Методи аналізу поведінки користувачів та ентитетів (UBA/UEBA) використовують алгоритми машинного навчання для створення базових моделей нормальної поведінки користувачів та пристроїв у мережі. Будь-які відхилення від цих моделей можуть сигналізувати про наявність підозрілої активності, що потребує подальшого розслідування. Аналіз поведінки дозволяє виявляти нові та невідомі загрози, які не можуть бути виявлені за допомогою традиційних методів, що базуються на підписах.

Системи управління подіями безпеки (SIEM)

Системи управління подіями безпеки (SIEM) є ще одним важливим інструментом у боротьбі з APT атаками [9]. SIEM забезпечують централізоване збирання, аналіз та кореляцію подій безпеки з різних джерел у реальному часі. Вони дозволяють виявляти складні атаки, що можуть залишатися непоміченими при використанні окремих інструментів. SIEM використовують правила кореляції,

що базуються на підписах та поведінковому аналізі, для ідентифікації підозрілих активностей та інцидентів безпеки.

Extended Detection and Response (XDR) та Endpoint Detection and Response (EDR)

XDR (Extended Detection and Response) та EDR (Endpoint Detection and Response) є сучасними підходами до виявлення та протидії загрозам. EDR фокусується на виявленні та реагуванні на загрози безпосередньо на кінцевих пристроях, таких як робочі станції та сервери. EDR рішення забезпечують детальний моніторинг активності на кінцевих пристроях, виявлення аномалій, збір даних для розслідування інцидентів та автоматизоване реагування на загрози. XDR розширює ці можливості, інтегруючи дані з різних джерел, включаючи мережеве обладнання, хмарні сервіси та інші системи, для забезпечення комплексного виявлення та реагування на загрози. XDR системи дозволяють отримати більш повну картину про стан безпеки організації, поєднуючи інформацію з різних точок входу та автоматизуючи процеси аналізу та реагування.

Антивірусні програми та системи захисту від шкідливого ПЗ

Антивірусні програми та системи захисту від шкідливого ПЗ є базовими інструментами для виявлення та блокування шкідливих програм, що використовуються у APT атаках. Сучасні антивірусні рішення використовують підписні бази, евристичні методи та аналіз поведінки для виявлення відомих та нових загроз. Вони можуть інтегруватися з іншими засобами безпеки, такими як SIEM та IDS, для забезпечення комплексного захисту.

Усі ці методи та інструменти грають важливу роль у виявленні та протидії APT атакам. Важливою є інтеграція різних засобів захисту в єдину систему, що дозволяє забезпечити багаторівневий підхід до безпеки та своєчасне реагування на загрози.

2.2 Порівняння ефективності та недоліки існуючих підходів

Існує багато рішень для захисту інфраструктури компаній, і часто ці рішення обираються не за параметром чистої ефективності, а за співвідношенням ціни та рівня захисту, що вони можуть надати. Важливо зрозуміти, що якщо система захисту буде дорожчою за ту інформацію, що її захищає, то така система одразу неефективна. Кожна організація при плануванні захисту своєї інформації має оцінити свою інформацію, ризики для неї, та відштовхуючись від цього створити план захисту. Обрати вендорів і конкретні рішення – наступний крок реалізації захисту.

Серед існуючих підходів до захисту можна виділити декілька основних категорій: XDR (Extended Detection and Response), EDR (Endpoint Detection and Response), SIEM (Security Information and Event Management), IDS (Intrusion Detection Systems) та антивірусні програми. Кожен з цих підходів має свої переваги та недоліки.

XDR (Extended Detection and Response) інтегрує дані з різних джерел, що забезпечує комплексне виявлення загроз, автоматизує процеси аналізу та реагування, зменшуючи час реакції на інциденти, та надає повну картину стану безпеки організації. Проте, впровадження та підтримка XDR є дорогою та потребує високої кваліфікації персоналу.

EDR (Endpoint Detection and Response) фокусується на виявленні та реагуванні на загрози безпосередньо на кінцевих пристроях, забезпечує детальний моніторинг активності, збір даних для розслідування інцидентів та автоматизоване реагування. Однак, EDR має обмежену здатність до виявлення мережевих загроз і може вимагати значних ресурсів для аналізу великої кількості даних.

SIEM (Security Information and Event Management) централізовано збирає, аналізує та корелює події безпеки з різних джерел, дозволяє виявляти складні атаки, що можуть залишатися непоміченими при використанні окремих інструментів, і використовує правила кореляції для ідентифікації підозрілих активностей.

Впровадження та обслуговування SIEM також є дорогими, і воно потребує значних ресурсів для аналізу та зберігання великих обсягів даних.

IDS (Intrusion Detection Systems) моніторить мережевий трафік та аналізує події у реальному часі, виявляючи підозрілу активність за допомогою підписних баз та алгоритмів виявлення аномалій. Проте, IDS має обмежену здатність до виявлення нових та невідомих загроз і може генерувати велику кількість хибнопозитивних спрацьовувань.

Антивірусні програми забезпечують базовий захист від відомих шкідливих програм, використовуючи підписні бази, евристичні методи та аналіз поведінки. Вони мають обмежену здатність до виявлення нових та складних загроз і не забезпечують комплексного захисту без інтеграції з іншими системами безпеки.

Кожна технологія захисту направлена на захист певних частин інфраструктури організації або на підсилення захисту вже захищених кінцевих точок. Тому порівнювати ці технології немає змісту, кожна з них доповнює захист. Нижче розглянемо кожну технологію та продукти, які реалізовують захист з використанням цих технологій, детальніше:

Системи виявлення та запобігання вторгнень (IDS/IPS):

Snort: Відкрите джерело IDS/IPS, що дозволяє виявляти вторгнення в мережу в реальному часі. Snort аналізує мережевий трафік і порівнює його з базою підписів, щоб виявляти аномалії та шкідливі дії.

Suricata: Потужна система IDS/IPS з відкритим кодом, яка підтримує високу продуктивність та інтеграцію з іншими інструментами безпеки. Suricata забезпечує детальний аналіз трафіку, включаючи підтримку різних мережевих протоколів та виявлення шкідливих дій.

Системи управління подіями безпеки (SIEM):

Splunk: Відоме рішення для аналізу великих обсягів даних та управління подіями безпеки. Splunk дозволяє централізовано збирати, аналізувати та корелювати події безпеки з різних джерел у реальному часі, забезпечуючи глибоке розуміння ситуації в організації.

IBM QRadar: Потужна платформа SIEM, яка забезпечує інтегроване управління подіями безпеки та аналіз загроз. QRadar дозволяє виявляти складні атаки, аналізуючи події з різних джерел та застосовуючи правила кореляції для ідентифікації підозрілих дій.

Аналіз поведінки користувачів та ентитетів (UBA/UEBA):

Exabeam: Платформа для аналізу поведінки користувачів та ентитетів, яка використовує алгоритми машинного навчання для створення моделей нормальної поведінки. Відхилення від цих моделей можуть сигналізувати про підозрілу активність, що потребує подальшого розслідування.

Splunk UBA: Модуль для аналізу поведінки користувачів, який інтегрується зі Splunk SIEM. Splunk UBA використовує машинне навчання для виявлення аномалій та нових загроз, що не можуть бути виявлені традиційними методами.

Рішення для захисту кінцевих точок (EDR) та системи розширеного виявлення та реагування (XDR):

Trend Micro XDR: Інтегрована платформа XDR, яка забезпечує комплексне виявлення та реагування на загрози, поєднуючи дані з кінцевих точок, мережевого обладнання, хмарних сервісів та інших систем. Trend Micro XDR дозволяє отримати більш повну картину про стан безпеки організації та автоматизувати процеси аналізу та реагування.

ESET Inspect (XDR): Рішення, яке забезпечує глибокий аналіз трафіку на кінцевих точках. ESET Inspect може виявляти аномалії та підозрілу активність, а при достатньо навчених спеціалістах, використання UBA/UEBA технологій може бути менш необхідним, оскільки фахівці можуть створити виключення та правила під патерни активності кінцевих точок.

Антивірусні програми та системи захисту від шкідливого ПЗ:

ESET Endpoint Security: Відоме своєю високою ефективністю у виявленні та блокуванні шкідливого програмного забезпечення. Використовує підписні бази, евристичні методи та аналіз поведінки для виявлення відомих та нових загроз.

Symantec Endpoint Protection: Забезпечує багаторівневий захист кінцевих точок від шкідливого ПЗ. Використовує підписні бази, аналіз поведінки та додаткові методи для виявлення та блокування загроз.

Кожна з цих технологій відіграє свою роль у комплексному захисті організації від кіберзагроз. Інтеграція цих інструментів у єдину систему дозволяє створити багаторівневий захист, що покращує виявлення загроз, скорочує час на реагування та мінімізує ризик поширення атак. Таким чином, використання різних технологій не є взаємозамінним, а навпаки – вони доповнюють одна одну, забезпечуючи більш надійний та всебічний захист інфраструктури організації.

Оскільки система XDR забезпечує більшість необхідних функцій захисту, розглядатимемо саме її. Зокрема, ESET Inspect (XDR) може аналізувати трафік на кінцевих точках. При достатньо навчених спеціалістах, використання UBA/UEBA технологій може бути менш необхідним, оскільки фахівці знають патерни активності кінцевих точок. SIEM можна замінити завдяки веб-консолям у ESET Inspect та ESET Protect, які централізують інформацію та забезпечують необхідний рівень аналізу і моніторингу.

Таким чином, вибір ESET Inspect є логічним, оскільки система XDR забезпечує більшість функцій захисту за більш доступною ціною та з меншими вимогами до чисельності та кваліфікації персоналу. Хоча з боку чистої ефективності може бути доцільно поєднувати декілька рішень, організації не завжди мають змогу це робити. У рамках пришвидшення реагування на APT загрози XDR цілком достатньо. Доцільно також використовувати разом з ESET Inspect продукт для безпеки кінцевих точок ESET Endpoint Security, що забезпечить комплексний та ефективний захист організації від сучасних кіберзагроз.

2.3 Виявлення ключових проблем та затримок у реагуванні на APT атаки

APT атаки (Advanced Persistent Threats) характеризуються високим рівнем складності, цілеспрямованістю та тривалістю, що робить їх важким для виявлення

та нейтралізації. Виявлення ключових проблем та затримок у реагуванні на такі атаки є критичним для розробки ефективних стратегій кіберзахисту. Нижче розглянемо основні проблеми та затримки, з якими стикаються організації у процесі реагування на APT атаки.

Недостатня видимість та моніторинг

Однією з основних проблем є недостатня видимість та моніторинг активності в мережі та на кінцевих точках. Багато організацій не мають інтегрованих систем, які дозволяють централізовано моніторити та аналізувати події безпеки у реальному часі. Відсутність ефективних інструментів для збору та кореляції даних призводить до того, що підозріла активність може залишатися непоміченою тривалий час.

Відсутність інтеграції інструментів безпеки

Інша проблема полягає у фрагментованості інструментів безпеки. Різні системи для виявлення вторгнень (IDS/IPS), управління подіями безпеки (SIEM), аналізу поведінки користувачів (UBA/UEBA) та захисту кінцевих точок (EDR/XDR) часто не інтегровані між собою. Це ускладнює централізоване управління безпекою та координацію дій під час реагування на інциденти.

Нестача кваліфікованих фахівців

Залучення та утримання висококваліфікованих фахівців з кібербезпеки є серйозною проблемою для багатьох організацій. Відсутність достатньої кількості експертів, здатних ефективно аналізувати дані, виявляти загрози та реагувати на інциденти, значно уповільнює процес виявлення та нейтралізації APT атак. Багато організацій не мають можливості забезпечити цілодобове моніторинг та оперативне реагування на інциденти.

Складність та тривалість атак

APT атаки можуть тривати місяці або навіть роки, залишаючись непоміченими. Зловмисники використовують різноманітні методи, включаючи соціальну інженерію, фішинг, експлуатацію вразливостей нульового дня та атаки на ланцюжок постачання. Складність та тривалість таких атак робить їх важкими для виявлення за допомогою традиційних методів захисту.

Недостатня автоматизація процесів

Відсутність автоматизації процесів виявлення та реагування на інциденти також є суттєвою проблемою [10]. Ручне виконання багатьох завдань затримує реагування та підвищує ризик помилок. Автоматизовані рішення, такі як системи розширеного виявлення та реагування (XDR), можуть значно покращити швидкість та ефективність реагування на інциденти.

Недостатня підготовка до інцидентів

Багато організацій не мають чітко визначених планів реагування на інциденти. Відсутність документованих процедур та регулярних тренувань може призвести до затримок у реагуванні та погіршення координації дій під час атаки. Регулярне тестування планів реагування та проведення симуляцій інцидентів є необхідними для підвищення готовності організації до кіберзагроз.

Рекомендації для покращення реагування на APT атаки

Для подолання зазначених проблем та затримок, організаціям необхідно впроваджувати комплексні заходи, що включають як технологічні, так і організаційні аспекти. Нижче наведено кілька ключових рекомендацій:

Інтеграція систем безпеки: Використання інтегрованих рішень, таких як XDR, які поєднують дані з різних джерел та забезпечують централізоване управління безпекою.

Підвищення кваліфікації персоналу: Регулярне навчання та підвищення кваліфікації фахівців з кібербезпеки, проведення симуляцій інцидентів та тестування планів реагування.

Автоматизація процесів: Впровадження автоматизованих рішень для виявлення та реагування на інциденти, що дозволяє скоротити час на виявлення та нейтралізацію загроз [11].

Покращення видимості: Використання сучасних інструментів для моніторингу та аналізу подій у реальному часі, що забезпечує підвищену видимість та контроль над IT-інфраструктурою.

Розробка чітких планів реагування: Створення та регулярне оновлення документованих процедур реагування на інциденти, проведення регулярних тренувань та тестування планів.

Впровадження цих заходів дозволить організаціям значно покращити свою здатність виявляти та реагувати на APT атаки, забезпечуючи надійний захист від сучасних кіберзагроз.

Висновки другого розділу

Для виявлення і протидії APT атакам використовуються різні методи та інструменти, зокрема системи виявлення вторгнень (IDS/IPS), системи управління подіями безпеки (SIEM), аналіз поведінки користувачів (UBA/UEBA), рішення для захисту кінцевих точок (EDR) та системи розширеного виявлення та реагування (XDR). Використання цих інструментів дозволяє покращити виявлення загроз і знизити час реагування на інциденти. Важливо також мати висококваліфікованих фахівців, постійно навчати персонал та інтегрувати різні засоби безпеки для забезпечення багаторівневого захисту.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗМЕНШЕННЯ ЧАСУ РЕАГУВАННЯ НА APT АТАКИ НА РОБОЧИХ САНЦІЯХ

3.1 Роль ESET Protect та Inspect у боротьбі з APT атаками та його функціональні можливості

ESET Protect та ESET Inspect є ключовими компонентами комплексного підходу до кібербезпеки в організації, забезпечуючи багаторівневий захист від передових персистентних загроз (APT). Ці інструменти пропонують централізоване управління безпекою та автоматизоване реагування на загрози, що значно підвищує ефективність захисту організацій. Розглянемо детальніше основні функціональні можливості кожного з інструментів.

Централізоване управління безпекою

ESET Protect та ESET Inspect являють собою веб-консолі, які забезпечують централізований контроль політик безпеки для захисту кінцевих точок. Вони дозволяють адмініструвати та моніторити інформацію, отриману з кінцевих точок, з єдиного інтерфейсу. Це спрощує управління безпекою та забезпечує більш ефективний моніторинг. Основні функції включають:

- **Моніторинг стану безпеки**: Адміністратори можуть отримувати інформацію про стан захисту кожного пристрою, включаючи встановлені оновлення та патчі.
- **Політики безпеки**: Можливість налаштування та застосування політик безпеки для різних груп користувачів та пристроїв, що забезпечує дотримання стандартів безпеки в організації.

Автоматичне реагування на загрози

ESET Protect та ESET Inspect дозволяють створювати правила автоматичного реагування на різні типи подій [12]. Це можуть бути як статично задані події, наприклад, виявлення певних сигнатур зловмисного програмного забезпечення або індикаторів компрометації (IOC), так і динамічно задані параметри, такі як нові, раніше не зустрічені загрози або критичні загрози. Завдяки цьому можна досягти

високого рівня автоматизації у реагуванні на загрози, що значно прискорює процес реагування та мінімізує ризики.

Виявлення загроз у реальному часі

ESET Protect та ESET Inspect використовують сучасні технології машинного навчання та аналізу поведінки для виявлення загроз у реальному часі:

- **Машинне навчання**: Аналіз великих обсягів даних для виявлення аномалій, які можуть вказувати на наявність шкідливого програмного забезпечення або несанкціонованої активності.
- **Поведінковий аналіз**: Моніторинг дій користувачів та систем для визначення відхилень від нормальної поведінки. Це дозволяє виявляти нові, невідомі загрози, які ще не мають підписів у базах даних.

Система сповіщень користувача

ESET Protect та ESET Inspect включають вбудовану систему сповіщень, яка інформує користувачів про виконання певних подій. Сповіщення можуть доставлятися різними методами, включаючи email-листи або HTTP POST-запити. Це дозволяє налаштовувати інформування у відповідності до потреб організації та забезпечувати оперативне реагування на інциденти.

Роль серверів керування та кінцевих точок

Сервери керування ESET є мозковим центром системи, тоді як веб-консолі виступають інтерфейсом для управління та відображення інформації. Кінцеві точки виконують функцію захисту, дотримуючись налаштованих політик безпеки. Це забезпечує надійний захист усіх компонентів інформаційної системи організації.

Розширене виявлення та реагування (EDR)

ESET Inspect надає розширені можливості для виявлення та реагування на загрози:

- **Аналіз інцидентів**: Детальний розгляд кожного інциденту, включаючи збирання доказів та зворотній аналіз для визначення першопричини атаки.

- **Автоматизоване реагування**: Система може автоматично виконувати дії для нейтралізації загроз, такі як ізоляція заражених пристроїв або видалення шкідливого програмного забезпечення.

Інтеграція з іншими системами безпеки

ESET Protect та ESET Inspect можуть інтегруватися з іншими системами безпеки, такими як системи управління подіями безпеки (SIEM) та системи виявлення вторгнень (IDS). Це дозволяє створити комплексну екосистему захисту, об'єднуючи різні рівні безпеки в єдину систему, що підвищує ефективність виявлення та реагування на загрози.

Моніторинг мережевої активності

ESET Inspect дозволяє відстежувати мережеву активність для виявлення підозрілих взаємодій між пристроями:

- **Аналіз трафіку**: Виявлення аномалій у мережевому трафіку, які можуть свідчити про наявність загрози.
- **Несанкціоновані підключення**: Виявлення та блокування підозрілих підключень до мережі.

Аналіз поведінки та машинне навчання

ESET Protect та ESET Inspect використовують методи аналізу поведінки та машинного навчання для адаптації до нових загроз:

- **Моделі поведінки**: Створення базових моделей нормальної поведінки користувачів та пристроїв у мережі. Відхилення від цих моделей можуть вказувати на наявність загрози.
- **Режим навчання**: Можливість увімкнути режим навчання на запланований час для автоматичного створення виключень з блокування, для спрощення подальшого налаштування та інтеграції у інфраструктуру.

Автоматизоване реагування на інциденти

ESET Inspect забезпечує можливості для автоматизованого реагування на інциденти:

- **Ізоляція заражених пристроїв**: Автоматичне відключення заражених пристроїв від мережі для запобігання подальшому поширенню загрози.

- **Видалення шкідливого ПЗ**: Автоматизовані дії для видалення шкідливого програмного забезпечення з кінцевих пристроїв.

Поглиблений аналіз загроз

ESET Protect та ESET Inspect надають інструменти для детального аналізу виявлених загроз:

- **Зворотній аналіз шкідливого ПЗ**: Вивчення шкідливого коду для розуміння його механізмів дії та вразливих місць.
- **Звітність**: Генерація детальних звітів про виявлені загрози та виконані дії для подальшого аналізу та вдосконалення заходів безпеки.

Одним із яскравих прикладів ефективного реагування на APT-атаку є нейтралізація загрози Industroyer2 [13], що була використана під час атаки на енергетичний сектор України навесні 2022 року. Завдяки тісній співпраці дослідників ESET та CERT-UA вдалося оперативно виявити та знешкодити шкідливе програмне забезпечення, яке могло б спричинити масштабну кібератаку. Цей випадок демонструє важливість швидкого та ефективного реагування на загрози для захисту критичної інфраструктури.

Детальний аналіз загрози та оперативне реагування дозволили не тільки запобігти масштабній атаці, але й надати цінну інформацію для підвищення рівня кіберзахисту в майбутньому. Співпраця між ESET та CERT-UA продовжується для забезпечення надійного захисту від сучасних кіберзагроз.

3.2 Налаштування та тестування ESET Protect та Inspect щодо реагування на APT атаки

Ефективне налаштування та тестування систем ESET Protect та ESET Inspect є ключовим аспектом забезпечення своєчасного реагування на APT атаки. Ці інструменти дозволяють забезпечити комплексний захист робочих станцій, надаючи можливість виявляти та нейтралізувати загрози на ранніх етапах. Відповідне налаштування політик безпеки, моніторинг у реальному часі та регулярне тестування систем є необхідними умовами для підвищення ефективності

кіберзахисту організацій.

Для забезпечення максимального захисту периметру організації рекомендується встановлювати продукти безпеки на всі кінцеві точки в організації. Це зумовлено тим, що кінцеві точки, на яких не встановлено продукт захисту, можуть стати "точками входу" під час кібератак.

Актуальність операційних систем та програмного забезпечення

Одним з ключових аспектів забезпечення безпеки є підтримання актуальності операційних систем, драйверів, програмного забезпечення та операційних систем апаратного обладнання. Вчасне оновлення програмного забезпечення може запобігти багатьом атакам, оскільки закриває відомі вразливості. Варто зазначити, що жоден продукт безпеки не може закрити вразливість в операційній системі краще, ніж вендор цієї операційної системи. Тому важливо забезпечити своєчасне застосування оновлень і патчів від розробників операційних систем та іншого програмного забезпечення.

Актуальність продукту захисту

Крім оновлення стороннього програмного забезпечення, важливо також підтримувати продукт захисту в найновішому стані. Для забезпечення максимальної ефективності, продукт захисту повинен мати можливість тримати вірусні бази в максимально актуальному стані, з оновленнями, які можуть проходити близько 24 разів на добу. Найновіші версії продукту захисту зазвичай отримують нові функції захисту, що підсилює захист організації.

Правильні налаштування політик безпеки

Після розгортання продукту захисту в інфраструктурі організації наступним кроком є правильне налаштування політик безпеки. Вендори продуктів безпеки зазвичай надають так звані Best Practices для налаштувань. Для ESET Protect це включає:

- **Налаштування політик безпеки**: Визначення та застосування політик безпеки для різних груп користувачів і пристроїв, обмеження доступу до критичних ресурсів, запобігання виконанню неперевірених програм.
- **Аналіз поведінки та машинне навчання**: Активація функцій аналізу

поведінки для відстеження аномалій у діях користувачів та систем, автоматичне оновлення моделей машинного навчання.

● **Система сповіщень**: Конфігурація системи сповіщень для оперативного інформування про виявлені загрози та інциденти, вибір методів доставки сповіщень, таких як email-листи, веб-хуки або HTTP POST-запити.

Рекомендації щодо налаштування та тестування продукту безпеки перед розгортанням

Перед розгортанням продукту безпеки ESET Endpoint Security, рекомендується перевести його в режим аудиту. Це необхідно для того, щоб продукт безпеки не перервав бізнес-процеси організації. Жоден продукт безпеки не застрахований від помилкових спрацьовувань (False Positive), і тільки додатковий ручний контроль може повністю запобігти цьому явищу. Налаштування ядра захисту продукту в режимі аудиту виглядатиме наступним чином:

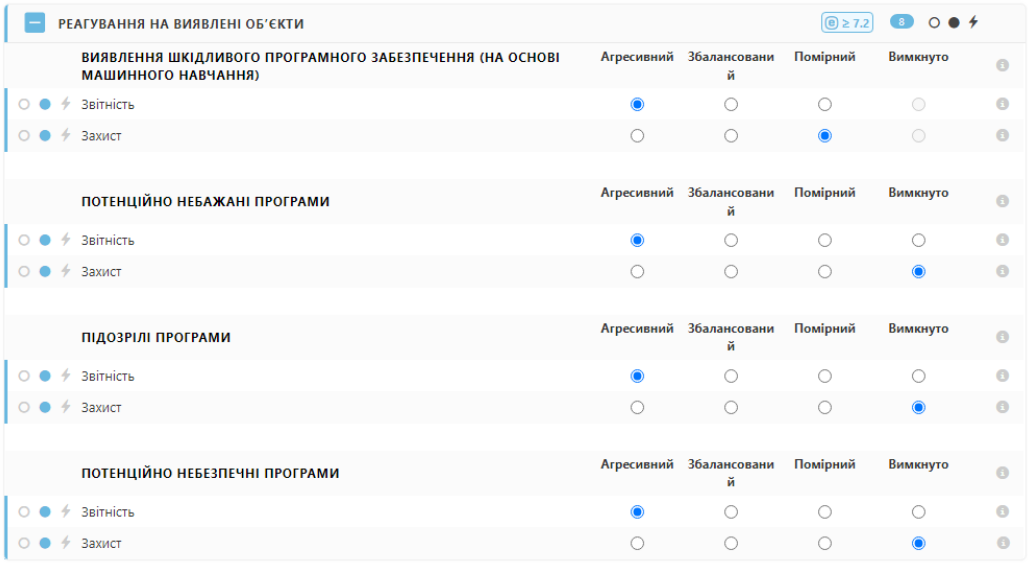

Рис. 3.1. Налаштування ядра виявлення у режим аудиту

На Рис. 3.1. продемонстрована таблиця, що визначає кожен модуль у двух режимах, Звітність та Захист.

Режим звітності: Всі модулі виявлення в агресивному режим по звітності. Це дозволяє спеціалісту з кібербезпеки отримувати докладні звіти про всі потенційні загрози, які були знайдені під час сканування кінцевих точок.

Режим захисту: Вимкнуті або майже вимкнуті захистні функції модулів. Це

дозволяє уникнути переривання бізнес-процесів, одночасно надаючи інформацію про можливі загрози.

Таке налаштування продукту безпеки дасть спеціалісту з кібербезпеки можливість "побачити" всі можливі загрози, які були знайдені під час сканування кінцевих точок, звіритись з переліком критичного для організації програмного забезпечення та додати його у виключення зі сканування або виконання, в залежності від потреб.

Після опрацювання всіх важливих файлів рекомендується поступово підвищувати рівень Захисту для увімкнення модулів в їх робочий стан.

Налаштування брандмауера

Брандмауер підтримує режим навчання, який рекомендується ввімкнути на період до двох тижнів. Це дозволить створити список правил фільтрації трафіку за портами, протоколами та напрямками на кінцевих точках. Приклад налаштування режиму навчання:

Режим навчання: Увімкнений режим навчання на брандмауері, щоб він автоматично створював правила на основі реального трафіку, що проходить через мережу.

Аналіз трафіку: Протягом двох тижнів спостерігайте за згенерованими правилами, коригуйте їх відповідно до політик безпеки організації.

Приклад таких налаштувань:

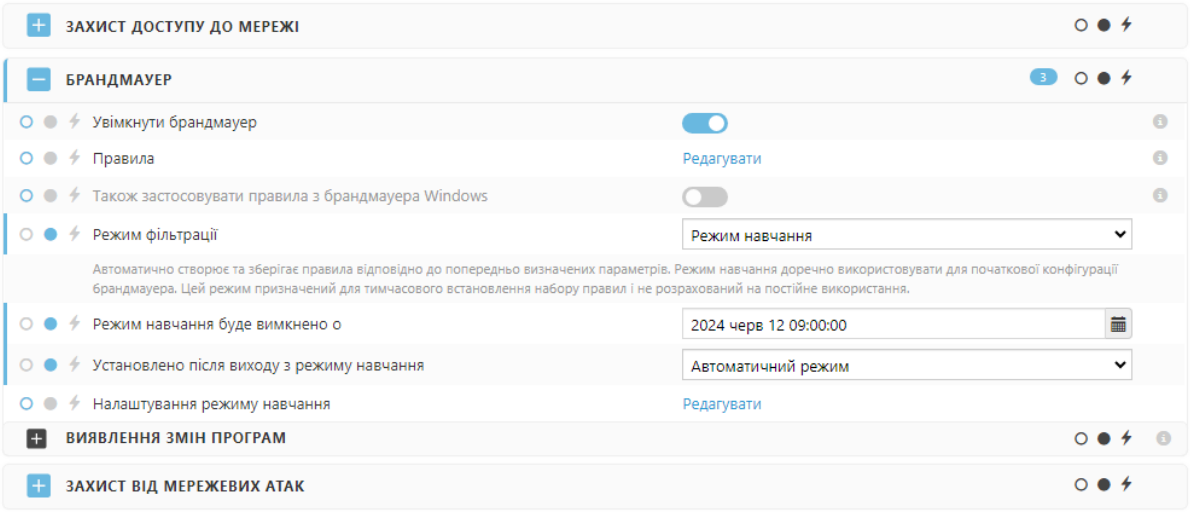

Рис. 3.2. Налаштування Брандмауера у режим навчання

Цей режим спростить інтеграцію продукту безпеки у організацію, виконуючи частину роботи спеціалістів автоматично. Також він допоможе працівникам зрозуміти, як правиль створювати правила блокування чи дозволу трафіку, що теж впливає на загальну підготовку персоналу.

Після завершення режиму аудиту та періоду навчання брандмауера:

Аналіз результатів: Потрібно проаналізувати результати аудиту та навчання.

Коригування налаштувань: Після завершення режиму навчання скоріше за все потрібно буде провести корекцію правил, що були автоматично створені на основі підключень що відбувались на кінцевих точка. Також потрібно буде видалити зайві правила, що насправді суперечать політиці безпеки компанії та проаналізувати, яке програмне забезпечення викликало ці підключення.

Перехід до повного захисту: Після перевірки та налаштування всіх компонентів продукту безпеки переведіть його з режиму аудиту в режим повного захисту.

Одним із варіантів налаштування ядра виявлення після завершення режиму аудиту можуть бути такі налаштування:

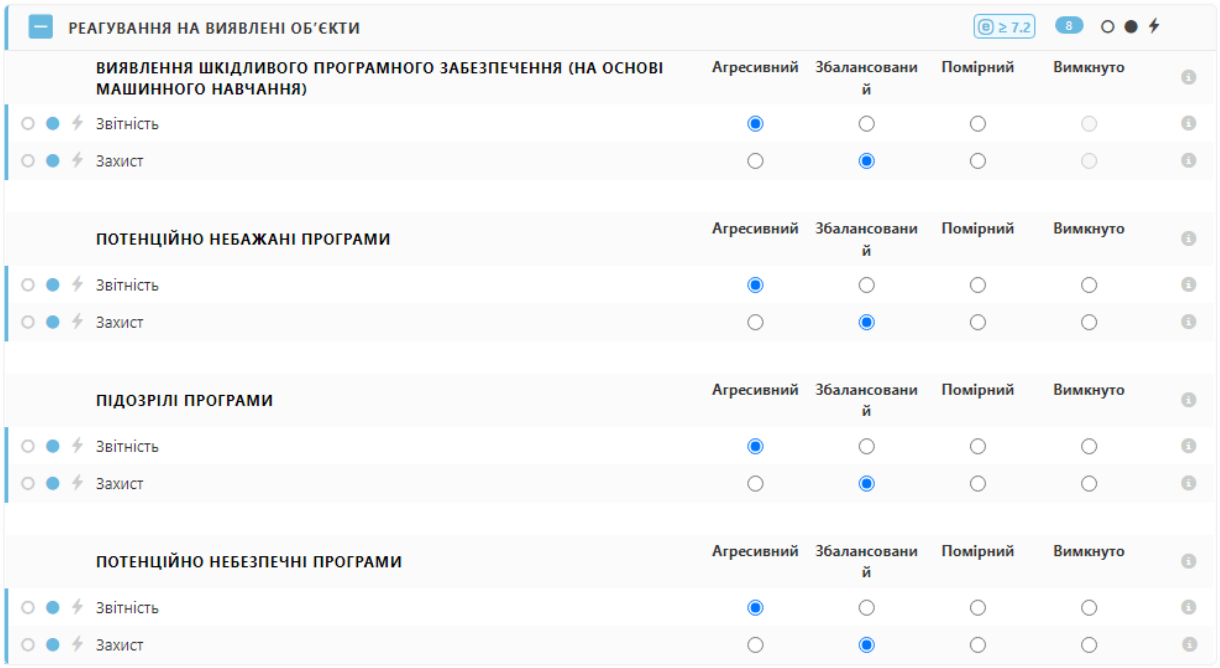

Рис. 3.3. Приклад налаштування ядра виявлення у режим захисту

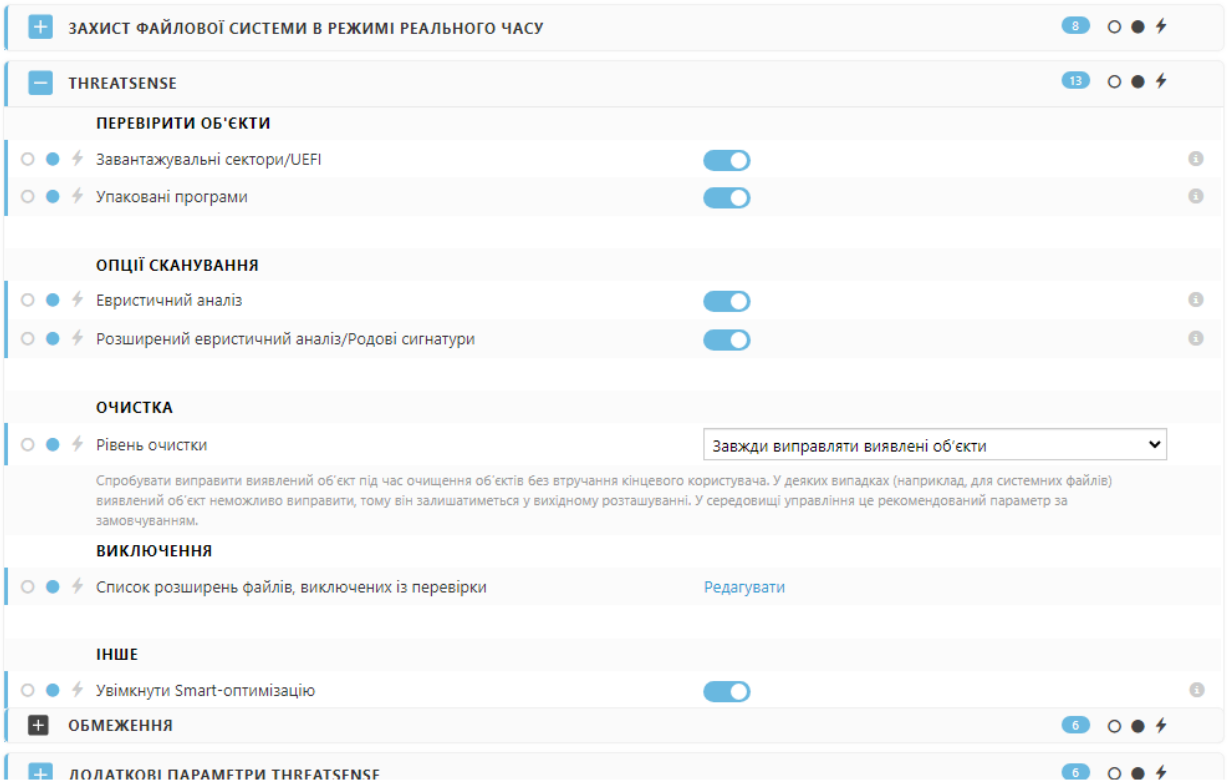

Рис. 3.4. Приклад налаштування параметрів сканування у режим захисту

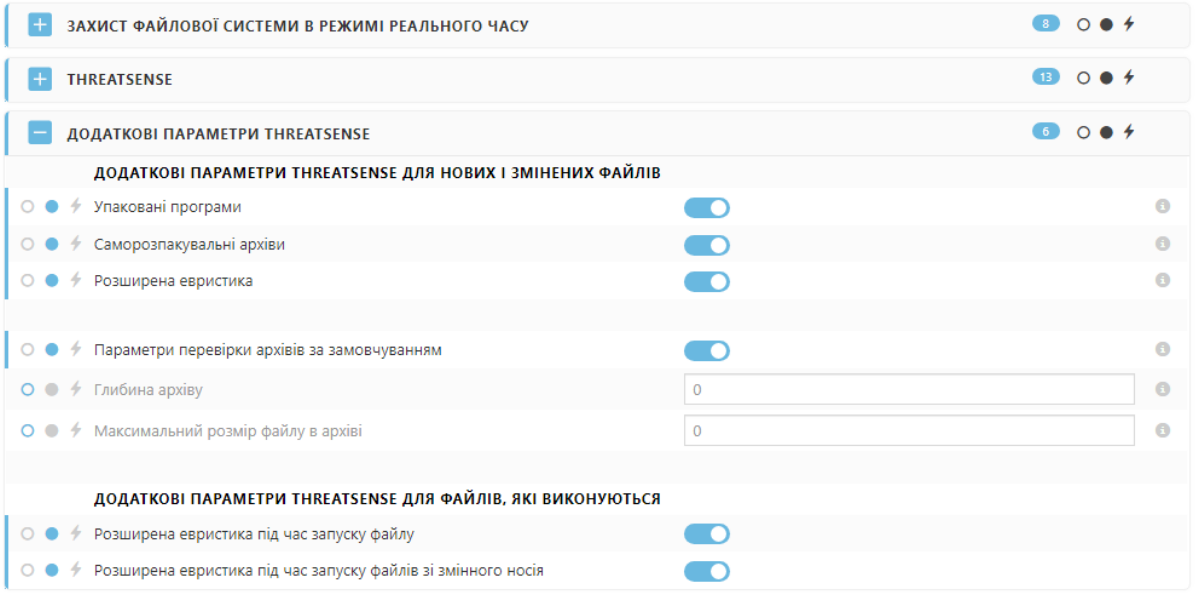

Рис. 3.4. Приклад налаштування параметрів сканування у режим захисту

Цей приклад налаштування ядра виявлення є одним із оптимальних, проте слід враховувати, що налаштування можуть варіюватися залежно від конкретних умов середовища та вимог власника. Кожна організація має свої унікальні потреби

та ризики, тому важливо адаптувати налаштування продукту безпеки відповідно до цих факторів.

Рекомендації з налаштування ядра виявлення

Індивідуальний підхід: Враховуйте специфічні особливості вашої організації, такі як структура мережі, типи використовуваних програм та рівень ризику.

Консультація з експертами: Залучайте експертів з кібербезпеки для оцінки ваших потреб та налаштування продукту безпеки відповідно до найкращих практик. Часто з цим можуть допомогти вендори програмного забезпечення.

Тестування та валідація: Проводьте регулярне тестування налаштувань, щоб переконатися, що вони ефективно захищають ваші системи без негативного впливу на бізнес-процеси. Тестування краще проводити на цільовій групі кінцевих точок, з можливістю відкату нових налаштувань, для того щоб мінімізувати вплив неправильних налаштувань.

Налаштування ESET Inspect після налаштування продукту захисту

Після коректного налаштування продукту захисту можна перейти до налаштування XDR – ESET Inspect. Ця система складається з керуючого сервера, що є ядром системи, бази даних для зберігання даних та веб-консолі, яка відповідає за відображення та можливість керування сервером. Щоб почати отримувати інформацію про події з кінцевих точок, на них потрібно розгорнути ESET Inspect Connector, який відповідає за відправку даних з кінцевих точок та виконання блокуючих дій згідно з налаштованими правилами.

Важливість інтеграції та налаштування ESET Inspect

Інтеграція та коректне налаштування ESET Inspect мають ключове значення для стримування та реакції на APT атаки. Ця система звертає увагу користувача на всі підозрілі події на кінцевих точках, допомагаючи виявити та запобігти проникненню на ранній стадії, щоб мінімізувати шкоду, яку може нанести загроза інформації. Присутні також блокуючі правила, наприклад honeypod для шифрувальників, що може зупинити атаку на її початку. Завдяки цим функціям, ESET Inspect дозволяє швидко реагувати на загрози, забезпечуючи високий рівень захисту організаційних ресурсів.

Прискорення реагування на загрози

Прискорене реагування на загрози потребує виділення з величезного обсягу інформаційних подій в інформаційній системі організації ті події, що можуть свідчити про спробу або реалізацію проникнення всередину периметру захисту. Окремо кожна така подія може бути легітимною і не підозрілою, але їх комбінація у певному порядку може свідчити про підозрілі дії на кінцевій точці, що вимагатиме більш детального розслідування.

Режим навчання для інтеграції ESET Inspect

Для прискорення інтеграції ESET Inspect у системи безпеки організації можна застосувати режим навчання. Це допоможе виключити з загального “білого шуму” подій в інформаційному середовищі повторювані легітимні дії від специфічних дій користувачів чи їх програмного забезпечення, що затверджене політиками безпеки. Автоматично створені виключення значно прискорять цей процес, хоча й не зможуть виключити всі повторювані легітимні події. Вони також потребуватимуть подальшої перевірки після додання, щоб виключити False Negative або зробити їх більш точковими, запобігаючи можливій навмисній або випадковій експлуатації.

Правильне налаштування ESET Inspect після налаштування продукту захисту є важливим етапом у забезпеченні комплексної кібербезпеки. Інтеграція ESET Inspect дозволяє своєчасно виявляти та реагувати на підозрілі події, що допомагає запобігти проникненню загроз всередину периметру захисту та мінімізувати потенційні ризики для інформаційних систем організації. Використання режиму навчання та регулярна перевірка налаштувань сприятимуть ефективному функціонуванню системи безпеки.

3.3 Рекомендації щодо зменшення часу реагування на APT атаки на робочих станціях на основі ESET Protect та Inspect

Гарантованого захисту від APT атак (Advanced Persistent Threats) не існує через їх складність і використання вразливостей нульового дня. APT атаки

представляють собою тривалі та цілеспрямовані кібернапади, що можуть залишатися непоміченими протягом тривалого часу, оскільки зловмисники часто використовують новітні та раніше невідомі методи атак. Спеціалісти з кібербезпеки можуть реагувати на такі атаки лише постфактум, коли вони вже готуються або реалізовуються. Це робить пришвидшення реагування на такі атаки одним із головних способів боротьби з ними та пом'якшення їх негативного впливу.

APT атаки можуть призводити до значних збитків, тому важливо не тільки виявляти і нейтралізувати загрози, але й мінімізувати їх вплив. Наприклад, своєчасне бекапування, включаючи використання "холодних носіїв", може значно знизити ризики втрати даних та допомогти відновити системи після атаки.

Важливість пришвидшення реагування на APT атаки

Пришвидшення реагування на APT атаки є критично важливим з кількох причин. По-перше, своєчасна реакція дозволяє мінімізувати шкоду від атак. APT атаки можуть бути тривалими та цілеспрямованими, що дає зловмисникам можливість завдати значної шкоди, якщо атака залишається непоміченою або на неї реагують занадто пізно. Оперативне виявлення та нейтралізація загроз може запобігти втраті конфіденційних даних, фінансових втрат та порушенню нормальної роботи систем.

По-друге, пришвидшення реагування забезпечує безперервність бізнес-процесів. У сучасних умовах більшість організацій сильно залежать від своїх IT-систем. Будь-яке втручання, спричинене кібернападом, може призвести до серйозних збоїв у роботі, що, в свою чергу, негативно впливає на продуктивність і репутацію компанії. Швидке реагування допомагає уникнути простоїв, забезпечуючи безперервну роботу бізнесу.

Крім того, миттєва реакція від відділу кіберзахисту дозволяє суттєво знизити вплив атак та захистити критичну інфраструктуру. Критична інфраструктура, така як енергетичні мережі, фінансові системи та урядові установи, є основною ціллю для APT атак через їх стратегічну важливість. Пошкодження таких систем може мати далекосяжні наслідки не тільки для окремої організації, але й для економіки та національної безпеки в цілому. Швидке реагування допомагає забезпечити

стабільність та захист найважливіших ресурсів.

Швидка реакція також є необхідною для збереження довіри клієнтів і партнерів. У разі інциденту, оперативне реагування демонструє здатність організації ефективно управляти кризовими ситуаціями та захищати дані своїх клієнтів. Це підвищує довіру до компанії та зменшує негативні наслідки для її репутації.

Нарешті, пришвидшення реагування на APT атаки сприяє покращенню загальної кібербезпеки організації. Постійне вдосконалення механізмів виявлення та реагування дозволяє виявляти та нейтралізувати нові типи загроз, підвищуючи рівень захищеності інформаційних систем. Це допомагає організації бути більш стійкою до майбутніх атак, забезпечуючи довгостроковий захист від кіберзагроз.

Рекомендації для пришвидшення реагування на APT атаки

Для пришвидшення реагування на APT атаки рекомендується виконувати цілий комплекс дій:

Моніторинг та оновлення індикаторів компрометації (IOC): Слідкування за новими індикаторами компрометації (IOC) на сайті CERT-UA є важливою складовою захисту. IOC включають в себе різні маркери, такі як хеші файлів, IP-адреси, домени та URL-адреси, які вказують на потенційно зловмисну активність. Оперативне оновлення правил захисту дозволяє уникнути багатьох атак, додаючи блокування за хешами вже використаних файлів або URL-адрес одноразових вебсервісів, чи попередження про підключення до легітимних.

Автоматизація сповіщень: Автоматизація процесів сповіщення є ключовим елементом пришвидшення реагування на загрози. Додавання автоматизованих попереджень на email-адреси для спрацювань за індикаторами компрометації дозволяє відповідальним особам отримувати своєчасні сповіщення та оперативно реагувати на виявлені загрози. Це значно знижує час реагування та підвищує ефективність захисту.

HTTP POST запити для складних алгоритмів реакції: Для створення більш складних алгоритмів реакції на спрацювання можна використовувати HTTP POST запити на вказаний сервер. Це дозволяє автоматизувати процеси обробки

сповіщень і зменшити час реакції на інциденти. Використання HTTP POST запитів для надсилання інформації про спрацювання на вказаний сервер допомагає створювати складні алгоритми реакції, що дозволяє автоматизувати процеси обробки сповіщень і зменшити час реакції на інциденти.

Додавання виключень на перевірені виявлення: Додавання виключень на вже перевірені виявлення на кінцевих точках також внесе свій вклад у пришвидшення реагування на нові загрози. Створення унікальних виключень для груп кінцевих точок зменшує кількість хибнопозитивних спрацювань, що пришвидшує їх аналіз. Це допомагає сфокусуватися на реальних загрозах, мінімізуючи витрати часу та ресурсів на обробку непотрібних сповіщень.

Аналіз аномальної активності: Атаки часто супроводжуються збільшенням виявлень на кінцевих точках. Отримання цього показника у реальному часі, наприклад за допомогою звітів, що генеруються кожну хвилину, та порівняння з середньодобовим за минулий тиждень, може вказувати на аномальну активність. Збільшення може свідчити про необхідність підсилення уваги до цієї кінцевої точки. Такі звіти можна створювати та отримувати за допомогою API команд до керуючого серверу, отримуючи результат у вигляді CSV таблиці. Це забезпечує швидке та зручне отримання даних для аналізу і прийняття відповідних заходів.

Запровадження цих методів та рекомендацій дозволить значно покращити швидкість реагування на APT атаки та підвищити рівень захисту організації від сучасних кіберзагроз. Інтеграція автоматизованих процесів, використання сучасних інструментів моніторингу та аналізу, а також регулярне оновлення систем безпеки сприятимуть ефективному захисту від потенційних загроз. Це не тільки підвищить ефективність захисту, але й знизить ризики втрат від атак, забезпечуючи безперервність бізнес-процесів та збереження довіри клієнтів та партнерів.

Висновки до третього розділу

ESET Protect та ESET Inspect є ключовими компонентами комплексного підходу до кібербезпеки в організаціях, забезпечуючи багаторівневий захист від передових персистентних загроз (APT). Ці інструменти дозволяють централізовано управляти безпекою, автоматизувати реагування на загрози та здійснювати

моніторинг у реальному часі. Вони використовують сучасні технології машинного навчання та поведінкового аналізу для виявлення аномалій, що допомагає швидше ідентифікувати та нейтралізувати потенційні загрози. Централізоване управління політиками безпеки спрощує моніторинг і підвищує ефективність захисту.

Для зменшення часу реагування на APT атаки рекомендується інтегрувати різні системи безпеки, забезпечити регулярне навчання персоналу та впровадити автоматизовані рішення для виявлення і реагування на інциденти. Важливо також покращити видимість та контроль над IT-інфраструктурою шляхом використання сучасних інструментів для моніторингу подій у реальному часі. Розробка чітких планів реагування, їх регулярне оновлення та проведення тренувань і симуляцій інцидентів підвищують готовність організацій до кіберзагроз та забезпечують надійний захист інформаційного середовища.

ВИСНОВКИ

Проведено аналіз сучасних методів зменшення часу реагування на APT атаки на робочих станціях на основі ESET Protect та Inspect. Досліджено шляхи та методи, які використовуються для забезпечення безпеки інформаційного середовища організацій.

Визначено ключові аспекти захисту інформаційного середовища організацій та принципи їх реалізації. Розглянуто сучасні методи захисту цих середовищ та запропоновано альтернативні методи, які ефективно використовуються для захисту корпоративних систем сьогодні.

Рекомендації, розроблені на основі дослідження сучасних практик, наукових статей та міжнародних стандартів, спрямовані на підвищення рівня захисту інформаційного середовища організацій без значної інтерференції з ефективністю зазначених процесів.

Здобуті результати дослідження вказують на значну загальну вразливість до APT атак та підкреслюють значення сегментації мережі та якісного планування у процесі побудови захищених середовищ.

Практичне значення одержаних результатів полягає у можливості застосування розроблених рекомендацій у різних організаціях, де критично важливим є забезпечення надійності та безпеки інформаційних систем. Використання ESET Protect та Inspect дозволяє значно скоротити час реагування на інциденти, підвищити рівень захисту від APT атак та забезпечити стабільну роботу організаційної інфраструктури.

У підсумку, проведене дослідження підтвердило ефективність використання сучасних інструментів кібербезпеки для захисту інформаційного середовища організацій. Розроблені рекомендації можуть стати основою для подальших досліджень та впровадження у практику нових підходів до забезпечення кібербезпеки. Дана робота сприяє підвищенню рівня безпеки та стійкості інформаційних систем до сучасних кіберзагроз, що є важливим кроком у розвитку захищених інформаційних середовищ.

ПЕРЕЛІК ПОСИЛАНЬ

1. NIST, COMPUTER SECURITY RESOURCE CENTER, Cyber Attack definition. URL: https://csrc.nist.gov/glossary/term/cyber_attack

2. IBM, What are advanced persistent threats? URL: https://www.ibm.com/topics/advanced-persistent-threats

3. America`s Cyber Defense Agency, Cyber-Attack Against Ukrainian Critical Infrastructure. URL: https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01

4. Reuters, U.S. firm blames Russian 'Sandworm' hackers for Ukraine outage. URL: https://www.reuters.com/article/us-ukraine-cybersecurity-sandworm-idUSKBN0UM00N20160108

5. IBM, What is a zero-day exploit? URL:https://www.ibm.com/topics/zero-day

6. TrendMicro, The Hack of Sony Pictures: What We Know and What You Need to Know. URL: https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/the-hack-of-sony-pictures-what-you-need-to-know

7. America`s Cyber Defense Agency, Avoiding Social Engineering and Phishing Attacks. URL: https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks

8. NIST, Guide to Intrusion Detection and Prevention Systems (IDPS). URL: https://www.nist.gov/publications/guide-intrusion-detection-and-prevention-systems-idps

9. IBM, What is security information and event management (SIEM)? URL: https://www.ibm.com/topics/siem

10. KROLL, The State of Incident Response - Findings Highlight Growing Reliance on IR and MDR Partners. URL: https://www.kroll.com/en/insights/publications/cyber/state-of-incident-response

11. RAPID7, SOC Automation: Threat Detection and Response with SIEM and SOAR. URL: https://www.rapid7.com/blog/post/2020/04/02/soc-automation-accelerate-threat-detection-and-response-with-siem-and-soar

12. ESET, Extended detection & response. URL: https://www.eset.com/int/business/solutions/xdr-extended-detection-and-response

13. ESET, ESET спільно з представником ДССЗЗІ України розповіли про загрозу Industroyer2 на конференції Black Hat. URL: https://www.eset.com/ua/about/newsroom/press-releases/company/eset-sovmestno-s-predstavitelem-dsszi-ukrainy-predstavili-issledovanie-ugrozy-industroyer2

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙН ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІ
КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Кваліфікаційна робота
на тему:

«Дослідження шляхів і розробка рекомендацій щодо зменшення часу реагування на APT атаки на робочих станціях на основі ESET Protect та Inspect»

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»

Виконав студент групи БСД-42: Артем МУРАВЙОВ
Керівник роботи: д.ф. доцент, Віталій МАРЧЕНКО

2

Об'єкт дослідження – процес забезпечення зменшення часу реагування на APT атаки

Предмет дослідження – методи та засоби зменшення часу реагування на APT атаки

Мета роботи – розробити рекомендації щодо застосування новітніх практик та покращення існуючих механізмів реагування на APT атаки.

Наукові завдання:

- Визначити ключові аспекти для захисту від APT атак.
- Проаналізувати існуючі методології та рекомендації для захисту від сучасних APT загроз.
- Визначити вимоги до рішень, які можуть використовуватись для захисту в інформаційному середовищі організацій.
- Розробити рекомендації щодо підвищення рівня безпеки інформаційного середовища організацій та держустанов в контексті захисту від APT атак.

Важливість захисту від APT атак

3

APT атаки є складними, цілеспрямованими та тривалими кібератаками, які використовують методи фішингу, соціальної інженерії та експлуатації вразливостей для проникнення в системи організацій. Ці атаки можуть завдати значної шкоди, включаючи викрадення конфіденційних даних, фінансові втрати та порушення нормальної діяльності. Для ефективного захисту від APT атак необхідно застосовувати комплексний підхід, який включає як технічні засоби, так і організаційні заходи, щоб вчасно виявляти і нейтралізувати загрози.

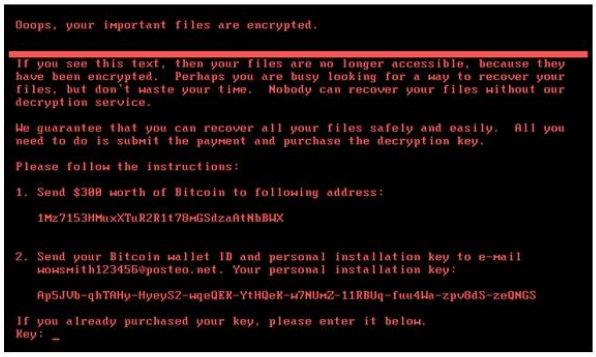

Рис. 1.1. Екран зашифрованої кінцевої точки як результат APT атаки

4

APT Атаки мають безліч способів розповсюдження, але як самі популярні та :

Фішинг та соціальна інженерія — це вид кібератаки, при якій зловмисники використовують підроблені повідомлення (зазвичай електронні листи або повідомлення в меседжерах), щоб змусити користувачів розкрити конфіденційну інформацію, таку як облікові дані, фінансова інформація, інша чутлива інформація. Ці атаки часто виглядають як легітимні запити від надійних джерел. Фішинг може бути спрямований на конкретних осіб або групи, використовуючи інфо

Експлуатація вразливостей — – це помилки або слабкі місця в коді, які можуть бути використані зловмисниками для отримання несанкціонованого доступу до систем. Особливо небезпечними є вразливості нульового дня, які залишаються невідомими до моменту їх експлуатації, що дозволяє зловмисникам діяти без перешкод до випуску виправлення виробником. Після виявлення вразливості вони розробляють експлоїти – спеціальні програми, які дозволяють використовувати ці вразливості для проникнення в систему

Атака на ланцюжок постачання — Зловмисники проникають через вразливості у постачальників або партнерів, що є частиною ланцюжка постачання. Такий підхід дозволяє зловмисникам проникнути в цільові системи через менш захищені точки доступу

Атака Industroyer2 як приклад APT атаки

5

Під час нової атаки кіберзлочинці зробили спробу розгорнути шкідливе програмне забезпечення Industroyer2 на високовольтних електричних підстанціях в Україні. На додаток до Industroyer2, група Sandworm використала декілька сімейств шкідливих програм для знищення даних, зокрема CaddyWiper.

«Нейтралізувати атаку Industroyer2 вдалося завдяки оперативному реагуванню українських захисників та CERT-UA. Ми надали українській стороні детальний аналіз загрози, яка у разі успіху могла б стати наймасштабнішою кібератакою від початку вторгнення. Наші дослідники готові й надалі співпрацювати із CERT-UA задля покращення кіберзахисту» — заявив Роберт Ліповський, дослідник ESET, на конференції Black Hat під час доповіді щодо Industroyer2.

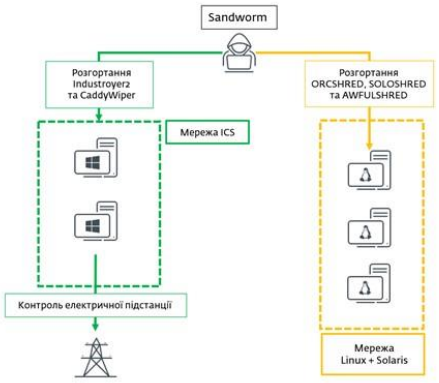

Рис.2.1. модель атаки

Методи та технології захисту від APT атак

6

Системи виявлення вторгнень (IDS) — IDS є одним із ключових інструментів у боротьбі з APT атаками. Вони можуть бути налаштовані для моніторингу мережевого трафіку та аналізу подій у реальному часі з метою виявлення підозрілої активності. Існує два основних типи IDS: мережеві (NIDS) та хостові (HIDS).

Системи управління подіями безпеки (SIEM) — SIEM забезпечують централізоване збирання, аналіз та кореляцію подій безпеки з різних джерел у реальному часі. Вони дозволяють виявляти складні атаки, що можуть залишатися непоміченими при використанні окремих інструментів. SIEM використовують правила кореляції, що базуються на підписах та поведінковому аналізі, для ідентифікації підозрілих активностей та інцидентів безпеки.

Extended Detection and Response (XDR) — інтегрує дані з різних джерел, що забезпечує комплексне виявлення загроз, автоматизує процеси аналізу та реагування, зменшуючи час реакції на інциденти, та надає повну картину стану безпеки організації.

7

Розробка рекомендацій щодо зменшення часу реагування на APT атаки

Гарантованого захисту від APT атак не існує через їх складність і використання вразливостей нульового дня. APT атаки представляють собою тривалі та цілеспрямовані кібернапади, що можуть залишатися непоміченими протягом тривалого часу, оскільки зловмисники часто використовують новітні та раніше невідомі методи атак.

Важливість пришвидшення реагування на APT атаки

Пришвидшення реагування на APT атаки є критично важливим з кількох причин. По-перше, своєчасна реакція дозволяє мінімізувати шкоду від атак. APT атаки можуть бути тривалими та цілеспрямованими, що дає зловмисникам можливість завдати значної шкоди, якщо атака залишається непоміченою або на неї реагують занадто пізно.

Крім того, миттєва реакція від відділу кіберзахисту дозволяє суттєво знизити вплив атак та захистити критичну інфраструктуру. Критична інфраструктура, така як енергетичні мережі, фінансові системи та урядові установи, є основною ціллю для APT атак через їх стратегічну важливість. Пошкодження таких систем може мати далекосяжні наслідки не тільки для окремої організації, але й для економіки та національної безпеки в цілому. Швидке реагування допомагає забезпечити стабільність та захист найважливіших ресурсів

8

Розробка рекомендацій щодо зменшення часу реагування на APT атаки

Моніторинг та оновлення індикаторів компрометації (IOC): Слідкування за новими індикаторами компрометації (IOC) на сайті CERT-UA є важливою складовою захисту. IOC включають в себе різні маркери, такі як хеші файлів, IP-адреси, домени та URL-адреси, які вказують на потенційно зловмисну активність. Оперативне оновлення правил захисту дозволяє уникнути багатьох атак

Автоматизація сповіщень: Автоматизація процесів сповіщення є ключовим елементом пришвидшення реагування на загрози. Додавання автоматизованих попереджень на email-адреси для спрацювань за індикаторами компрометації дозволяє відповідальним особам отримувати своєчасні сповіщення та оперативно реагувати на виявлені загрози.

Додавання виключень на перевірені виявлення: Додавання виключень на вже перевірені виявлення на кінцевих точках також внесе свій вклад у пришвидшення реагування на нові загрози. Створення унікальних виключень для груп кінцевих точок зменшує кількість хибнопозитивних спрацювань, що пришвидшує їх аналіз.

Аналіз аномальної активності: Атаки часто супроводжуються збільшенням виявлень на кінцевих точках. Отримання цього показника у реальному часі, наприклад за допомогою звітів, що генеруються кожну хвилину, та порівняння з середньодобовим за минулий тиждень, може вказувати на аномальну активність.