ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до бакалаврської роботи

на тему:

ДОСЛІДЖЕННЯ ШЛЯХІВ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ ВІД ПРОГРАМ-ВИМАГАЧІВ КОРПОРАТИВНОГО СЕРЕДОВИЩА НА БАЗІ ACRONIS

Виконав студент 4 курсу, групи БСД-41
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Кагарлик Д. Т.
(прізвище та ініціали)
Керівник Гайдур Г.І.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2023

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

Somnia, RansomBoggs, Prestige – назви атк програм-вимагачів

Protect – захист

Ransomware – програма-вимагач

ВСТУП

Актуальність дослідження. Актуальність виявлення програм-вимагачів в інфраструктурі організації неможливо переоцінити. Останніми роками атаки програм-вимагачів стають все більш поширеними та можуть завдати значної шкоди даним, репутації та фінансовій стабільності організації.

Якщо програму-вимагач виявлено на ранній стадії, можна запобігти шифруванню критичних файлів і мінімізувати вплив атаки. Однак, якщо програми-вимагачі залишаються непоміченими, вони можуть поширюватися мережею організації та шифрувати всі файли, роблячи їх недоступними та спричиняючи значні простої та втрату продуктивності.

Крім того, атаки програм-вимагачів часто призводять до вимоги викупу з боку зловмисників, що може бути дорогим для організацій і може не гарантувати повернення зашифрованих даних.

Впроваджуючи ефективні заходи виявлення програм-вимагачів, організації можуть зменшити ризик атак програм-вимагачів і пом’якшити вплив будь-яких атак, які трапляються. Це включає в себе впровадження заходів безпеки, таких як брандмауери, системи виявлення вторгнень і антивірусне програмне забезпечення, а також проведення регулярних оцінок уразливості та навчання співробітників, щоб переконатися, що співробітники обізнані про ризики атак програм-вимагачів і знають, як їх уникнути.

Згідно з різними звітами та дослідженнями, останніми роками кількість атак програм-вимагачів зростає, а фінансові збитки, завдані цими атаками, значні.

Наприклад, згідно зі звітом SonicWall Cyber Threat Report за 2021 рік, у 2020 році число атак програм-вимагачів у всьому світі зросло на 62%, було зареєстровано понад 304 мільйони атак програм-вимагачів. У звіті також зазначається, що середня сума викупу зросла на 171% у 2020 році, причому найвища зареєстрована сума викупу становила 30 мільйонів доларів.

Крім того, у звіті Coveware, фірми з відновлення програм-вимагачів, за 2021 рік було встановлено, що середня сума викупу в першому кварталі 2021 року становила 220 298 доларів США, причому найбільша зареєстрована сума викупу становила 50 мільйонів доларів.

Ці статистичні дані підкреслюють важливість виявлення та запобігання атакам програм-вимагачів в інфраструктурах організацій. Впроваджуючи ефективні заходи безпеки та проводячи регулярне навчання співробітників, організації можуть зменшити ризик атак програм-вимагачів і пом’якшити вплив будь-яких атак, які трапляються.

Таким чином, виявлення програм-вимагачів в інфраструктурі організації має вирішальне значення для запобігання та пом’якшення впливу атак програм-вимагачів, які можуть мати серйозні наслідки для організацій будь-якого розміру. Тому тема бакалаврської роботи є своєчасною та актуальною.

Об’єкт дослідження – процес протидії програмам-вимагачам в інформаційній системі організації.

Предмет дослідження – методи та засоби захисту від програм-вимагачів корпоративне середовища на базі Acronis.

Мета роботи – розробити рекомендації щодо застосування методів та засобів протидії програмам-вимагачам в інформаційній системі організації на базі Acronis.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Завдання бакалаврської роботи:

дослідити загрози, які виникають та їх наслідок від атак програм-вимагачів в інфраструктурі організації;

визначити методи та засоби протидії програмам-вимагачам в інформаційній системі організації;

розробити рекомендації щодо застосування методів та засобів протидії програмам-вимагачам в інформаційній системі організації на базі Acronis.

Практичне значення одержаних результатів: рекомендації протидії програмам-вимагачам в інформаційній системі організації, які можуть бути використані у сфері забезпечення кібербезпеки у корпоративних інформаційних системах.

1 АНАЛІЗ ВПРОВАДЖЕННЯ СИСТЕМ ПРОТИДІЇ ПРОГРАМАМ-ВИМАГАЧАМ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ОРГАНІЗАЦІЇ

1.1. Аналіз вразливості організацій від атак програм - вимагачів.

Атаки програм-вимагачів є значною загрозою для організацій будь-якого розміру та галузей. Ось аналіз уразливості організацій від атак програм-вимагачів:

Залежність від технологій: багато організацій значною мірою покладаються на технології у своїй повсякденній діяльності, що робить їх уразливими до атак програм-вимагачів. Це особливо вірно для організацій, які покладаються на хмарні служби або мають співробітників, які працюють віддалено.

Недостатня обізнаність співробітників: атаки програм-вимагачів часто поширюються через фішингові електронні листи або інші методи соціальної інженерії. Багато співробітників можуть не знати про ризики або знати, як ідентифікувати підозрілі електронні листи, що робить їх більш уразливими до цих атак.

Застаріле програмне забезпечення та системи: атаки програм-вимагачів часто використовують уразливості застарілого програмного забезпечення та систем. Організації, які не оновлюють своє програмне забезпечення та системи останніми виправленнями та оновленнями системи безпеки, більш уразливі до цих атак.

Відсутність резервних копій: організації, які не регулярно створюють резервні копії своїх даних, більш уразливі до атак програм-вимагачів. Без резервного копіювання вони можуть бути змушені заплатити викуп за відновлення своїх даних, що може бути дорогим і навіть не гарантувати повернення їхніх даних.

Складність IT-інфраструктури. Організації зі складною IT-інфраструктурою можуть бути більш уразливими до атак програм-вимагачів. Це пояснюється тим, що

може бути важче захистити та контролювати всі різноманітні системи та пристрої, які є частиною інфраструктури.

Відсутність політики безпеки: організації, які не мають чіткої політики та процедур безпеки, можуть бути більш уразливими до атак програм-вимагачів. Це може включати політику щодо навчання співробітників, контролю доступу та реагування на інциденти.

Фінансові стимули для зловмисників: атаки програм-вимагачів часто мають фінансову мотивацію, і зловмисники можуть націлитися на організації, які, на їхню думку, швидше за все сплатять викуп. Це може включати організації, які, як вважають, мають глибокі кишені або цінні дані.

Загалом організації будь-якого розміру та галузі вразливі до атак програм-вимагачів. Для організацій важливо проявляти активність у своєму підході до кібербезпеки, зокрема регулярно створювати резервні копії своїх даних, оновлювати свої системи, навчати працівників безпечним практикам і мати чіткі політики та процедури безпеки. Вживаючи цих заходів, організації можуть допомогти зменшити свою вразливість до атак програм-вимагачів і мінімізувати вплив будь-яких атак, які трапляються.

Організації є вразливими до програм-вимагачів. Існує вектор атаки за яким працюють вимагачі. Вимагачам потрібна точка входу для атаки на мережу. Незалежно від того, чи є це недоліком безпеки в застарілому програмному забезпеченні, слабким паролем, викраденими обліковими даними для входу чи навіть довірливим співробітником, кіберзлочинці знайдуть спосіб використати вразливість і отримати своє програмне забезпечення-вимагач. Дедалі частіше зловмисники навіть вербували співробітників , щоб отримати внутрішній доступ до внутрішніх систем цільової організації [3,4]. Вектор атак на інформаційну систему організації для проведення атаки програми-вимагача показано на рис.1.1.

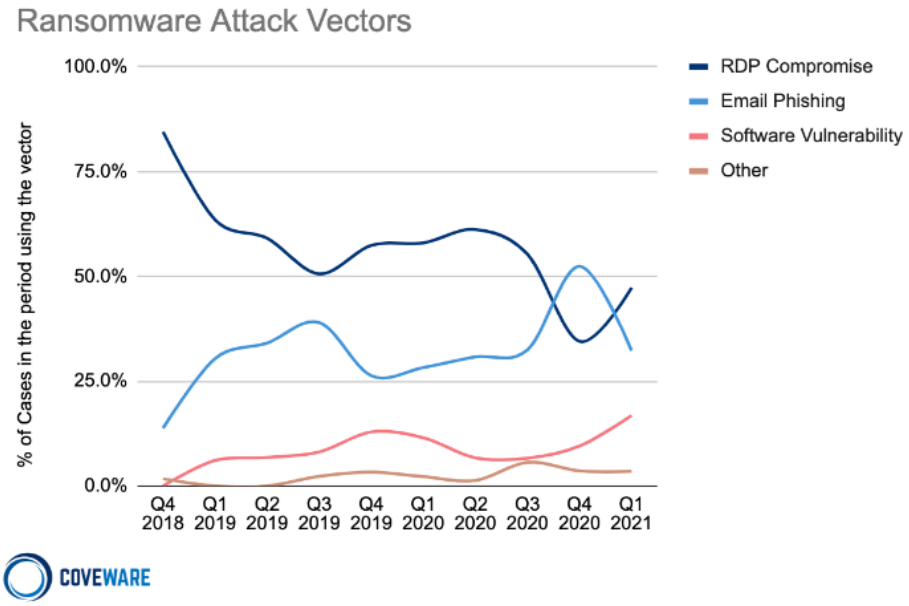

Рис.1.1. Вектор атак на організації для поширення програм-вимагачів

Фішингові листи

Фішингові атаки – це електронні листи та інші повідомлення, призначені для того, щоб оманою змусити когось розкрити конфіденційні особисті дані або відкрити шкідливий файл [3].

Фішингові кампанії націлені на конкретних осіб, тоді як китобійні атаки спрямовані на високовартісних людей, таких як керівники старших класів. Кількість шкідливих електронних листів зросла на 600% під час триваючої кризи COVID-19 [3].

Протокол віддаленого робочого столу

Протокол віддаленого робочого стола Microsoft (RDP) дозволяє мережевим адміністраторам легко отримувати доступ до пристроїв у їхніх мережах. Але з правильними обліковими даними для входу хакери можуть зробити те саме [3].

Законні облікові дані адміністратора можна отримати за допомогою фішингу, витоку даних, злому методом грубої сили або введення облікових даних (з використанням відомих комбінацій імені користувача та пароля на інших порталах входу). Зробити віддалений доступ доступним лише через VPN-з’єднання , а не розкривати його для всього Інтернету, є одним із способів, як компанії можуть краще захистити від уразливостей RDP [3].

Уразливості програмного забезпечення

Хакери використовують уразливості в застарілому програмному забезпеченні, щоб зламати незахищені системи та сервери, включно з корпоративними серверами VPN, і встановити програми-вимагачі. Використання поточного програмного забезпечення є найкращим способом закрити цей тип вектора атак програм-вимагачів [3].

Деякі банди програм-вимагачів заробили стільки грошей, що вони достатньо багаті, щоб придбати вразливості нульового дня , що є нещодавно виявленими слабкими місцями, які залишаються невідомими розробникам програмного забезпечення. Кібератаки, які використовують ці недоліки безпеки, називаються експлойтами нульового дня [3].

Розглянемо для прикладу вектор атаки програми-вимагача від початку до отримання цілі.

1. Фішинг
2. Програмне забезпечення віддаленого доступу
3. Дамп облікових даних ОС
4. Інтерпретатор команд і сценаріїв.
5. Віддалене керування Windows.
6. Виявлення облікового запису.
7. Створення облікового запису.
8. Дійсні облікові записи: облікові записи домену.
9. Порушити захист.
10. Викрадання через веб-службу.
11. Знищення даних.
12. Дані зашифровані для впливу.

Отже, організаціям необхідно ретельно підходити до захисту своєї організаці, шляхом використання спеціалізованого програмного забезпечення, з метою виявлення та протидійї атакам програм-вимагачів.

1.2. Аналіз загроз від програм-вимагачів в організаціях при надані послуг

Загрози програм-вимагачів створюють значні ризики для організацій як у плані фінансових втрат, так і з точки зору репутаційної шкоди. Ось аналіз загроз від програм-вимагачів в організаціях:

Фінансові збитки: атаки програм-вимагачів можуть призвести до значних фінансових втрат для організацій, включаючи вартість виплати викупу, вартість відновлення даних і вартість втрати продуктивності під час простою. У деяких випадках ціна атаки програм-вимагачів може бути настільки високою, що призведе до закриття організації.

Втрата даних: атаки програм-вимагачів можуть призвести до втрати важливих даних, зокрема конфіденційної інформації про клієнтів, фінансових даних та інтелектуальної власності. Це може мати значний вплив на роботу та репутацію організації.

Порушення роботи: атаки програм-вимагачів можуть спричинити значні збої в роботі організації, зокрема простої та втрату продуктивності. Це може призвести до порушення термінів, затримки проектів і зниження задоволеності клієнтів.

Шкода репутації: атаки програм-вимагачів можуть завдати шкоди репутації організації, особливо якщо конфіденційні дані втрачено або інформація про клієнта скомпрометована. Це може призвести до втрати довіри з боку клієнтів і зацікавлених сторін.

Відповідність нормативним вимогам. Багато галузей підпадають під дію нормативних вимог щодо захисту даних і конфіденційності. Атаки програм-вимагачів, які призводять до втрати даних або несанкціонованого доступу, можуть призвести до невідповідності та потенційних юридичних і фінансових наслідків.

Ризик ланцюжка постачання. Атаки програм-вимагачів також можуть становити загрозу для ланцюга постачання організації, особливо якщо критичні постачальники постраждали від атаки. Це може призвести до збоїв у роботі організації та ланцюгу постачання.

Загалом програми-вимагачі створюють значні ризики для організацій будь-якого розміру та галузей. Організаціям важливо вживати профілактичних заходів, щоб захистити себе від атак програм-вимагачів, зокрема регулярно створювати резервні копії даних, оновлювати програмне забезпечення та системи, навчати працівників безпечним методам, а також мати чіткі політики та процедури безпеки. Здійснюючи ці кроки, організації можуть допомогти знизити ризики атак програм-вимагачів і мінімізувати вплив будь-яких атак, які трапляються.

Постачальники послуг не захищені від програм-вимагачів. 7 з 10 компаній визнають, що не готові відповісти на атаку;

31% компаній повідомляють про щоденні кібератаки;

13 000 доларів США це середня сума викупу, яку вимагають від організацій;

250 000 доларів на годину - це середня вартість незапланованих простоїв.

Так, коли в березні 2020 року почалася пандемія Covid-19, 10 постачальників медичних послуг у США зазнали атаки групи програм-вимагачів Ryuk. Група програм-вимагачів спиралася на той факт, що нагальна потреба в доступі до систем і файлів пацієнтів спонукатиме цих працівників швидко платити.

Будівельну компанію Bouygues було скомпроментовано програмою-вимагачем Maze. Сотні систем були заражені, що вплинуло на роботу компанії у всьому світі на декілька днів. Вимога в розмірі 10млн.евро не була виплачена.

Finastra – одна з найбільших у світі фітнес компній була змушена виключити критично важливі системи від атаки програми-вимагача. Атака була спрямована на конфіденційні дані, що порушило роботу багатьох клієнтів.

На одну з найбільших страхових компаній США CNA було здійснено кібератаку з використанням нового варіанту шкідливого ПЗ Phoenix CryptoLocker. 21 березня

зловмисники розгорнули в мережі CNA програму-вимагач, що зашифрувала 15 тис. пристроїв. Шифрувальник також захопив комп'ютери співробітників, що працюють віддалено, які під час атаки були підключені до корпоративного VPN.

Німецький технологічний гігінт Softwere AG по страждав від програми-вимагача Clop із вимогою 20 млн. доларів. Коли переговори про виплату припинили, Clop почав зливати інформацію в темну мережу.

Зокрема українських користувачів атакували такі шкідливі програми з цієї категорії, як Somnia, RansomBoggs та Prestige. Загроза Somnia для знищення даних атакувала українські організації в листопаді. Тоді як інша програма-вимагач RansomBoggs, яка пов'язана з російською групою кіберзлочинців Sandworm, теж була націлена на установи в Україні. Ще одна програма Prestige з цієї категорії атакувала логістичні компанії в Україні та Польщі [2].

За цей період найбільша кількість виявлених зразків програм-вимагачів була зафіксована у Китаї та США, а Україна опинилася на 4 місці, як за підсумками жовтня-грудня, так і всього 2022 року.

Значне зростання кількості атак програм-вимагачів за останні роки можна здебільшого пояснити одним фактором: впровадженням RaaS, або програми-вимагача як послуги . У цій системі розробник створює різновид програм-вимагачів, а потім ліцензує її іншим кіберзлочинцям для використання в їхніх атаках. Таким чином, модель RaaS має дві основні переваги для хакерів:

Найпоширеніші цілі атак програм-вимагачів

Хоча загальна кількість атак зростає, цілями нападів стають частіші певні сектори економіки. Зокрема, уряд, технології, охорона здоров'я та наукові установи поглинули основну масу атак. З усіх розглянутих атак лише на ці чотири сектори припадає 57% усіх атак.

За цей час технологічний сектор опинився під дедалі більшою загрозою. З 2017 по 2019 рік лише 7% зареєстрованих атак програм-вимагачів були спрямовані на технологічні компанії. За останні два роки ця частка підскочила до понад 20%.

Хоча атаки на державні установи часто мають політичні мотиви, хакери, які атакують технічні та медичні організації, можуть вважати, що ці групи мають більшу ймовірність заплатити. Крім того, наше власне дослідження виявило, що лікарням і постачальникам медичних послуг може не вистачати бюджету, необхідного для оновлення своїх систем, що робить їхню інфраструктуру безпеки більш вразливою.

Ось огляд найпоширеніших цілей програм-вимагачів у розбивці за роками та секторами.

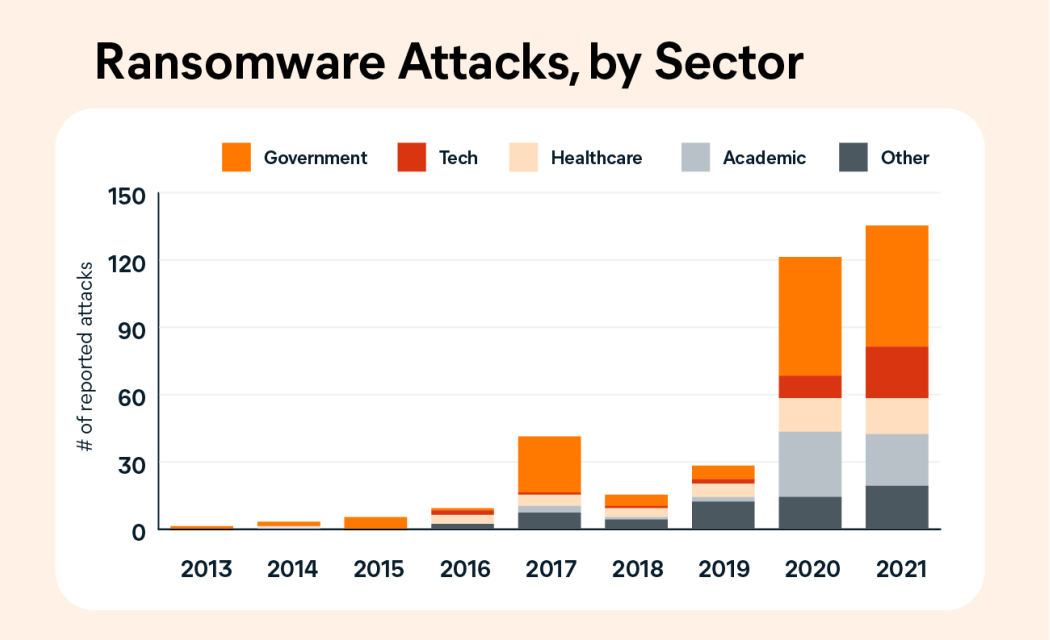

Рис.1.1. Статистика атак по галузям

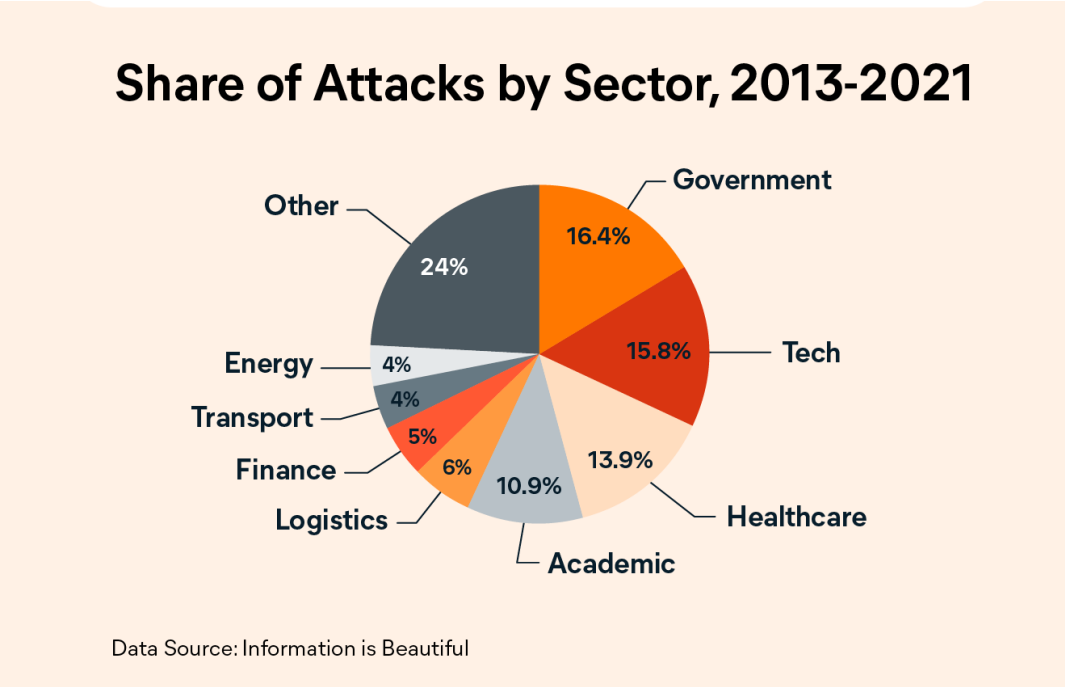

Рис 1.2. Цілі програм-вимагачів [3]

Атаки програм-вимагачів за країнами

Атаки програм-вимагачів відбуваються по всьому світу, але організації в США стають цілями частіше, ніж організації зі штаб-квартирами в іншому місці. Стверджується, що багато провідних груп програм-вимагачів базуються в росії та інших країнах Східної Європи, і вони, як правило, уникають націлювання на жертв у своєму регіоні. Це пов’язано з переконанням, що російський уряд зазвичай відмовляється переслідувати кіберзлочинців, які атакують лише іноземні цілі .

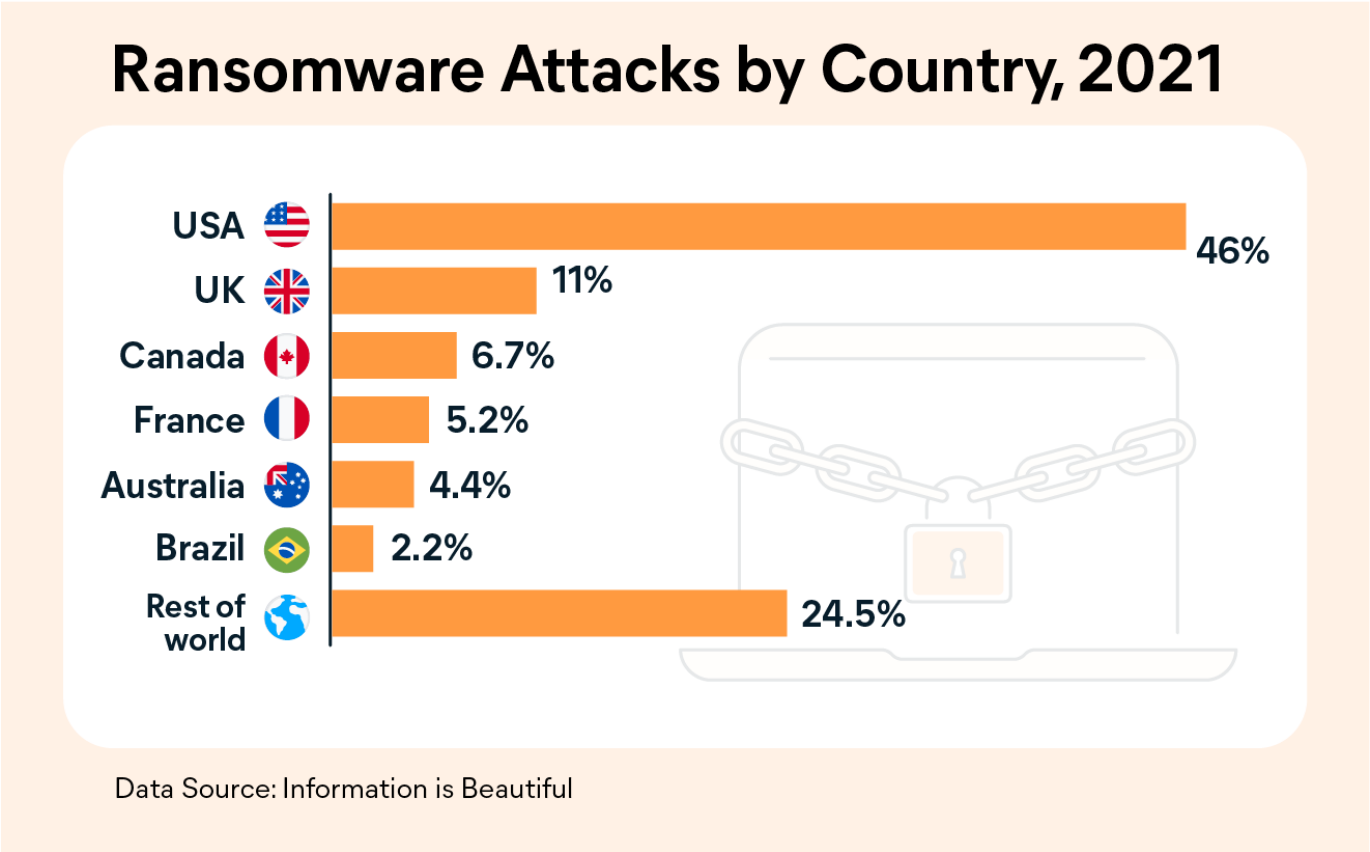

Рис. 1.3. Кількість атак програм-вимагачів[3]

Масштабні атаки програм-вимагачів можуть призвести до майже повного припинення роботи організації, і легко може здатися, що сплата викупу є найкращим способом повернути все до нормального стану.

Запобігання атакам програм-вимагачів вимагає пильності як від організацій, так і від окремих осіб. Організації повинні захищати свої мережі від вторгнень, навчаючи персонал розпізнавати атаки. Тим часом кожен може захиститися від програм-вимагачів , дотримуючись основних правил щодо кібербезпеки.

Найпоширеніші варіанти програм-вимагачів у першому кварталі 2021 року

Rank	Ransomware Type	Market Share %	Change in Ranking from Q4 2020
1	Sodinokibi	14.2%	-
2	Conti V2	10.2%	+4
3	Lockbit	7.5%	+6
4	Clop	7.1%	New in Top Variants
5	Egregor	5.3%	-3
6	Avaddon	4.4%	+3
7	Ryuk	4.0%	-4
8	Darkside	3.5%	New in Top Variants
9	Suncrypt	3.1%	-1
9	Netwalker	3.1%	-5
10	Phobos	2.7%	-1

Top 10: Market Share of the Ransomware attacks

Рис. 1.4. Найпоширеніші варіанти програм-вимагачів [4]

1.3. Аналіз рішень для вибору рішень протидії програмам-вимагачів в організації

Для якісного та надійного захисту інформаційної системи організації від вірусів потрібні потужні засоби захисту, як антивірусні так і інші. Зазвичай, у більшості випадків всі зараження комп'ютера та пов'язані із цим неприємності стаються по вині самого користувача. А це може бути крадіжка особистої або конфіденційної інформації інформації (номерів банківських карточок, паролів та ін.), видалення важливих даних з інформаційної системи, а також шифрування інформації із наступним вимаганням грошей за те, що її розшифрувують. Тому про кібербезпеку організації необхідно завчасно подбати.

Особливо важливо антивірусним захистом використовувати резервне копіювання даних. Тут можливо скористатися вбудованою у Windows функцією, але для кращого захисту організацій необхідно користатися більш надійними рішеннями. Такими рішеннями є програми, для прикладу, Acronis Cyber Protect, Paragon Drive Backup, Aomei Backupper, R-Drive Image та інші. Тут можна знайти як безкоштовні версії так і професійні із порівняно більшим функціоналом. Але краще брати в організації професійні – ліцензійні версії.

Сучасні антивірусні рішення хоч і забезпечує захист інформаційних систем, але для захисту від програм-вимагачів необхідно застосовувати додатково встановлювати одну із спеціальних утиліт. Такі утиліти виправлять наслідки діяльності шкідливих програм (крім розшифрування файлів). До таких відносяться: RansomFree, Malwarebytes Anti-Ransomware, CryptoPrevent. Вони допоможуть видалити такі програми-вимагачі як WannaCry, Cryptolocker, Locky та ін.

Щоб дізнатися, який саме вірус-вимагач заразив інформаційну систему потрібно запустити безкоштовний веб-додаток ID Ransomware. Для ідентифікації цього вірусу потрібно завантажити ReadMe файл із вимогами вірусу або сам заражений файл. Дізнатися саме який вірус достатньо важливо, оскільки ідентифікація порушника допоможе більш точно скласти план необхідних дій для нейтралізації атаки.

Розглянемо призначення деяких програм, які протидіють програмам-вимагачам.

Trend Micro Anti Ransomware — програмний продукт, який призначений для боротьби із вірусними програмами-вимагачами, які блокують робочий стіл [4].

Перший використовується у випадку якщо заблокований вхід у ОС в звичайному режимі але в безпечному режимі можна зайти на комп’ютер (скриншот зверху).

В другому випадку на комп’ютер не виходить зайти у жодному із режимів. В такому випадку завантажується інша версія продукту, запустивши яку (на іншому комп’ютері, звичайно) з’явиться вікно для створення завантажувального носія із якого потрібно завантажитися та просканувати систему.

Cybereason RansomFree — безкоштовна програма для комп'ютерів під керуванням ОС Windows, яка захистить від програм шифрувальників. Для виявлення троянів-шифрувальників дане рішення використовує поведінковий аналіз замість сигнатурних виявлень. Як тільки відбудеться шифрування файлів RansomFree запропонує користувачеві дозволити його чи зупинити та видалити джерело шифрування. Тестування показали, що програма ефективна проти 99 відсотків шифрувальників та включає такі трояни як Locky, Cryptowall, TeslaCrypt, Jigsaw, Cerber та інші. Дана розробка зможе захистити навіть від ще невідомих троянських програм, оскільки вони скоріш за все будуть використовувати схожі методи шифрування [4].

Рішення безкоштовне для використання та може працювати разом із основним антивірусом.

Malwarebytes Anti-Ransomware — безкоштовне рішення для захисту від програм-вимагачів (CryptoLocker, CryptoWall чи CTBLocker). Програма використовує проактивні технології та сумісна із вже встановленим антивірусом. Даний продукт, використовуючи моніторинг системи із метою пошуку програм-вимагачів здатний зупинити загрозу ще до того як вона почне змінювати користувацькі файли. Програма має за результатами тестів високу ефективність та здатна знаходити самі нові версії програм-вимагачів, навіть ті, які ще не зустрічалися.

Acronis Ransomware Protection використовує комбінацію сигнатурних і поведінкових методів для виявлення атак програм-вимагачів. Ось як працює кожен метод:

Виявлення на основі сигнатур: Acronis Ransomware Protection використовує виявлення на основі сигнатур для виявлення відомих загроз програм-вимагачів. Цей метод передбачає порівняння поведінки файлів у вашій системі з базою даних відомих сигнатур програм-вимагачів. Якщо він знайде збіг, він негайно заблокує програму-вимагач і не дозволить їй зашифрувати ваші файли.

Виявлення на основі поведінки: Acronis Ransomware Protection також використовує виявлення на основі поведінки для виявлення нових і невідомих загроз програм-вимагачів. Цей метод передбачає моніторинг поведінки файлів і програм у вашій системі на наявність підозрілої активності. Він шукає закономірності та аномалії, які можуть свідчити про атаку програм-вимагачів. Наприклад, він може шукати раптові сплески шифрування файлів або незвичні зміни розширень файлів. Якщо він виявить будь-яку підозрілу активність, він негайно заблокує програму-вимагач і відновить усі зашифровані файли до початкового стану.

Загалом, Acronis Ransomware Protection розроблено як комплексний захист від атак програм-вимагачів. Використовуючи методи виявлення як на основі сигнатур, так і на основі поведінки, він може швидко виявляти та реагувати на відомі та невідомі загрози програм-вимагачів. Це допомагає гарантувати, що і файли захищено від атак програм-вимагачів і що адміністратор безпеки зможете швидко відновити будь-яку завдану шкоду.

Тож для подальшого дослідження шляхів протидії програмам-вимагачам будемо розглядати Acronis Ransomware Protection.

2 МЕТОДИ ТА ЗАСОБИ ЩОДО ЗАХИСТУ ВІД ПРОГРАМ-ВИМАГАЧІВ КОРПОРАТИВНЕ СЕРЕДОВИЩА НА БАЗІ ACRONIS

2.1 Компоненти архітектури рішення Acronis Cyber Protect

Метою Acronis Cyber Protect є надання комплексного рішення кібербезпеки, яке поєднує захист даних і можливості резервного копіювання з розширеними функціями кібербезпеки для захисту від сучасних загроз, таких як зловмисне програмне забезпечення, програми-вимагачі та фішингові атаки.

Acronis Cyber Protect пропонує єдине рішення, яке об’єднує резервне копіювання, аварійне відновлення, захист від зловмисного програмного забезпечення на основі штучного інтелекту, програмне забезпечення-вимагач та інші функції безпеки в одному рішенні. Мета полягає в тому, щоб спростити управління кібербезпекою та захистом даних, зробивши їх більш доступними для компаній будь-якого розміру.

Основні функції Acronis Cyber Protect включають:

Резервне копіювання та відновлення: Acronis Cyber Protect пропонує розширені можливості резервного копіювання та відновлення, які дозволяють компаніям швидко відновлювати дані після втрати даних або аварій.

Захист від зловмисних програм і програм-вимагачів: рішення використовує функції захисту від шкідливих програм і програм-вимагачів на базі ШІ для захисту від найновіших загроз і запобігання втраті даних.

Керування виправленнями: рішення містить функції керування виправленнями, які автоматизують оновлення програмного забезпечення, зменшуючи ризик кібератак, які використовують уразливості застарілого програмного забезпечення.

Навчання з питань кібербезпеки: Acronis Cyber Protect включає навчання з питань кібербезпеки, щоб допомогти співробітникам розпізнавати загрози безпеці та реагувати на них.

Віддалений доступ до робочого столу: рішення містить функції доступу до віддаленого робочого столу, які забезпечують віддалений доступ до робочих станцій і серверів, дозволяючи підприємствам безпечно підтримувати віддалену робочу силу.

Мета Acronis Cyber Protect — надати компаніям комплексне рішення, яке захищає від сучасних загроз кібербезпеці, одночасно спрощуючи керування захистом даних і кібербезпекою.

Acronis Cyber Protect — це комплексне рішення для кіберзахисту, яке пропонує численні можливості для забезпечення безпеки даних, програм і систем. Окрім резервного копіювання та аварійного відновлення, захисту від зловмисного програмного забезпечення та керування виправленнями, Acronis Cyber Protect містить такі функції:

Оцінка вразливості: Acronis Cyber Protect проводить оцінку вразливості, щоб виявити потенційні слабкі місця в системах і програмах, що дозволяє компаніям завчасно усунути ці вразливості, перш ніж ними скористаються кібер-зловмисники.

Фільтрування URL-адрес. Рішення містить можливості фільтрації URL-адрес, які запобігають доступу користувачів до шкідливих веб-сайтів або веб-сайтів, які, як відомо, розповсюджують шкідливе програмне забезпечення.

Нотаріальне засвідчення файлів: Acronis Cyber Protect використовує технологію блокчейн для створення цифрових відбитків важливих файлів, гарантуючи їх цілісність і автентичність. Ця функція особливо корисна для підприємств, яким необхідно дотримуватися нормативних вимог щодо цілісності даних.

Розширений захист від загроз: Acronis Cyber Protect містить розширені функції захисту від загроз, такі як аналіз поведінки та евристичне сканування, щоб виявляти складні кібератаки та реагувати на них.

Управління ідентифікацією та доступом: рішення включає функції керування ідентифікацією та доступом, такі як багатофакторна автентифікація та контроль доступу на основі ролей, щоб гарантувати, що лише авторизовані користувачі мають доступ до конфіденційних даних і програм.

Загалом мета Acronis Cyber Protect — надати підприємствам комплексне рішення для кіберзахисту, яке охоплює всі аспекти безпеки даних і системи. Рішення призначене для спрощення управління

Acronis Cyber Protect складається з кількох компонентів, які разом забезпечують комплексне рішення з кібербезпеки та захисту даних. Ці компоненти та їхні функції:

Резервне копіювання та відновлення: компонент резервного копіювання та відновлення надає розширені можливості резервного копіювання та відновлення, що дозволяє підприємствам швидко відновлювати дані у разі аварії або втрати даних. Цей компонент також включає такі функції, як інкрементне резервне копіювання, резервне копіювання на основі знімків і детальне відновлення.

Захист від зловмисного програмного забезпечення: компонент захисту від зловмисного програмного забезпечення використовує передові алгоритми та машинне навчання для виявлення та запобігання зловмисному програмному забезпеченню, вірусам та іншим загрозам. Цей компонент містить такі функції, як виявлення на основі сигнатур, евристичний аналіз і захист у режимі реального часу.

Керування виправленнями: компонент керування виправленнями автоматизує оновлення програмного забезпечення та внесення виправлень, зменшуючи ризик кібератак, які використовують уразливості застарілого програмного забезпечення. Цей компонент містить такі функції, як розгортання виправлень, сканування виправлень і оцінка вразливостей.

Аварійне відновлення: компонент аварійного відновлення дозволяє підприємствам швидко відновлюватися після катастроф, таких як стихійні лиха, апаратні збої або кібератаки. Цей компонент включає такі функції, як планування

аварійного відновлення, перехід після відмови та відновлення після збою, а також оркестрування відновлення сайту.

Безпека та відповідність: Компонент безпеки та відповідності містить такі функції, як багатофакторна автентифікація, контроль доступу на основі ролей і звітність про відповідність, щоб гарантувати, що підприємства дотримуються нормативних вимог і підтримують надійну безпеку.

Віддалена робоча сила: компонент віддаленої робочої сили включає такі функції, як захищений віддалений доступ, інфраструктура віртуального робочого столу (VDI) і захист кінцевої точки, щоб гарантувати безпеку та продуктивність віддалених працівників.

Загалом Acronis Cyber Protect пропонує комплексне рішення, яке охоплює всі аспекти кібербезпеки та захисту даних. Рішення розроблено для спрощення керування кібербезпекою та захистом даних, що робить його більш доступним для компаній будь-якого розміру.

Рішення Acronis Cyber Protect складається з таких компонентів, які можна встановлюються в інформаційній системі організації.

Сервер керування

Сервер керування Cyber Protect складається з ряду служб, які відповідають за функції керування Acronis Cyber Protect і забезпечують веб-інтерфейс користувача. Ці служби керують агентами, групами та планами захисту; надсилають повідомлення; збирає дані, створює та зберігає звіти тощо. Зазвичай сервер керування встановлюється першим і є точкою входу в керування інфраструктурою Acronis Cyber Protect. Він фактично не бере участі в жодних операціях резервного копіювання, відновлення чи інших операціях маніпулювання даними.

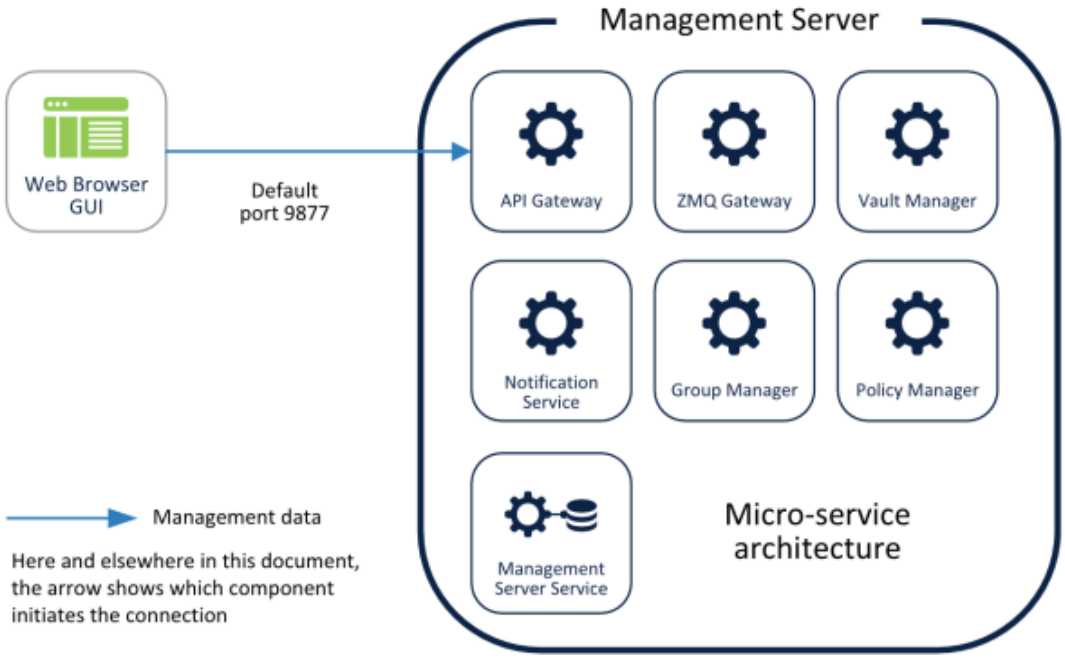

Рис. 2.1. Сервер керування

В архітектурі Acronis Cyber Protect використовуються компоненти для віддаленого встановлення. Це архів усіх інсталяційних компонентів, знайдених у повному виконуваному файлі інсталяції Acronis Cyber Protect. Його необхідно встановити, щоб мати можливість віддалено надсилати розгортання агентів із сервера керування Cyber Protect. Якщо функція віддаленого встановлення з графічного інтерфейсу продукту не потрібна, не потрібно встановлювати цей компонент, щоб заощадити місце.

Служба сканування

Виконує антишкідливе сканування резервних копій у хмарному сховищі, локальній або спільній папці. Для служби сканування потрібна база даних Microsoft SQL Server або PostgreSQL Server. При використанні вказаних баз даних на веб-консолі будуть доступні такі функції:

Плани резервного сканування.

Віджет деталей сканування резервних копій.

Корпоративний білий список.

Безпечне відновлення.

Агенти захисту

Агенти захисту Acronis також інстальовано як ряд служб, відповідальних за виконання конкретних завдань резервного копіювання, відновлення, реплікації та інших завдань із маніпулювання даними на потрібних машинах, які необхідно захищати. На рисунку 2.2. показано компонентів агентів захисту. Зазвичай вони встановлюються на кожному пристрої, який потребує захисту, а потім додаються до серверу керування Cyber Protect.

Однак агенти Acronis можуть працювати повністю незалежно і не потребують постійного зв’язку з сервером керування для виконання запланованих операцій резервного копіювання. Також можна встановити ізольований агент і повністю відмовитися від сервера керування, хоча в цьому випадку ним доведеться керувати через командний рядок.

Рис.2.2. Компоненти агентів захисту

Для захисту різних джерел даних використовуються різні типи агентів, але всі вони мають однакову архітектуру, протоколи зв’язку та переважну більшість функцій.

Нижче показано список доступних агентів.

Агент для Windows

Агент для Linux

Агент для Mac

Агент для VMware (Windows)

Агент для VMware (віртуальний пристрій)

Агент для Hyper-V

Агент для масштабованих обчислень НС3 (віртуальний пристрій)

Агент з обміну

Агент для SQL

Агент для Active Directory

Конструктор завантажувальних носіїв

Це окремий графічний інструмент, який використовується для створення двох різних типів завантажувальних носіїв Acronis: носія за замовчуванням на основі Linux і носія на основі WinPE.

Зазвичай потрібно інсталювати лише один екземпляр цього інструменту на одній із ваших машин, оскільки носій, створений на одній машині, працюватиме на інших.

Завантажувальний носій Acronis — це повністю самостійний інструмент із функціями резервного копіювання та відновлення, які надає агент. Це дозволяє відновити будь-яку систему з «пристрою», якщо у вас є сам носій і файл, який містить вашу резервну копію.

Cyber Protect Monitor

Цей компонент встановлюється разом із агентом і забезпечує базову взаємодію з агентом із панелі завдань або рядка меню вашої операційної системи. Використовуючи Cyber Protect Monitor, ви можете перевірити або зупинити запущене резервне копіювання безпосередньо з машини, на якій інстальовано агент.

Вузол зберігання

Цей компонент забезпечує кероване централізоване місце зберігання, яке агенти можуть використовувати як цільове резервне копіювання. Він потрібен для каталогізації, централізованого резервного копіювання на стрічку та дедуплікації.

Служба каталогу

Служба каталогу індексує всі ваші резервні копії, щоб забезпечити пошук і відновлення файлів у резервних копіях. Це не потрібно для відновлення файлів, тільки для пошуку.

Сервер PXE

Ця служба працює в поєднанні з Bootable Media Builder і дозволяє використовувати завантажувальний носій для завантаження через мережу.

Схему мережі, яку буде впроваджено в інформаційну систему організації Acronis Cyber Protect Appliance буде виглядати як показано на рис.2.3

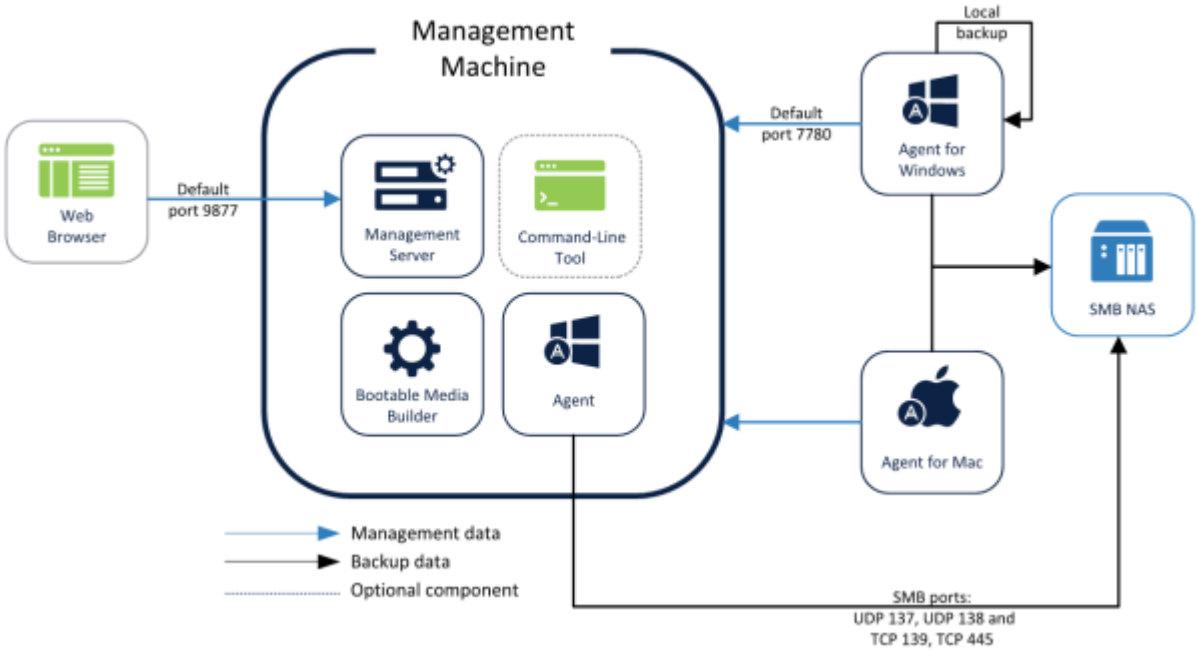

Рис.2.3. Архітектура рішення Acronis Cyber Protect Appliance

2.2. Функцональні можливості Acronis Ransomware Protection

Acronis Ransomware Protection — це пакет програм, який забезпечує безпеку інформації на вашому ПК. Він поєднує в собі дві функції, які доповнюють одна одну, щоб забезпечити вам покращений захист ваших особистих даних:

1. Активний захист Acronis

Ця служба захищає ваш комп’ютер від програм-вимагачів — зловмисного програмного забезпечення, яке блокує доступ до деяких ваших файлів або всієї системи та вимагає викуп за розблокування. На основі евристичного підходу Acronis Active Protection відстежує процеси, що виконуються на вашому комп’ютері,

використовуючи режим реального часу. Коли він виявляє сторонній процес, який намагається зашифрувати ваші файли або вставити шкідливий код у справний процес, він інформує вас про це та запитує, чи хочете ви дозволити процесу змінювати ваші файли чи заблокувати процес. Навіть якщо ваші файли були зашифровані програмою-вимагачем, ви можете відновити їх із тимчасових копій.

2. Резервне копіювання на рівні файлу в Acronis Cloud

Ви можете захистити такі файли, як документи, фотографії, музичні файли та відеофайли, від пошкодження або втрати, створивши їх резервні копії в безпечній хмарі Acronis. Оскільки файли зберігаються у віддаленому сховищі, вони захищені навіть у разі втрати, викрадення чи знищення комп’ютера. За потреби ваші дані можна повністю відновити на новому пристрої. Зміни до захищених файлів відбуваються автоматично в хмарному сховищі, щоб підтримувати резервну копію в актуальному стані. З Acronis Ransomware Protection можливо безкоштовно отримати 5 ГБ простору для хмарного сховища.

Acronis Mobile

Оскільки у вас є простір для зберігання в Acronis Cloud, можливо використовувати його для захисту не лише даних на комп’ютері, але й мобільних даних. Acronis Mobile — це безкоштовна програма, яка дозволяє створювати резервні копії ваших даних у Acronis Cloud, а потім відновлювати їх у разі втрати чи пошкодження на тому самому чи новому мобільному пристрої. Додаток підтримує смартфони та планшети під управлінням операційних систем iOS або Android. Додаткову інформацію див. у Acronis Mobile (стор. 15).

За допомогою настільної програми Acronis True Image або програми Acronis True Image NAS можливо створити резервну копію своїх мобільних даних на комп’ютері або пристрої NAS.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАСТОСУВАННЯ МЕТОДІВ ТА ЗАСОБІВ ПРОТИДІЇ ПРОГРАМАМ-ВИМАГАЧАМ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ОРГАНІЗАЦІЇ НА БАЗІ ACRONIS

3.1 Розробка рекомендацій щодо налаштування Acronis Ransomware Protection

Системні вимоги Acronis Ransomware Protection потребує такого обладнання:

1. Процесор Pentium 1 ГГц
2. 1 ГБ оперативної пам'яті
3. 1,5 ГБ вільного місця на жорсткому диску
4. Роздільна здатність екрану 1024 x 768
5. Миша або інший вказівний пристрій (рекомендується)

Інші вимоги: підключення до Інтернету.

Для запуску Acronis Ransomware Protection потрібні права адміністратора:

- Операційні системи:
- Windows 7 SP1 (всі версії)
- Windows 8 (всі версії)
- Windows 8.1 (всі версії)
- Windows 10 (всі версії)

Інсталяція Acronis Захист від програм-вимагачів

Щоб інсталювати Acronis Ransomware Protection необхідно виконати наступні кроки:

1. Запустіть інсталяційний файл. Перед початком процесу інсталяції Acronis Ransomware Protection перевірить наявність нової збірки на веб-сайті. Якщо така є, буде запропоновано інсталювати нову версію.
2. Натисніть "Встановити".

Acronis Ransomware Protection буде інстальовано на системний розділ (зазвичай C:).

3. У вікні, що відкриється, увійдіть до свого облікового запису Acronis. Розглянемо більш докладніше відомості щодо облікового запису Acronis

Щоб Acronis Ransomware Protection працював, потрібно ввійти в систему під своїм обліковим записом Acronis. Коли ви вийдете з системи, Acronis Active Protection продовжить працювати, але програма припинить оновлювати хмарну резервну копію.

Кроки створення облікового запису Acronis.

Після першого запуску Acronis Ransomware Protection ви побачите форму реєстрації.

Якщо у вас ще немає облікового запису Acronis:

1. Заповніть реєстраційну форму.

Щоб зберегти ваші особисті дані в безпеці, оберіть надійний пароль, захистіть його від потрапляння в чужі руки і час від часу змінюйте його.

2. Натисніть "Створити обліковий запис".

3. На вказану вами адресу буде надіслано електронний лист. Відкрийте цей лист і підтвердіть своє бажання створити обліковий запис.

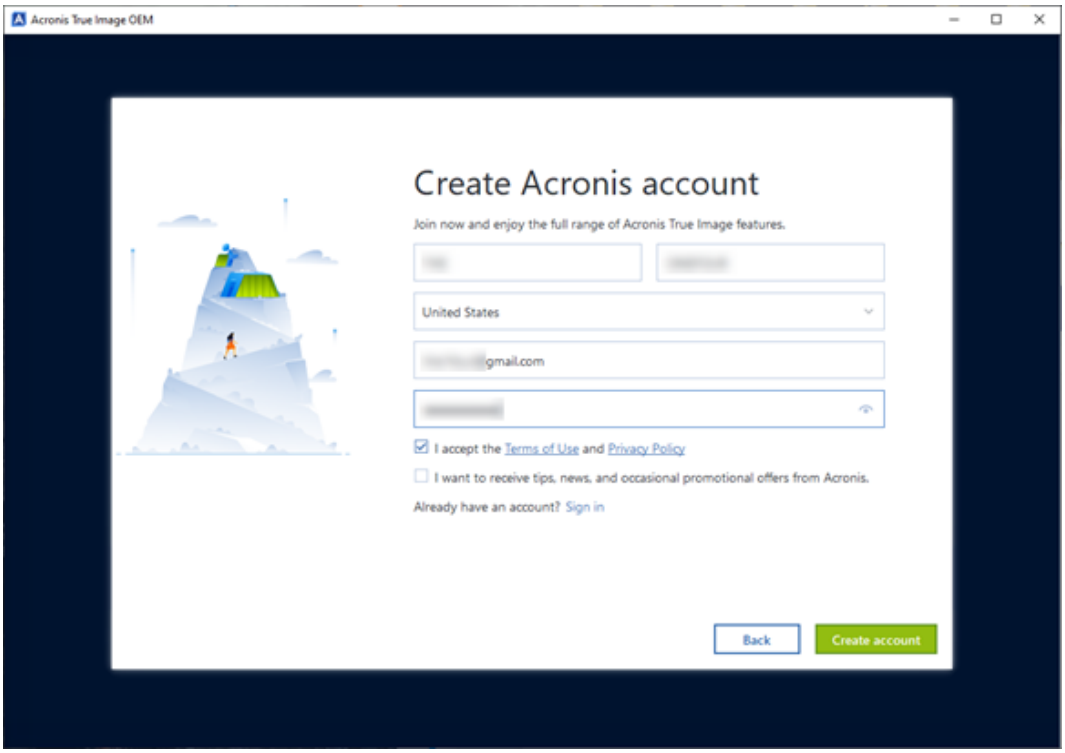

Рис.3.1. Створення облікового запису

Як увійти в систему

Увійдіть до свого облікового запису Acronis:

1. Щоб переключитися з форми реєстрації на форму входу, натисніть Я вже маю обліковий запис.

2. Введіть свою реєстраційну електронну адресу та пароль, а потім натисніть "Увійти".

Як вийти з системи

Щоб вийти з облікового запису Acronis:

1. Запустіть Acronis Захист від програм-вимагачів.

2. Клацніть на іконку облікового запису, а потім натисніть "Вийти".

1.2. Рекомендації щодо активного захисту Acronis.

Acronis Active Protection — це функція Acronis True Image, програмного забезпечення для резервного копіювання та відновлення. Він призначений для захисту

вашого комп’ютера від атак програм-вимагачів, відстежуючи вашу систему на наявність підозрілої поведінки та зупиняючи загрози, перш ніж вони завдадуть будь-якої шкоди. Ось як працює Acronis Active Protection:

Моніторинг у режимі реального часу: Acronis Active Protection постійно відстежує ваш комп’ютер на предмет будь-якої підозрілої активності, включаючи зміни файлів або створення нових файлів, які можуть вказувати на атаку програм-вимагачів.

Аналіз поведінки: Acronis Active Protection використовує алгоритми машинного навчання для аналізу поведінки файлів і програм на вашому комп’ютері. Він шукає закономірності та аномалії, які можуть свідчити про атаку програм-вимагачів.

Автоматична відповідь: якщо Acronis Active Protection виявляє атаку програм-вимагачів, вона автоматично зупиняє атаку та скасовує будь-які зміни, внесені до ваших файлів. Це гарантує захист ваших даних і можливість швидкого відновлення після атаки.

Білий список: Acronis Active Protection підтримує список надійних програм і файлів на вашому комп’ютері. Це лише дозволяє цим програмам і файлам вносити зміни у вашу систему, запобігаючи завданню шкоди невідомим або неавторизованим програмам.

Загалом Acronis Active Protection — це потужний інструмент, який може допомогти захистити ваш комп’ютер від атак програм-вимагачів. Відстежуючи вашу систему в режимі реального часу та використовуючи передові алгоритми машинного навчання, вона може швидко виявляти загрози та реагувати на них, перш ніж вони завдадуть будь-якої шкоди.

Вимагачі - це шкідливе програмне забезпечення, яке блокує доступ до деяких файлів або всієї системи і вимагає викуп за розблокування. Програма показує вікно з повідомленням про те, що ваші файли заблоковані і що ви повинні терміново заплатити, інакше ви більше не зможете отримати до них доступ. Повідомлення також

може бути замасковане під офіційну заяву органів влади, наприклад, поліції. Мета повідомлення - налякати користувача і змусити його заплатити, не звертаючись за допомогою до IT-спеціаліста або органів влади. Крім того, немає жодних гарантій, що ви відновите контроль над своїми даними після сплати викупу.

Ваш комп'ютер може бути атакований вірусом-вимагачем, коли ви відвідуєте небезпечні веб- сайти, відкриваєте повідомлення електронної пошти від невідомих людей або переходите за підозрілими посиланнями в соціальних мережах чи миттєвих повідомленнях.

Програми-вимагачі можуть заблокувати ваш доступ:

– Весь комп'ютер

Ви не зможете користуватися Windows або робити що-небудь на своєму комп'ютері. Як правило, в цьому випадку програми-вимагачі не шифрують ваші дані.

– Конкретні файли

Зазвичай це ваші особисті дані, такі як документи, фотографії та відео. Програми-здирники шифрують файли і вимагають гроші за ключ шифрування, який є єдиним способом розшифрувати ваші файли.

– Додатки

Програми-здирники блокують деякі ваші програми, щоб ви не могли їх запустити. Найчастіше воно атакує ваш веб-браузер.

Для захисту комп'ютера від програм-вимагачів Acronis Ransomware Protection використовує технологію Acronis Active Protection. Заснована на евристичному підході, ця технологія відстежує процеси, запущені на вашому комп'ютері, в режимі реального часу. Коли вона виявляє сторонній процес, який намагається зашифрувати ваші файли або впровадити шкідливий код у здоровий процес, вона інформує вас про це і запитує, чи хочете ви дозволити процесу модифікувати ваші файли або заблокувати його.

Евристичний підхід широко використовується в сучасному антивірусному програмному забезпеченні як ефективний спосіб захисту даних від шкідливих

програм. На відміну від сигнатурного підходу, який може виявити лише один зразок, евристичний підхід виявляє сімейства шкідливих програм, які включають зразки зі схожою поведінкою. Ще однією перевагою цього підходу є здатність виявляти нові види шкідливих програм, які ще не мають сигнатур.

Acronis Active Protection використовує поведінкову евристику та аналізує ланцюжки дій, виконаних програмою, які потім порівнюються з ланцюжком подій у базі даних шаблонів шкідливої поведінки. Оскільки цей метод не є точним, він допускає так звані помилкові спрацьовування, коли програма, якій ви довіряєте, виявляється шкідливим програмним забезпеченням. Щоб уникнути таких ситуацій, Acronis Active Protection запитує вас, чи довіряєте ви виявленому процесу. Коли той самий процес буде виявлено вдруге, ви можете додати його до списку дозволів і встановити для нього дію за замовчуванням, позначивши його як довірений або заблокований. Якщо ви цього не зробите, ви зможете додати цей процес до чорного списку. У цьому випадку цей процес буде заблоковано щоразу, коли він намагатиметься змінити ваші файли.

Щоб зібрати якомога більше різних шаблонів, Acronis Active Protection використовує машинне навчання. Ця технологія базується на математичній обробці великих обсягів даних, отриманих за допомогою телеметрії. Це підхід, що самонавчається, адже чим більше даних обробляється, тим точніше можна визначити, чи є той чи інший процес програмним забезпеченням-вимагачем, чи ні.

Коли служба Acronis Active Protection увімкнена, вона відстежує процеси, запущені на вашому комп'ютері, у режимі реального часу. Виявивши сторонній процес, який намагається зашифрувати ваші файли, служба повідомить вас про це і запитає, чи хочете ви дозволити цьому процесу змінити ваші файли або заблокувати його.

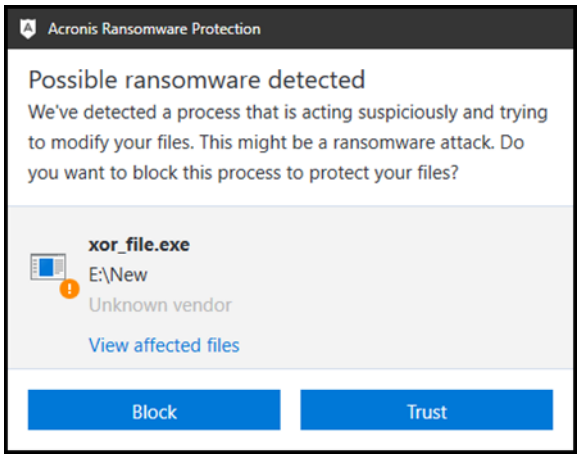

Рис.3.2. Виявлення стороннього процесу Acronis Ransomware Protection

Перш ніж прийняти рішення, ви можете переглянути список файлів, які буде змінено.

Щоб дозволити процесу змінювати файли, натисніть *Довіряти*. Якщо ви не впевнені, що процес є безпечним і законним, рекомендуємо натиснути *Блокувати*. У будь-якому разі, під час наступного запуску процесу Acronis Ransomware Protection запитає вас про це знову. Щоб надати процесу постійний дозвіл або блокувати його щоразу, коли він намагатиметься змінити ваші файли, встановіть прапорець *Запам'ятати мій вибір для цього процесу*, а потім натисніть *Блокувати* або *Довіряти*. Процес буде додано до списку дозволів. Ви можете керувати цим списком у Налаштуваннях.

Після блокування процесу рекомендуємо перевірити, чи не були ваші файли зашифровані або пошкоджені в будь-який спосіб. Якщо це так, натисніть *Відновити* змінені файли. Acronis

Ransomware Protection виконає пошук останніх версій файлів і відновить файли з тимчасових копій, які було попередньо створено під час перевірки процесу.

Щоб зробити цю дію типовою, встановіть прапорець *Завжди відновлювати файли після блокування процесу*.

Коли служба Acronis Active Protection увімкнена, вона відстежує процеси, запущені на вашому комп'ютері, у режимі реального часу. Виявивши сторонній

процес, який намагається зашифрувати ваші файли, служба повідомить вас про це і запитає, чи хочете ви дозволити йому змінити ваші файли або заблокувати процес.

Ви можете налаштувати параметри Acronis Active Protection і керувати процесом захисту з кількох місць:

– Розділ Acronis Active Protection

– Область сповіщень панелі завдань Windows

Розділ Acronis Active Protection містить статистику процесу захисту та дає змогу налаштувати список дозволів Acronis Active Protection.

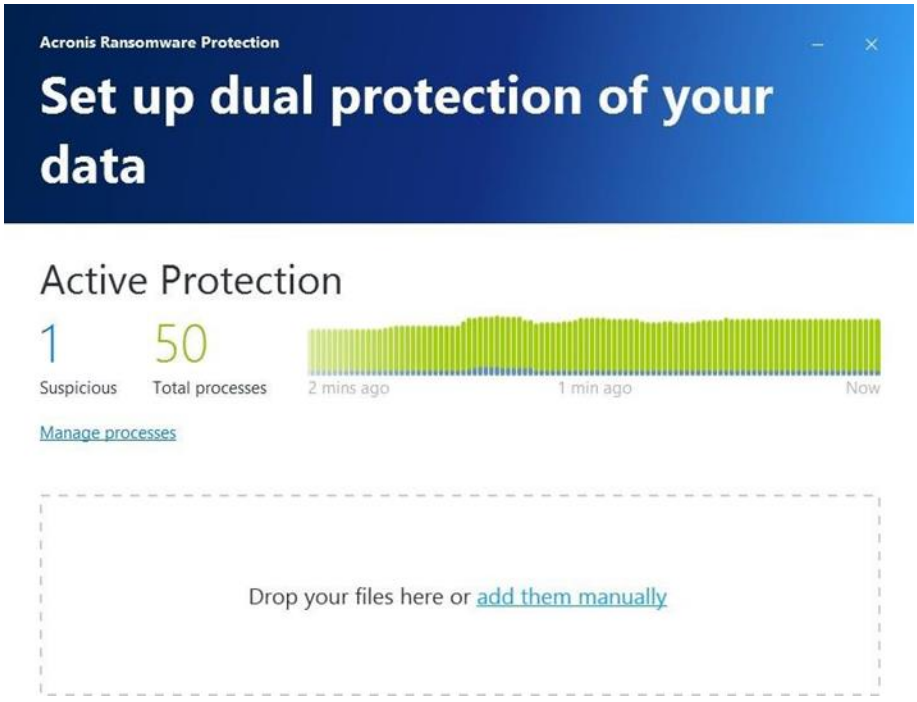

Рис.3.3. Статистика процесу захисту

Цей розділ надає такі можливості:

– Моніторинг в режимі реального часу:

- Поточна кількість процесів, що аналізуються.
- Поточна кількість підозрілих процесів (с. 20).
- Керування списком дозволів.

Цей список дозволяє вам довіряти або блокувати додатки.

Область сповіщень панелі завдань Windows

Клацнувши правою кнопкою миші на піктограмі області сповіщень, ви відкриєте наступні пункти меню:

– Вимкнути активний захист (Turn on Active Protection) - натисніть, щоб увімкнути або вимкнути захист від програм-вимагачів.

– Відкрити - натисніть, щоб відкрити головне вікно програми.

3.3. Розробка рекомендацій резервного копіювання файлів і папок

Acronis Ransomware Protection дає змогу створювати резервні копії файлів, зокрема документів, фотографій, музичних і відеофайлів, у хмарному сховищі Acronis Cloud. У разі їх пошкодження або втрати на вашому комп'ютері, їх можна легко відновити з хмарного сховища.

Для резервного копіювання файлів і папок:

1. Запустіть Acronis Ransomware Protection.

2. Відкрийте крок конфігурації резервної копії підручника або головне вікно програми.

3. Щоб вказати файли і папки, які потрібно створити резервну копію, виконайте одну з наведених нижче дій:

– У Провіднику або іншому файловому менеджері виберіть файли та папки, а потім перетягніть їх у вікно Захист від програм-вимагачів Acronis.

– Натисніть Додати їх вручну, а потім перейдіть до папок на ваших дисках. Резервне копіювання розпочнеться автоматично.

Перше резервне копіювання може зайняти значну кількість часу. Подальші процеси резервного копіювання, ймовірно, будуть набагато швидшими, оскільки через Інтернет передаватимуться лише зміни у файлах. Acronis Ransomware Protection перевіряє зміни даних кожні 15 хвилин і автоматично завантажує їх до Acronis Cloud.

Щоб змінити налаштування резервного копіювання, клацніть значок шестерні в головному вікні програми.

Оскільки Acronis Ransomware Protection постійно відстежує резервні копії даних і завантажує зміни в Acronis Cloud, резервне копіювання може досить швидко зайняти місце в сховищі. Щоб зменшити кількість версій файлів і оптимізувати використання хмарного простору, Acronis Ransomware Protection зберігає лише наступні версії файлів:

- Всі версії за останню годину.
- Перші версії кожної години за останні 24 години.
- Перша версія кожного дня за останній тиждень.
- Перша версія щотижня протягом останнього місяця.
- Перша версія кожного місяця.

Всі інші версії автоматично видаляються. Правила зберігання встановлені заздалегідь і не можуть бути змінені.

Оскільки доступний простір у хмарному сховищі Acronis обмежений, потрібно керувати ним, видаляючи застарілі дані або дані, які вам більше не потрібні. Очищення можна виконати різними способами:

Видалення всієї резервної копії:

1. Перейдіть на сайт https://www.acronis.com/my/online-backup/webrestore/, а потім увійдіть до свого облікового запису Acronis.
2. На вкладці Стан сховища вкажіть резервну копію, яку потрібно видалити, клацніть значок шестерні, а потім натисніть Видалити.

Видалення певних файлів і папок

Ви також можете керувати Acronis Cloud, видаляючи окремі файли та папки.

1. Перейдіть на сайт https://www.acronis.com/my/online-backup/webrestore/, а потім увійдіть до свого облікового запису Acronis.
2. Виберіть файли і папки, які ви хочете видалити, а потім натисніть Видалити.

3.4. Розробка загальних рекомендацій потидії програмам-вимагачам

Загальна порада чітка: ніколи не платіть викуп . Ось чому:

Ви не можете бути впевнені, що це спрацює.

Хоча кіберзлочинці можуть пообіцяти повернути ваші дані, немає гарантії, що вони справді виконають це. Неможливо знати, що станеться, доки ви не заплатите — і ви можете виявити, що ваші дані все ще заблоковані. У будь-який спосіб неможливо навіть розшифрувати ваші дані. Деякі варіанти сімейства програм-вимагачів Petya незворотні.

Ви заохочуєте майбутні атаки.

Коли жертви платять викуп, це «доводить» зловмиснику, що програми-вимагачі працюють. Розробники програм-вимагачів і хакерські групи можуть використовувати свої прибутки для фінансування розробки кращого програмного забезпечення та більш руйнівних методів атак.

Деякі атаки програм-вимагачів можуть бути буквально питанням життя та смерті . Зловмисники використовують цю терміновість, коли націлюються на лікарні, комунальні служби та подібні установи. Не завжди можливо витримати атаку та дочекатися розшифрування програми-вимагача.

З цієї причини, хоча СБУ закликає жертв не платити , воно також співчуває тим, хто це зробив. Багато компаній не бажають розкривати інформацію про кібератаки, але це може допомогти владі в боротьбі з програмами-вимагачами та іншими кіберзлочинами.

Атаки програм-вимагачів становлять серйозну загрозу вашим даним, і їх важко відновити, якщо їх не вжити належним чином. Ось кілька рекомендацій щодо протидії атакам програм-вимагачів:

Резервне копіювання даних. Одним із найважливіших кроків, які ви можете зробити для захисту від атак програм-вимагачів, є регулярне резервне копіювання даних. Таким чином, якщо ваші файли зашифровані або іншим чином скомпрометовані, ви зможете відновити їх із резервної копії замість того, щоб платити викуп.

Використовуйте програмне забезпечення безпеки: встановлюйте та регулярно оновлюйте програмне забезпечення безпеки, включаючи антивірусні та антишкідливі програми. Це може допомогти запобігти зараженню вашого комп'ютера програмами-вимагачами.

Оновлюйте програмне забезпечення: оновлюйте операційну систему та інше програмне забезпечення за допомогою останніх виправлень безпеки та оновлень. Багато атак програм-вимагачів використовують уразливості застарілого програмного забезпечення.

Будьте обережні з вкладеннями електронної пошти: будьте обережні, відкриваючи вкладення електронної пошти або натискаючи посилання в електронних листах, особливо якщо вони з невідомих або підозрілих джерел. Програми-вимагачі часто поширюються через фішингові електронні листи.

Використовуйте надійні паролі. Використовуйте надійні паролі та двофакторну автентифікацію, щоб захистити свої онлайн-акаунти від злому. Багато атак програм-вимагачів можуть поширюватися через зламані облікові записи.

Навчіть себе та інших: ознайомте себе та інших у своїй організації з програмами-вимагачами та як їх уникнути. Це може включати навчання безпечній електронній пошті, способи виявлення спроб фішингу та дії у випадку атаки програм-вимагачів.

Виконуючи ці кроки, ви можете захистити свої дані та мінімізувати наслідки атаки програм-вимагачів. Важливо бути проактивним і бути пильним, щоб запобігти цим типам загроз і реагувати на них.

ВИСНОВКИ

В результаті виконання бакалаврської роботи було отримано наступні результати:

Проведено аналіз щодо атак програм-вимагачів для організацій. Організації будь-якого розміру та галузі вразливі до атак програм-вимагачів. Для організацій важливо проявляти активність у своєму підході до кібербезпеки, зокрема регулярно створювати резервні копії своїх даних, оновлювати свої системи, навчати працівників безпечним практикам і мати чіткі політики та процедури безпеки.

На основі аналізу було визначено що програми-вимагачі створюють значні ризики для організацій будь-якого розміру та галузей. Організаціям важливо вживати профілактичних заходів, щоб захистити себе від атак програм-вимагачів, зокрема регулярно створювати резервні копії даних, оновлювати програмне забезпечення та системи, навчати працівників безпечним методам, а також мати чіткі політики та процедури безпеки. Здійснюючи ці кроки, організації можуть допомогти знизити ризики атак програм-вимагачів і мінімізувати вплив будь-яких атак, які трапляються.

На основі отриманих даних для подальшого дослідження шляхів протидії програмам-вимагачам будо розглянуто Acronis Ransomware Protection, яке працює на базі Acronis Cyber Protect.

Acronis Cyber Protect пропонує комплексне рішення, яке охоплює всі аспекти кібербезпеки та захисту даних, для якого визначено архітектуру та основні компоненти.

Acronis Ransomware Protection — це пакет програм, який забезпечує безпеку інформації на вашому ПК. Він поєднує в собі дві функції, які доповнюють одна одну, щоб забезпечити покращений захист ваших особистих даних.

В результаті дослідження розроблено рекомендації щодо протидій прогамам вимагачам. І як основна порада - ніколи не платіть викуп. Кіберзлочинці можуть

пообіцяти повернути ваші дані, немає гарантії, що вони справді виконають це. Використання запропонованого рішення дозволить упередити атаки такого типу.

ПЕРЕЛІК ПОСИЛАНЬ

1 Вплив програм вимагачів [Електронний ресурс] Режим доступу: https://www.acronis.com/en-us/solutions/ransomware-protection/.

2 Рейтинг інтернет загроз [Електронний ресурс] Режим доступу: https://www.unian.ua/techno/communications/reyting-internet-zagroz-ukrajinciv-naychastishe-atakuvali-programi-vimagachi-ta-zagrozi-dlya-android-12137310.html.

3 Avast - biggest ransomware attacks [Електронний ресурс] Режим доступу: https://www.avast.com/c-biggest-ransomware-attacks .

4 Вектор атак програм-вимагачів [Електронний ресурс] Режим доступу: https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound.

5 Acronis Cyber Protect. Посібник. - 2022. 101с.

6 Acronis Ransomware Protection. Guide. – 2017. 27с.

7 Загрози витоку [Електронний ресурс] Режим доступу: https://www.kingston.com/en/support/technical/acronis-download.

8 Огляд рішень [Електронний ресурс] https://sovety.pp.ua/index.php/ua/statti/windows/sistema/2776-boremosya-iz-programami-vimagachami-vidalennya-program-vimagachiv-ta-rozshifruvannya-zashifrovanikh-fajliv.

КОПІЇ ДЕМОНСТРАЦІЙНИХ АРКУШІВ