ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЯ ПРОТИДІЇ СПАМУ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ОРГАНІЗАЦІЇ НА БАЗІ CYREN EMAIL SECURITY ENGINE»

Виконав: студент 6 курсу, групи БСДМ-62
Спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Бурлін М. О.
(прізвище та ініціали)
Керівник Гайдур Г.І.
(прізвище та ініціали)
Рецензент _____
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.

КИЇВ – 2022

РЕФЕРАТ

Текстова частина магістерської роботи: 75 сторінки, 16 рисунків, 25 джерел.

Об'єкт дослідження – процес захисту корпоративної пошти користувачів від спам атак.

Предмет дослідження – технологія управління захистом поштових скринь користувачів з використанням рішення Cyren Email Security Engine.

Мета роботи – дослідити управління захистом поштових скринь корпоративних користувачів з використанням рішення Cyren Email Security Engine.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, розширений аналіз та діагностика завдяки рішенню Cyren Email Security Engine, Symantec BrightMail, сервісу SpamAssassin та ін.

В роботі проведено аналіз проблеми захисту корпоративної пошти та користувачів від спаму та небажаних листів.

Досліджено методи та засоби управління захистом поштових скринь корпоративних клієнтів на прикладі рішення Cyren Email Security Engine. Визначено призначення, основні функції та склад програмного комплексу Cyren Email Security Engine.

На основі досліджень проведених в роботі розроблено варіант управління захистом корпоративних поштових скринь та клієнтів інформаційної системи та рекомендації щодо застосування технології управління їх захистом на підприємстві.

Галузь використання – кібербезпека.

БЕЗПЕКА ПОШТОВИХ СКРИНЬ, ІНФОРМАЦІЙНА БЕЗПЕКА, ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ, ЗАХИСТ ІНФОРМАЦІЇ, РЕВЕРС-ІНЖИНИРИНГ, ХМАРНІ ТЕХНОЛОГІЇ, СПАМ, ПЕНТЕСТ, INFORMATION SECURITY, INFORMATION TECHNOLOGIES, ANTISPAM EMAIL SOLUTIONS, REVERSE ENGINEERING, PROTECTION OF INFORMATION.

ABSTRACT

Master's thesis: 75 pages, 16 figures, 25 sources.

Object of research – the process of protecting users' corporate mail from spam attacks.

Subject of research – the technology of managing the protection of users' mailboxes using the Cyren Email Security Engine solution.

The aim of research – investigate the management of the protection of users' mailboxes using the Cyren Email Security Engine solution.

Research methods – study of the literature on this topic, analysis of operational documentation, international standards and their comparison, advanced analysis and diagnostics thanks to Cyren Email Security Engine, Symantec BrightMail, SpamAssassin service, etc.

The paper analyzes the problem of protecting corporate mail and users from spam and unwanted letters.

The methods and means of managing the protection of mailboxes of corporate clients were studied using the Cyren Email Security Engine solution as an example. The purpose, main functions and composition of the Cyren Email Security Engine software complex are defined.

On the basis of research carried out in the work, a variant of managing the protection of corporate mailboxes and clients of the information system and recommendations for the application of technology for managing their protection at the enterprise have been developed.

The field of use is cybersecurity.

MAILBOX SECURITY, INFORMATION SECURITY, INFORMATION TECHNOLOGIES, INFORMATION PROTECTION, REVERSE ENGINEERING, CLOUD TECHNOLOGIES, SPAM, PENTEST, INFORMATION SECURITY, INFORMATION TECHNOLOGIES, ANTISPAM EMAIL SOLUTIONS, REVERSE ENGINEERING, PROTECTION OF INFORMATION.

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – Операційна система

ПЗ – Програмне забезпечення

API – Application Programming Interface

SaaS – Програма як послуга (Software as a service)

НД ТЗІ – нормативний документ технічного захисту інформації

ПБ – політика безпеки

CA – Certificate Authority

PKI – Public Key Infrastructure

MSP – Managed service provider

ШІ – штучний інтелект

КІС – Корпоративна інформаційна система

DNS – Domain name server

SBL – Spamhaus block list

AUP – Acceptable use policy

RBL – Realtime Blackhole List

RFC – Request for Comments

PGP – Pretty Good Privacy

GPG – GNU Privacy Guard

SPF – Sender Policy Framework

FP – False Positive

ВСТУП

Актуальність дослідження. У наш час використання пошти стало невід'ємною частиною роботи більшості організацій і корпорацій. Багато з них все частіше звертаються за допомогою до перевірених вендорів з постачання готових рішень у галузі безпеки від спаму та фішингу. Завдяки цьому компанії можуть не мати власний штат спеціалістів з кібербезпеки, а встановлення і управління може здійснити і звичайний користувач. Комп'ютерні адміністратори можуть самі надавати необхідний доступ на перегляд листів від різних груп відправників, або ж блокувати їх. Щоб адміністратори могли контролювати свої комп'ютерні системи, вони мають почати використовувати програмне забезпечення, яке допомагає контролювати всі облікові записи користувачів в одному місці.

Вищенаведені аргументи актуалізують тему даної магістерської роботи, зміст якої становлять дослідження технології управління захистом поштових скринь корпоративних користувачів з використанням рішення Cyren Email Security Engine.

Об'єкт дослідження – процес захисту корпоративної пошти користувачів від спам атак.

Предмет дослідження – технологія управління захистом поштових скринь користувачів з використанням рішення Cyren Email Security Engine.

Мета роботи – дослідити управління захистом поштових скринь корпоративних користувачів з використанням рішення Cyren Email Security Engine.

Наукові завдання:

дослідити сутність проблеми кібербезпеки поштових скринь в інформаційній системі організацій;

проаналізувати існуючі методи та засоби протидії спаму в інформаційцній системі організації;

проаналізувати основні функції Cyren Email Security Engine.

розробити рекомедації щодо застосування технології протиції спаму користувачів корпоративної інформаційної системи та фахівців з кібербезпеки на основі Cyren Email Security Engine.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, розширений аналіз та діагностика завдяки рішенню Cyren Email Security Engine, Symantec BrightMail, сервісу SpamAssassin та ін.

Практичне значення одержаних результатів полягає у розробці рекомендацій технології захисту кінцевих користувачів коропоративної мережі від спаму.

Апробація результатів магістерської роботи було оприлюднено на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 27 жовтня 2022 року в Державному університеті телекомунікацій, м. Київ, в журналі «Сучасний захист інформації» №1(49), 2022 р., в статті «Методики фішингу в мобільних системах».

1 АНАЛІЗ ПРОБЛЕМ СПАМУ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ОРГАНІЗАЦІЇ

1.1 Аналіз загрози спаму на корпоративні поштові скрині та кінцевих користувачів

Спам – це будь-яке небажане цифрове повідомлення, яке масово розсилається. Найчастіше спам надсилається електронною поштою, але він також може поширюватися через текстові повідомлення, телефонні дзвінки чи соціальні мережі.

Види спаму

Спамери використовують багато форм зв’язку для масової розсилки своїх небажаних повідомлень. Деякі з них є маркетинговими повідомленнями про продаж небажаних товарів. Інші типи спаму можуть поширювати зловмисне програмне забезпечення, обманом змусити вас розкрити особисту інформацію або налякати, щоб ви подумали, що вам потрібно заплатити, щоб уникнути проблем.

Спам-фільтри електронної пошти вловлюють багато таких типів повідомлень, а оператори телефонного зв’язку часто попереджають вас про «ризик спаму» від невідомих абонентів. Через електронну пошту, текстове повідомлення, телефон або соціальні мережі, деякі спам-повідомлення все-таки проходять, і ви хочете розпізнати їх і уникнути цих загроз[1].

Рис. 1.1. Інфографіка поширення спаму за типами файлів

Фішингові листи

Фішингові електронні листи – це тип спаму, який кіберзлочинці надсилають багатьом людям, змушуючи жертв надати конфіденційну інформацію, як дані для входу на веб-сайт або дані кредитної картки[2].

Brett Jackson, директор Cyren, каже про фішингові електронні листи наступне: «Фішинг — це найпростіший вид кібератаки, який водночас є найнебезпечнішим і найефективнішим. Це тому, що він атакує найбільш вразливий і потужний комп'ютер на планеті: людський розум».

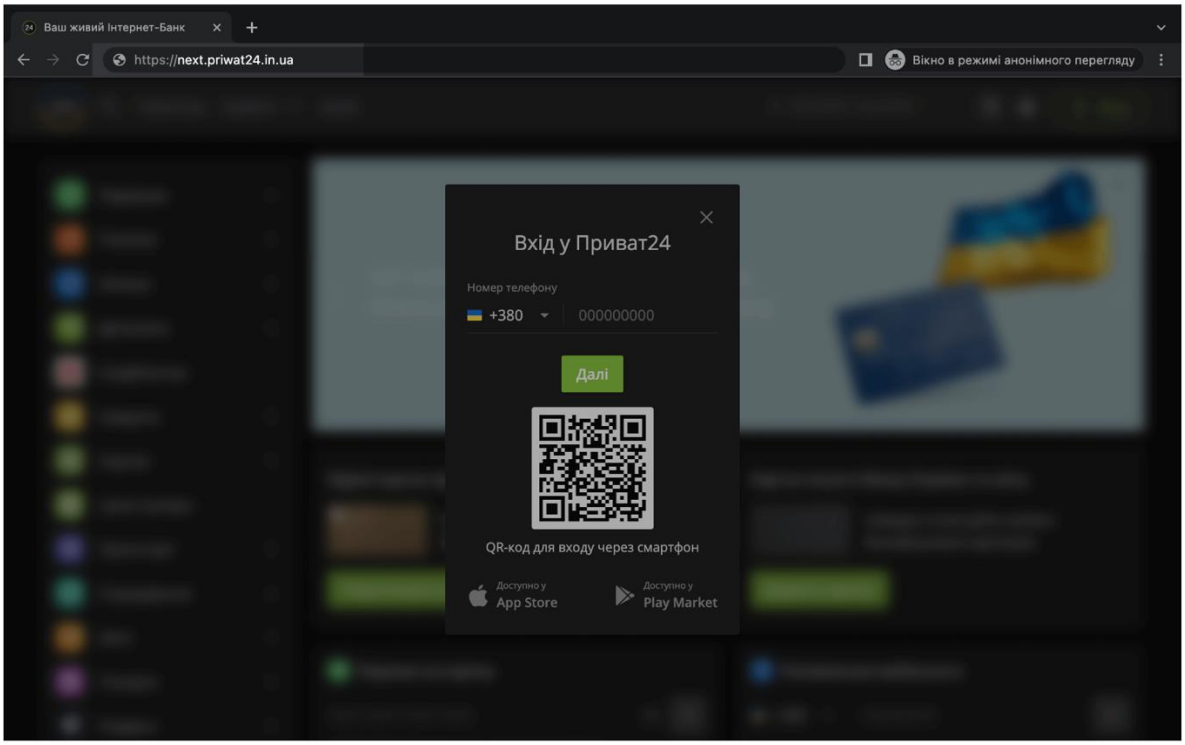

Рис. 1.2. Приклад фішингового сайту

Підробка електронної пошти

Підроблені електронні листи імітують або підробляють електронний лист від законного відправника та просять вас вжити певних дій. Добре виконані підробки містять знайомий бренд і вміст, часто від великої відомої компанії, такої як PayPal або Apple. До поширених спам-повідомлень електронної пошти відносяться:

- вимога про оплату неоплаченого рахунку;
- запит на скидання пароля або підтвердження облікового запису;
- перевірка покупок, які ви не робили;
- запит на оновлену платіжну інформацію;

- шахрайство служби технічної підтримки;

У шахрайстві технічної підтримки спам-повідомлення вказує на те, що у вас є технічна проблема, і вам слід зв'язатися зі службою технічної підтримки, зателефонувавши за номером телефону або натиснувши посилання в повідомленні. Подібно до спуфінгу електронної пошти, ці типи спаму часто повідомляють, що вони надходять від великої технологічної компанії, як Microsoft, або компанії з кібербезпеки, як Cyren.

Якщо ви вважаєте, що у вас є технічна проблема або зловмисне програмне забезпечення на вашому комп'ютері, планшеті чи смартфоні, вам слід завжди відвідувати офіційний веб-сайт компанії, якій ви хочете зателефонувати для технічної підтримки, щоб знайти офіційну контактну інформацію[3]. Віддалена технічна підтримка часто передбачає віддалений доступ до вашого комп'ютера, щоб допомогти вам, і ви не хочете випадково надати цей доступ шахраю з технічної підтримки.

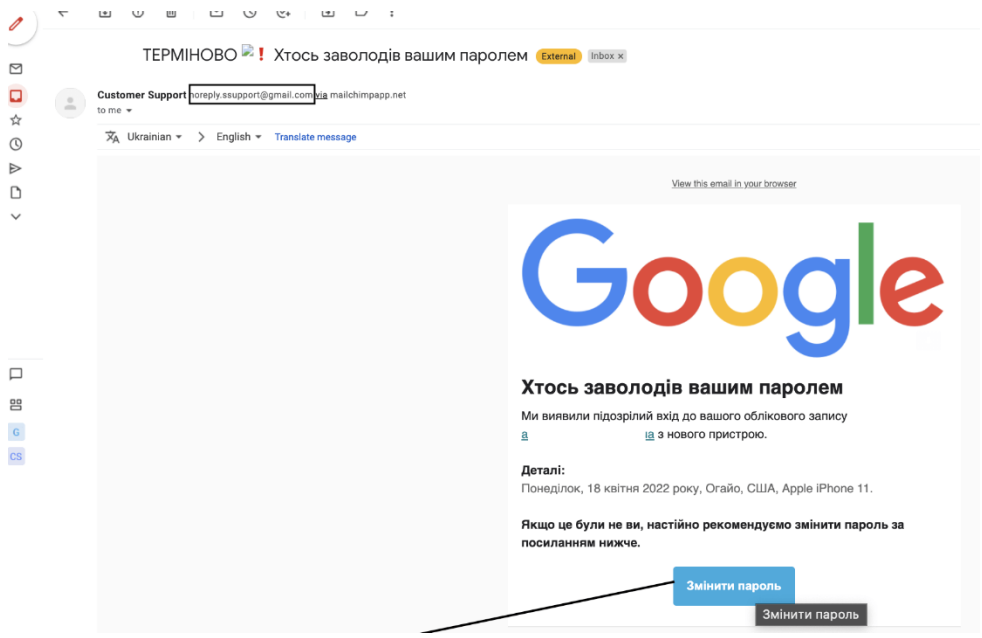

Рис.1.3. Приклад листа, відправлений з підробленої пошти

Шахрайство з поточними подіями

Гарячі теми в новинах можна використовувати в спам-повідомленнях, щоб привернути вашу увагу. У 2020 році, коли світ зіткнувся з пандемією Covid-19 і спостерігалося збільшення кількості робочих місць з дому, деякі шахраї розсилали

спам-повідомлення, обіцяючи віддалену роботу з оплатою в біткоїнах[4]. У тому ж році ще одна популярна тема спаму була пов’язана з пропозицією фінансової допомоги малому бізнесу, але шахраї зрештою попросили надати реквізити банківського рахунку. Заголовки новин можуть бути помітними, але остерігайтеся їх щодо потенційних спам-повідомлень.

Шахрайство з попередньою оплатою

Цей тип спаму, ймовірно, знайомий усім, хто користується електронною поштою з 90-х чи 2000-х років. Цей тип спаму, який іноді називають електронними листами «нігерійського принца», оскільки він був передбачуваним відправником повідомлень протягом багатьох років, обіцяє фінансову винагороду, якщо ви спочатку надасте аванс готівкою[5]. Відправник зазвичай вказує, що цей готівковий аванс є певною комісією за обробку або заставою для розблокування більшої суми, але після оплати вони зникають. Щоб зробити це більш особистим, подібний тип шахрайства передбачає, що відправник прикидається членом сім’ї, який потрапив у біду та потребує грошей, але якщо ви платите, результат, на жаль, той самий.

Шкідливий спам

Скорочення від «спам зловмисного програмного забезпечення» або «зловмисний спам», malspam – це спам-повідомлення, яке доставляє зловмисне програмне забезпечення на ваш пристрій. Нічого не підозрюючи читачі, які натискають посилання або відкривають вкладення електронної пошти, отримують певний тип зловмисного програмного забезпечення, включаючи програми-вимагачі, трояни, боти, викрадачі інформації, криптомайнери, шпигунські програми та кейлоггери[6]. Звичайним способом доставки є додавання шкідливих сценаріїв до вкладення знайомого типу, як-от документ Word, PDF-файл або презентація PowerPoint. Після відкриття вкладеного файлу сценарії запускаються та отримують шкідливе програмне забезпечення.

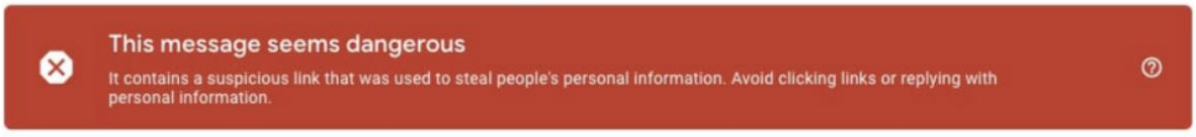

Рис. 1.4. Приклад банеру при отриманні шкідливого листа

Спам-дзвінки та спам-повідомлення

Ви коли-небудь отримували автоматизований дзвінок? Це називається спамом. Текстове повідомлення від невідомого відправника із закликом натиснути невідоме посилання? Це називається спамом текстових повідомлень або «смішингом», поєднанням SMS і фішингу[7].

Якщо ви отримуєте спам-дзвінки та текстові повідомлення на свій Android або iPhone, більшість основних операторів надають вам можливість повідомити про спам. Блокування номерів — ще один спосіб боротьби з мобільним спамом. У США ви можете додати свій номер телефону до Національного реєстру заборонених телефонних дзвінків, щоб спробувати зменшити кількість небажаних дзвінків, які ви отримуєте, але все одно слід бути уважними до шахраїв, які ігнорують цей список.

Чому це називається спамом?

"Спам" спочатку був продуктом Hormel Foods Corporation, США. Так називалася консерва зі свинини та шинки зі спеціями. Це абревіатура, що складається з початкових літер слів "пряна свинина та шинка".

Так що це продукт з харчової промисловості, який не був пов'язаний із комп'ютерами та Інтернетом. Тільки завдяки англійській комічній групі Monty Python, відомій своїм незвичайним гумором, спам став синонімом масової електронної пошти[8].

Через їх постійне повторення жарту - і одного і того ж слова "спам" за короткий час - користувачі каналів Usenet / News (Великобританія) прийняли його у свій лексикон. Масове поширення статті в новинах також стало називатися спам. Звідти термін пізніше перейшов і до інших інтернет-ЗМІ.

Тепер під спамом ми завжди маємо на увазі масове поширення одного й того самого. Інтернет-користувачі найчастіше вживають це слово, пов'язуючи його з відправленням чи отриманням феноменальних обсягів електронної пошти чи повідомлень у соцмережах[9].

Чому спам шкідливий

Спам – це катастрофа, оскільки близько 90% повідомлень електронної пошти є спамом. Спам повторюється і заповнює поштові скриньки. Це витрачає пропускну здатність, впливає на продуктивність сервера та споживає місце на жорсткому диску та пам’ять. Спам присутній скрізь і його не уникнути. Спам впливає на продуктивність співробітників, оскільки спонукає їх перевіряти пошту з поважних причин. Витрачено значний, дорогоцінний час. Спам може бути небезпечним, оскільки відкриття спаму, натискання будь-яких посилань або завантаження будь-яких вкладень може заразити пристрій небезпечним шкідливим програмним забезпеченням[10].

Значення ваших електронних адрес

Якщо ваша папка "Вхідні" заповнена спамом, це продемонструє цінність вашого ідентифікатора електронної пошти. Відкритий обмін адресами електронної пошти має свої недоліки. Скрупульозні організації можуть націлити на ваш ідентифікатор спам-електронну пошту. Адреси електронної пошти збираються зі списків клієнтів, адресних книг, списків контактів, соціальних мереж, веб-сайтів і чатів[11]. На пристроях Android деякі програми запитують доступ до адресної книги (контактів), навіть якщо це їм не потрібно. Деякі програми таємно збирають дані зі списку контактів на пристрої Android. Користувачів Android попереджають перевірити необхідність дозволів, запитуваних програмами[12].

1.2 Аналіз впливу спаму на корпоративну інформаційну систему

Електронний спам існує з перших днів електронної пошти, так звана небажана пошта. Спам може містити різні типи вмісту та теми, такі як реклама, рекламні акції, чудові пропозиції, порнографія та безліч інших речей.

За даними команди експертів із безпеки електронної пошти Cyren, приблизно 80% трафіку електронної пошти, який отримують компанії, є небажаною поштою[13].

Якщо ми подумаємо, що згідно з даними дослідницької компанії Radicati Group, до 2024 року буде надсилатись і отримувати понад 360 мільярдів електронних листів на день, ми говоримо про мільярди надісланих і отриманих електронних листів зі спамом щодня.

Проблема зі спамом полягає в тому, що він сильно втручається в оточення компанії. По-перше, є питання продуктивності. По-друге, йдеться про безпеку та захист інформації та даних вашої компанії[14].

Які проблеми у вашій компанії викликає спам?

1. Це впливає на продуктивність вашої компанії

Спам пов'язаний із втратою продуктивності у вашій компанії, оскільки він займає вашу команду непотрібними завданнями. Це правда, що відкриття поштової скриньки та видалення всього спаму може не зайняти багато часу. Тим не менш, спам – це марна трата часу та відволікання для ваших співробітників, які можуть витрачати енергію на більш продуктивну діяльність.

2. Це впливає на ваші бізнес-послуги та робить компанію більш вразливою

спамерам майже нічого не коштує розсилати мільйони електронних листів. Проблема для вашого бізнесу – масова атака.

Якщо ваша компанія не готова обробляти велику кількість повідомлень, багато ваших послуг можуть бути перервані.

Окрім втрати нового бізнесу через перешкоди комунікації компанії, масова атака часто робить ваш бізнес уразливим до інших загроз і кібератак.

3. Він містить зловмисне програмне забезпечення, наприклад програми-вимагачі та шпигунські програми

Сьогодні спам є одним із найбільш широко використовуваних векторів поширення загроз, у тому числі зловмисного програмного забезпечення.

Ці, здавалося б, нешкідливі посилання та вкладення можуть становити реальну загрозу для вашого бізнесу, приховуючи програми-вимагачі, шпигунські програми та трояни, які дозволяють зловмиснику отримати доступ до комп'ютера, а потім і до всієї мережі компанії.

До речі, згідно зі звітом Verizon, близько 94% зломів за допомогою зловмисного програмного забезпечення відбуваються через використання шкідливих електронних листів.

4. Він містить загрози фішингу та спуфінгу

Спам широко використовується для підробки та фішингу, що також може бути пов’язано з розповсюдженням зловмисного програмного забезпечення. Фішинг і спуфінг використовуються, коли кіберзлочинець створює підроблений веб-сайт для викрадення облікових даних з наміром зламати вашу ділову мережу або отримати доступ до конфіденційної інформації. Уявіть, що зловмисник може спробувати спонукати працівника здійснити оплату за неіснуючим рахунком або надати облікові дані для доступу до системи.

5. Це може спричинити юридичні проблеми

У крайньому випадку, залежно від типу спаму, наприклад спаму порнографічного характеру, ваша компанія може зіткнутися з юридичними проблемами через неправильне використання електронної пошти для незаконної діяльності.

Крім того, може статися так, що кіберзлочинець захопить і використає домен вашої компанії для розповсюдження спаму, що може мати наслідки згідно з певним законом. Це крайні випадки, але вони заслуговують на увагу[15].

За даними GFI Software, лише за останній рік 68% організацій зіткнулися з серйозними порушеннями або повною зупинкою повсякденної діяльності внаслідок принаймні одного інциденту, пов’язаного зі спамом. 45% опитаних постраждали три рази на рік, що суттєво вплинуло на продуктивність, а також створило значні витрати для бізнесу, якщо комп’ютери та сервери потребують дезінфекції або перевстановлення для відновлення після відкриття та запуску спаму на основі шкідливих програм. користувачем. Приблизно 7% респондентів також зізналися, що їхній бізнес більше 10 разів на рік потрапляє в очі через серйозні збої, пов’язані зі спамом[16].

Основні висновки включають:

- Фішинг є найпоширенішим типом спаму, з яким борються організації, 46,5% респондентів назвали його найпоширенішим типом спаму, який отримує їх організація.
- Спам про азартні ігри був другим за поширеністю типом спаму: 39% респондентів назвали його головною проблемою.
- Банківський спам від реальних, але небажаних компаній був третьою найбільшою проблемою, про що повідомили 35% респондентів.
- 54% опитаних помітили підвищення рівня спаму в порівнянні з минулим роком, тоді як лише 15% помітили зниження рівня вхідного спаму.
- 79% компаній покладаються на те, що кінцеві користувачі виявляють найкраще рішення щодо будь-якого спаму, який не перехопив спам-фільтр на стороні сервера чи клієнта.

Незважаючи на передбачуване зростання обсягу спаму, яким організації повинні керувати, загальна частка спаму в трафіку електронної пошти залишається відносно низькою. Частково завдяки зростаючій залежності від електронної пошти для повсякденного ділового спілкування та збільшенню обсягу – як внутрішнього, так і зовнішнього – 50% опитування повідомили, що спам становить не більше 15% загального трафіку електронної пошти, що зменшує обсяг і деструктивний характер деяких типів спаму є більшою проблемою[17]. Проте чверть учасників опитування також визнали, що спам становить до чверті загального трафіку електронної пошти, а ще 8% сказали, що на спам припадає до половини загального трафіку. Ці підвищені показники захворюваності значно збільшують шанси того, що зловмисний спам пройде фільтри та введе в оману користувачів, які нічого не підозрюють.

Цифри подібні, якщо дивитися на вплив зберігання електронної пошти. Ефективна фільтрація в поєднанні з хорошою політикою та навчанням має гарантувати, що більша частина спаму затримується на сервері, а все, що просочується, або обробляється за допомогою заходів щодо спаму на стороні клієнта та найкращих практик для користувачів[18].

У той час як 56% опитаних сказали, що спам займає до 15% від загальної кількості збережених і архівованих електронних листів, а чверть (24%) стверджують, що ця цифра становить не більше 10% від загальної пам'яті, решта 21% мають справу з великими накладними витратами на сховище, при цьому до половини сховища пошти займає спам, що коштує компанії грошей і не приносить жодної користі[19].

Серхіо Галіндо, генеральний менеджер GFI Software[20], каже: «Злочинці все частіше використовують спам для доставки зловмисного програмного забезпечення на робоче місце з метою спричинення збоїв, утримання комп'ютерів і серверів з метою отримання викупу або навіть викрадення цінної інформації, яку можна продати чи використати для інших цілей. шахрайство. Заражені машини означають непродуктивність комп'ютерів і користувачів, обмежують бізнес-діяльність і втрачають гроші. Викрадені дані можуть призвести до чого завгодно: від штрафів до втрати довіри клієнтів, тоді як навіть спам, не пов'язаний із зловмисним програмним забезпеченням, створює перешкоди, засмічуючи поштові скриньки, заповнюючи пам'ять і забираючи час IT-адміністраторів, які можуть бути використані для виконання більш цінних завдань».

Дослідження показало, що кожен п'ятий кінцевий користувач в опитаних організаціях зобов'язаний активно боротися зі спамом, який не затримується спам-фільтрами. У той час як 44% сказали, що співробітники їхньої організації ігнорують спам – це не ідеально, але ігнорований спам є принаймні інертним спамом – третина (33%) визнала відсутність вказівок щодо того, хто несе відповідальність за роботу зі спамом, який потрапляє до кінцевого користувача.

Згідно з чвертю (24%) опитаних, найпоширенішою формою збою, пов'язаного зі спамом, є зараження шкідливим програмним забезпеченням. Коли організації зазнають збоїв, пов'язаних зі спамом – наприклад, користувач натискає вкладений файл із зловмисним програмним забезпеченням або посилання на веб-сайт, наповнений зловмисним програмним забезпеченням – зриви для бізнесу є суттєвими. Опитування показало, що 58% опитаних втратили до трьох годин продуктивності в результаті спаму. Майже третина (31%) втратили до п'яти годин

на інцидент, тоді як 9% втратили до дев’яти годин – більше одного робочого дня в більшості офісних організацій.

«Не слід недооцінювати вплив спаму на бізнес. Втрата продуктивності не лише має каскадний ефект у всьому бізнесі, але й безпосередньо впливає на прибутки компанії. Якщо вам пощастить, час, витрачений IT-спеціалістами на відновлення ПК або сервера, буде швидким, але якщо машини та дані будуть викрадені або заблоковані в результаті шахрайства зловмисного програмного забезпечення-вимагача, час і витрати для організації можуть швидко згорнути», — додав Галіндо.

Сліпе незалежне дослідження було проведено для GFI Software компанією Opinion Matters, у якій взяли участь 200 британських керівників IT-рішень в організаціях із кількістю співробітників від 5 до 1000 осіб.

1.3 Актуальність спам атак на користувацькі поштові скриньки сьогодні

1.3.1 Спам під час COVID-19

Всесвітня організація охорони здоров'я (ВООЗ) — це одне з основних джерел інформації про спалах коронавірусу, на яке посилаються усі новинні портали. Авторитетність ВООЗ використовують і шахраї. Зокрема, зловмисники відправляють листи з новинами нібито від офіційної організації , але насправді їх ціль — змусити потенційних жертв натиснути на шкідливі посилання. Як правило, після переходу на таке посилання користувач може встановити шкідливі програми на пристрій, які здатні викрадати персональні дані або дані для входу в систему[20].

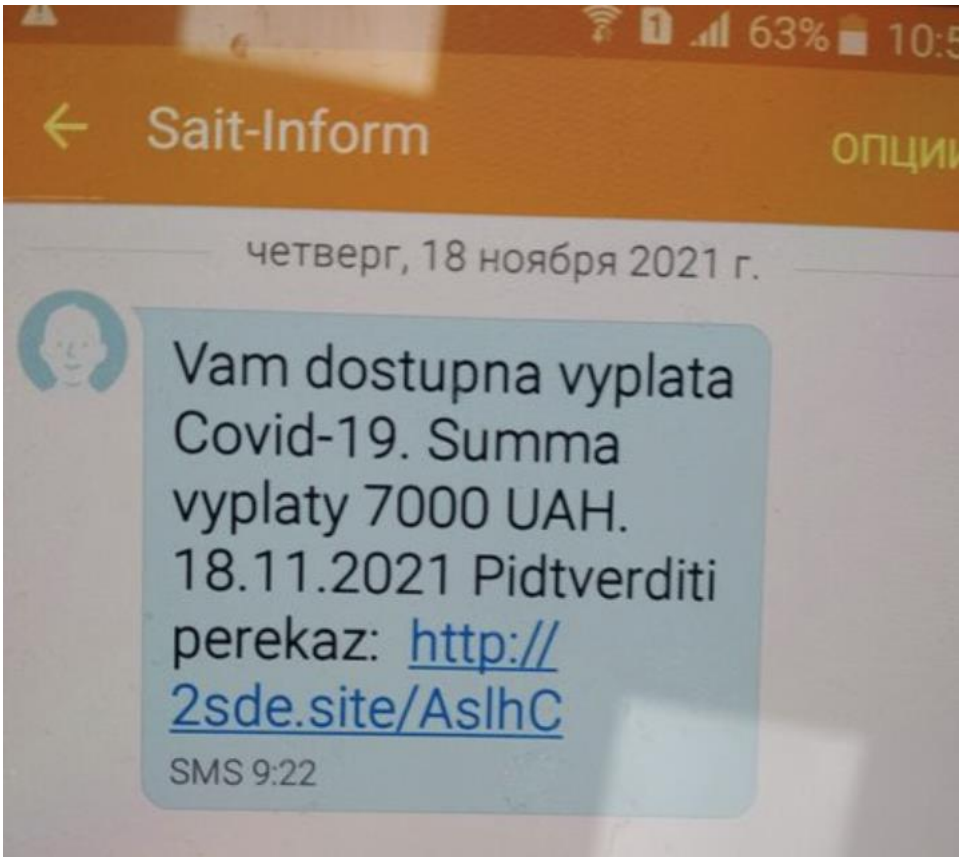

Рис 1.5. Фішингове повідомлення

Схеми з використанням теми благодійності

Також поширеним видом шахрайства є використання теми благодійності, щоб змусити жертву купити вакцину для дітей в Китаї. У випадку з коронавірусом злочинці використовують існуючі схеми шахрайства та адаптують свій контент до COVID-19.

Людей, які отримали листи про коронавірус, закликали перевести біткоїни на гаманці зловмисників. Хоча цей метод працює лише для невеликого відсотка користувачів, він надзвичайно привабливий у фінансовому плані для світових злочинців.

Спам із закликами до дії

Ще один тип шахрайства — розсилка електронних листів із фіктивними пропозиціями замовити маски для обличчя, які нібито захищають вас від небезпечних захворювань. Натомість жертви несвідомо надають особисту та фінансову інформацію шахраям. Цей тип шахрайства стає все більш популярним через страх людей. За даними Google Trends, кількість запитів «дезінфікуючий

засіб для рук» і «маска для обличчя» досягла неймовірної кількості. Злочинці активно використовують підвищений попит на ці товари для отримання фінансової вигоди. За даними Sky News, у лютому лише у Великобританії шахраї заробили 800 000 фунтів стерлінгів (1 мільйон доларів)[21].

Кіберзлочинці завжди використовують катастрофи та гарячі події на свою користь. З початком кризи COVID-19 спамери розпочали різноманітні тематичні спамерські компанії проти робітників, закладів охорони здоров'я та навіть широкої громадськості. Звіт від Microsoft показав, що в березні кібератаки, пов'язані з COVID-19, досягли безпрецедентного рівня, більшість з цих шахрайств є підробленими веб-сайтами COVID-19, згідно з даними охоронної компанії RiskIQ.

APWG повідомила, що цілями є переважно працівники, закладів охорони здоров'я та безробітні.

Було виявлено три основні мети спамерських листів, пов'язаних з COVID-19. Шахраї зосередили свої зусилля на:

- просити пожертвування фальшивим благодійним організаціям;
- збір облікових даних;
- впровадження шкідливого ПО.

У четвертому кварталі 2020 року APWG OpSec Security виявили, що фішингові атаки на фінансові інститути були найбільш поширеними. Спам SaaS і веб-пошти зменшився з 30,4% усіх атак у третьому кварталі 2020 року до 23,2% у четвертому кварталі.

1.2.2 Спам під час війни

Насьогодні є досить актуальним не тільки війна на полі бою, але й у кіберпросторі. Таким чином у жовтні 2022 року почали активно поступати фішингові та заздалегідь інфіковані електронні листи від імені Офісу Президента, СБУ та Генштабу Збройних Сил України. Про це повідомив начальник Генштабу Збройних Сил України: «Останнім часом на електронну пошту та в месенджери почали надходити листи нібито від прес-служби начальника Генштабу ЗСУ.»[22]

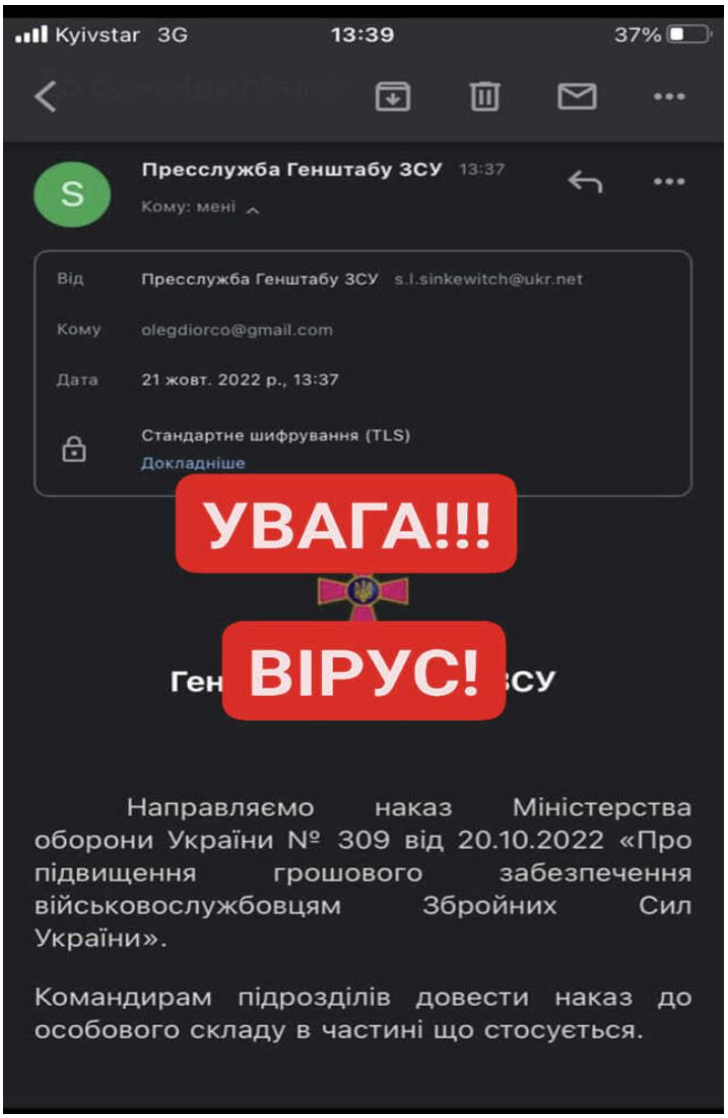

Рис. 1.6. Фейковий лист

Спам може бути корисним?

Норвезький експерт з кібербезпеки вже у травні створив веб-сайт, який дозволяє будь-кому надсилати електронні листи про війну в Україні на 150 російських електронних адрес одночасно, щоб росіяни мали можливість почути правду, яку приховує їх уряд. По всій Росії задіяні більше 100 мільйонів електронних скриньок на які приходять сотні тисяч повідомлень з однаковою інтригуючою темою «Я вам не ворог.»

Повідомлення з'являється російською мовою з перекладом англійською і починається так: «Дорогий друже, я пишу тобі, щоб висловити свою стурбованість

безпечним майбутнім наших дітей на цій планеті. Більшість світу засудила вторгнення Путіна в Україну».

Довгий електронний лист продовжує закликати росіян відмовитися від війни в Україні та шукати правду про вторгнення в недержавних службах новин.

Лише за кілька днів понад 22 мільйони цих електронних листів потрапили в російські скриньки, і їх надсилають волонтери з усього світу, які жертвують свій час і адреси електронної пошти на цю справу.

Це один із зростаючої кількості незвичайних способів, якими хакери, хактивісти та звичайні люди в усьому світі намагаються зв'язатися з росіянами в Інтернеті, щоб обійти блокування ЗМІ та цензуру. Ідея одного польського користувача Твіттера розмістити відгуки про війну з російським бізнесом у Google і Yandex стала вірусною.

В інших місцях хакерські групи стверджують, що спотворили російські новинні сайти з повідомленнями до росіян «зупинити Путіна».

Але спам-кампанія електронної пошти, створена невеликою командою в Норвегії, здається, захопила уяву тисяч людей, які шукали способів допомогти росіянам дізнатися про війну.

Автор проекту, 50-річний Фабіан, який керує комп'ютерним мережевим бізнесом, не хоче, щоб його прізвище публікували, побоюючись помсти з боку російської влади. Він каже, що відчув потребу щось зробити після того, як дедалі більше хвилювався щодо можливості Третьої світової війни[23].

Його веб-сайт, який ВВС не називає, обходить російську цензуру за допомогою поєднання розумних обчислень і людської влади. Система дозволяє людям надсилати його шаблонне повідомлення на десятки російських електронних адрес одночасно, і, за його оцінками, десятки тисяч добровольців зробили це з моменту запуску веб-сайту.

Фабіан побудував його разом із п'ятьма колегами, які минулих вихідних працювали без зусиль, щоб виконати роботу. Вони почали з пошуку в Інтернеті відомих російських електронних адрес і склали список із 90 мільйонів облікових записів, які, на їхню думку, є активними. Він каже, що сила системи полягає в тому,

щоб змусити волонтерів використовувати власні облікові записи електронної пошти замість масового обміну повідомленнями на адреси електронної пошти за допомогою програмного забезпечення для спаму.

Користувачі можуть обрати контакт від одного до 150 росіян. Потім одним клацанням миші клієнт електронної пошти за умовчанням (наприклад, Outlook або Gmail) завантажує унікальні адреси електронної пошти, тему та основний текст, готовий для надсилання.

Люди також можуть персоналізувати вміст, щоб збільшити ймовірність того, що їхні електронні листи будуть прочитані.

Є дві причини, каже Фабіан, для використання особистих облікових записів електронної пошти людей: електронні листи потрапляють через фільтри спаму, якщо вони надіслані з реальних облікових записів, і в невеликій кількості.

«Але також люди можуть отримувати відповіді від росіян, спілкуватися з ними та вести розмови про війну» - каже автор.

Фабіан стверджує, що деякі облікові записи будуть менш активними, ніж інші, і в деяких випадках електронний лист може опинитися в папці небажаної пошти. Але багато повідомлень читаються, каже він, і деякі росіяни відповідають.

1.2.3 Спам атаки в залежності від країни походження

Спам є глобальною проблемою, але деякі країни майже не роблять, щоб утримати спамерів від діяльності в межах своїх кордонів. Ці країни, як правило, мають або слабкі, або взагалі відсутні закони про спам. Вони стають безпечними гаванями для операцій зі спамом і підривають глобальні зусилля з припинення спаму; навіть на шкоду власній нації, мережам і громадянам.

Деякі Інтернет-провайдери в цих країнах неохоче або прямо відмовляються вживати заходів без такої підстави в законі, навіть якщо більшість Інтернет-провайдерів використовують угоди «Політики прийнятного використання» (AUP), які виконуються на договірній основі. Здається, лише тоді, коли світ загалом визнає погану репутацію цих країн, вживаються будь-які заходи.

Ця діаграма показує кількість записів SBL для кожної країни, включаючи джерела спаму, а також розміщення спам-сервісів – веб-сайтів, DNS тощо.

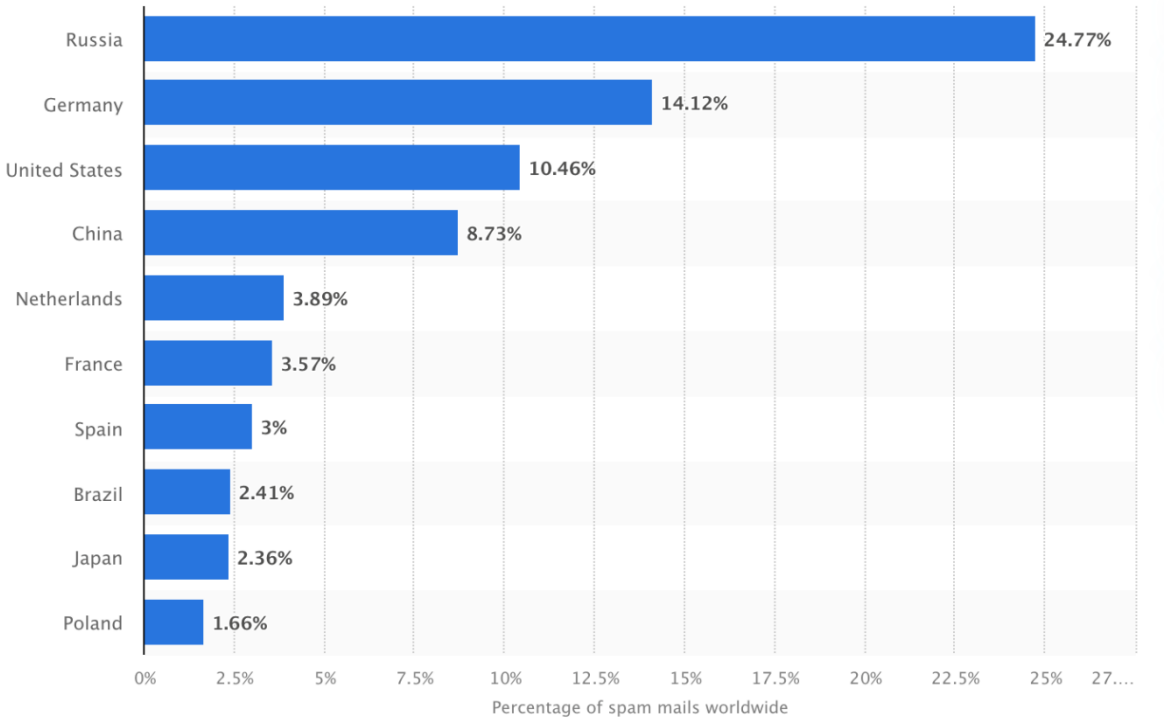

Рис. 1.7. Кількість спамерів в залежності від країни походження (від загальної кількості листів)

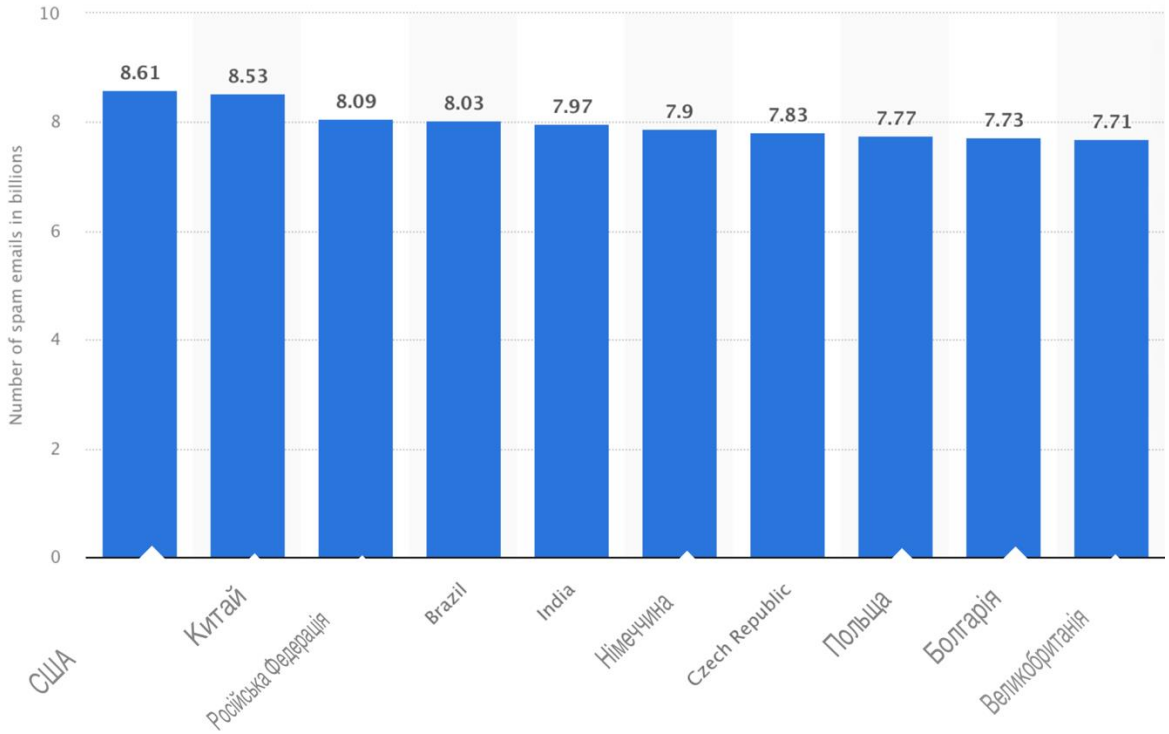

Рис 1.8. Кількість спам листів за країною походження

2 МОЖЛИВІ МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ВІД СПАМ АТАК КОРПОРАТИВНИХ КОРИСТУВАЧІВ НА ОСНОВІ CYREN EMAIL SECURITY ENGINE

2.1. Призначення та основні можливості продукту Cyren Email Security Engine

Cyren Email Security Engine - це хмарна служба захисту бізнес-електронної пошти, яка підходить для використання корпоративними IT-відділами або постачальниками керованих послуг. Опція багатокористувацької платформи дозволяє MSP забезпечувати захист від спаму та зловмисного програмного забезпечення систем електронної пошти своїх клієнтів без небезпеки витоку даних між обліковими записами клієнтів. Програма надає інформацію з понад 200 мільйона доменів, щоб надати користувачеві краще розуміння поточних загроз. Використовуючи програмне забезпечення, користувач може переглядати проблемні повідомлення електронної пошти в карантині та заносити підозрілих відправників у чорний список, щоб не зв'язуватися з ними[24].

Cyren Email Security Engine є дуже ефективним фільтром спаму. Перевага цього інструменту перед конкурентами полягає в тому, що він дуже простий у застосуванні. Служба надається як плагін для всіх основних систем електронної пошти, включно з хмарними, такими як Microsoft Exchange і Gmail. Додавання цього плагіна налаштовує виклик віддаленого процесу для сканування кожного вхідного листа

Система виявлення від Cyren здатна виявляти спам, фішингові та масові електронні листи, які називаються «сірою поштою», а також шкідливі посилання та зловмисне програмне забезпечення, а також блокує DDoS-атаки. Сервіс також перевіряє вихідні листи. Для додаткового захисту програма використовує шифрування SSL та TLS, щоб захистити вашу взаємодію від стеження. Якщо клієнт-сервер вийде з ладу, інструмент використовуватиме автоматичне

чергування пошти, щоб допомогти вам якнайшвидше повернутися до нормальної роботи.

Система використовує поєднання виявлення загроз на основі ШІ та чорних списків електронних та IP-адрес. Він переглядає вихідні адреси електронної пошти та співвідносить їх із відомими ідентифікаторами співробітників, щоб блокувати спроби видавання себе за іншу особу. Він також може виявляти зловмисні посилання на сайти, які видають себе за іншу особу або заражені сайти.

Cyren має 99,9% успішного блокування спаму. Інформаційні листи також блокуються, але зберігаються в карантині, пропонуючи можливість завантажити їх. Він встановлює баланс між відсіюванням шкідливих повідомлень без блокування повідомлень від законних користувачів електронної пошти. З точки зору підприємства, це платформа для боротьби зі спамом, яка не заважає повсякденній роботі.

Для розпізнавання останніх загроз Cyren використовує суміш машинного навчання та байєсівського аналізу для виявлення нових атак. Потужний захист електронної пошти від загроз нульового дня чудово підходить для мінімізації впливу нових загроз електронної пошти. Також спам-фільтр використовує чорний та білий списки.

Щоб запобігти проникненню вірусів у вашу скриньку вхідних повідомлень, програма дозволяє попередньо переглядати та видаляти електронні листи перед їх завантаженням на комп’ютер. Блокуючи подібні електронні листи, ви можете переглядати інформацію в електронному листі, не відкриваючи його, піддаючи комп’ютер ризику передачі вірусу.

Фільтрування — ще один спосіб, за допомогою якого Cyren відстежує вхідні електронні листи на наявність підозрілих ознак. Фільтр може виявляти вміст спаму та образливі слова, щоб відправника можна було автоматично додати до чорного списку з подальшої кореспонденції. Щоб зупинити помилкові сповіщення, ви можете додати колег і клієнтів до списку «друзів».

Фільтр Cyren працює кількома мовами та може блокувати спам англійською, іспанською, німецькою, французькою, італійською, польською, данською тощо.

Після того, як підозрілу електронну пошту буде позначено, програмне забезпечення додасть відправника до чорного списку та заблокує майбутні електронні листи, які надходять до вашої папки "Вхідні".

Система Cyren працює за моделлю краудсорсингу. Коли користувач отримує електронний лист і позначає його як спам, адреса електронної пошти джерела та IP-адреса позначаються. Якщо достатньо користувачів позначає те саме джерело, воно додається до глобального чорного списку.

Інтерфейс користувача простий у навігації, і ви можете переглядати статистику заблокованих повідомлень. Крім того, ви також можете повідомити про зловживання спамом одним натисканням кнопки, якщо вам потрібно зібрати інформацію. Можливість упорядкувати всю цю інформацію безпеки допомагає переконатися, що ви знаєте про все, що намагається отримати доступ до вашого облікового запису.

Інструмент ідеально підходить для корпоративних користувачів, оскільки пропонує інтеграцію з Office 365. Якщо служба електронної пошти Office 365 вимикається, користувач може натомість надсилати електронні листи з веб-панелі Cyren. У разі збою інформаційна панель дозволяє підтримувати роботу служби.

Баланс між прийнятними та забороненими адресами електронної пошти взаємопов’язаний із серією інших сканувань і перевірок кожного надходження електронного листа.

Користувач також може контролювати, що відбувається з тими електронними листами, які перехоплює фільтр спаму. Наприклад, ви можете відхилити їх, щоб відхилити передачу, зберегти пошту або перенаправити її в іншу поштову скриньку[25].

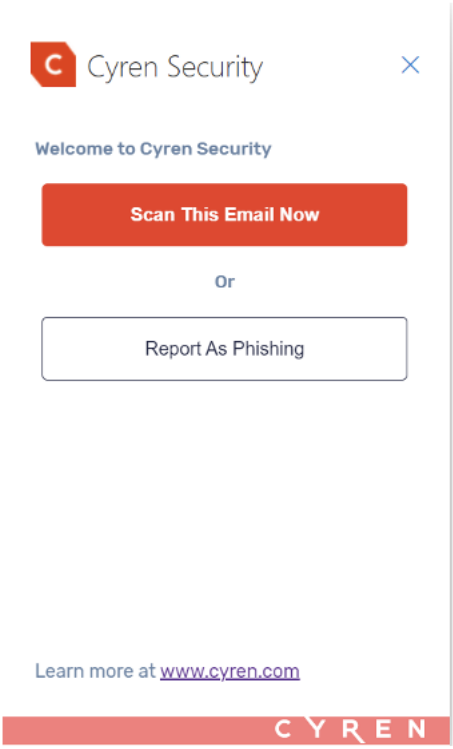

Рис. 2.1. Інтерфейс плагіну для Outlook

Cyren Email Security Engine — хороший вибір для будь-якого бізнесу. Малі підприємства можуть отримати доступ до trial-версії, який захищає лише 5 обліковий запис електронної пошти, але також можна зареєструвати кілька облікових записів.

Будь-яка компанія, яка має систему електронної пошти – а це кожна компанія – виграє від використання Cyren Email Security Engine. Систему може налаштувати будь-який адміністратор, тому вам не потрібні виняткові технічні навички для встановлення та керування цим сервісом.

Оскільки Cyren Email Security Engine також перевіряє вихідні електронні листи, пропонує систему захисту від втрати даних, вбудовану в службу фільтрації електронної пошти. Це робить цей інструмент дуже хорошим вибором для підприємств, які повинні дотримуватися стандартів захисту конфіденційних даних.

Службу Cyren легко налаштувати, і вам не потрібно розміщувати програмне забезпечення на серверах вашої компанії. Цю систему можна застосувати дуже швидко, і вона надає можливість продавати додаткові послуги для MSP, які бажають додати додаткові послуги до своїх прейскурантів.

2.2 Архітектура Cyren Web Security Engine

Механізм веб-безпеки Cyren класифікує URL-запити користувачів таким чином:

1. Web Security Engine встановлено на партнерському пристрої, наприклад, Web Security Gateway.

2. Партнерський пристрій отримує HTTP-запит.

3. Пристрій використовує механізм для перевірки класифікації URL. Система веб-безпеки спочатку перевіряє локальний кеш на наявність значень; зазвичай більше 99% запитів вирішується локально кеш-пам'яттю, мінімізуючи затримку.

4. За потреби Web Security Engine надсилає запит Cyren's GlobalView щодо відповідних оновлень.

5. Партнерський пристрій блокує, дозволяє або видаляє вміст відповідно до класифікацію, яку він отримує від механізму фільтрації URL-адрес GlobalView.

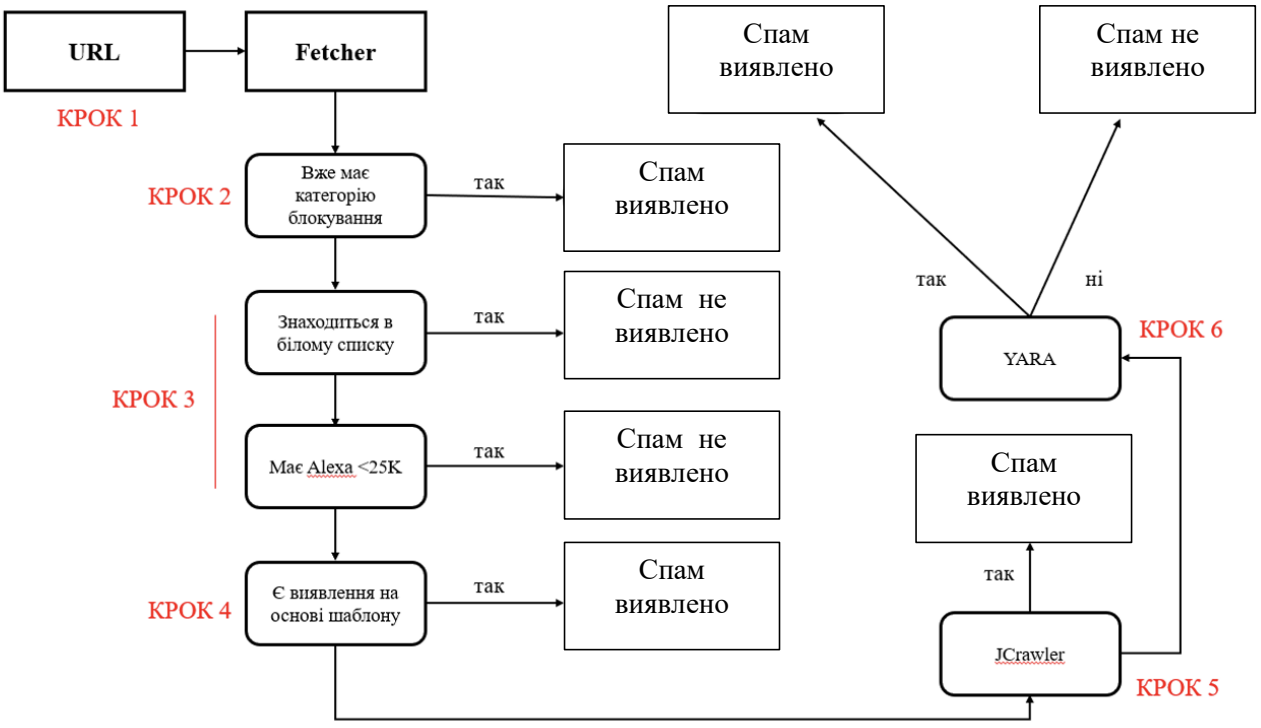

Рис 2.2. Логіка роботи Cyren Email Security Engine

Деталі SDK:

- 64 категорії, 8 з яких пов’язані з безпекою — повертає до 5 категорій на URL-адресу;
- мова та контент-агностик; широке охоплення глобальних сайтів;
- база даних містить ~200 мільйонів найбільш релевантних URL-адрес;
- конфігурований відбиток кешу з автоматичним налаштуванням вмісту кешу;
- висока продуктивність: >50 000 запитів на секунду з низьким використанням ресурсів;
- підтримує http, https, ftp та інші протоколи.

Усі ці фактори усувають обмеження щодо локального сховища та дає клієнтам та партнерам Cyren гнучкість:

- глобальні диверсифіковані джерела даних, отримані з мільярдів транзакцій щодня;
- масивна централізована база даних, що містить усі необхідні класифікації URL-адрес;
- легкі, економічні локальні клієнти, які зберігають лише ті дані, які вам потрібні і це потрібно, усуваючи ресурсомісткі оновлення;
- безперервне відстеження, неперевершена точність.

Механізм веб-безпеки Cyren інтелектуально визначає, коли та як глибоко сканувати кожний сайт, використовуючи кілька методів:

- найкраща безпека «нульового дня»;
- класифікація, орієнтована на клієнта, що запускається після кожного нового відвіданого сайту;
- аналіз динаміки сайту та поведінки користувачів для визначення глибини сканування;
- постійне відстеження для забезпечення точної класифікації URL-адрес у будь-який момент.

Постачальники систем безпеки обміну повідомленнями тепер можуть досягти безпрецедентної продуктивності та рівня виявлення, блокування зомбі-трафіку до його потрапляння в мережі клієнтів.

Cyren Email Security Engine може похизуватися використанням найповнішої у світі мережі безпеки електронної пошти — Cyren's GlobalView — це вбудований аналіз IP-репутації в режимі реального часу:

- ідентифікуйте сотні тисяч нових зомбі (зламані облікові записи та хост комп’ютери) щодня;
- постійне відстеження трафіку з десятків мільйонів IP-адрес;
- точна класифікація мільярдів електронних листів на тиждень у режимі реального часу.

GlobalView від Cyren компілює як історичні, так і найновіші відправники дані про репутацію з дуже різноманітних джерел трафіку в кожній країні з охопленням

від керованих служб і мережевих апаратних пристроїв до програмного забезпечення для настільних ПК. Запатентована технологія Recurrent Pattern Detection автоматично збирає це у високорівневий перегляд усіх відправників, розрізняючи в реальному часі легітимних корпоративних відправників, дійсних видавців, зомбі(спуфнуті ПК або пошти) та спамерів або ж розповсюджувачів зловмисного програмного забезпечення.

Цікаві факти:

- зомбі розсилають 85% усього спаму, приблизно 120 мільярдів повідомлень на день;
- близько 200 000-500 000 зомбі «оживають» щодня;
- типовий зомбі-ботнет надсилає до 1 мільярда повідомлень за кілька годин;
- зазвичай в одному ботнеті міститься 10 000–200 000 зомбі;
- 5–10 мільйонів зомбі активні в будь-який день.

Додаткові можливості рішення Cyren Email Security Engine :

- виявлення ботнету в реальному часі — менше хвилини від початку атаки;
- оцінка високої точності на основі Cyren's GlobalView:
- 80+ мереж постачальників, що охоплюють 190 країн;

- Джерела: брандмауери, пристрої обміну повідомленнями, програмне забезпечення для настільних ПК, xSP;
- сукупні атрибути: інформація DNS, географія, динамічні IP-адреси, загальнодоступні RBL, тощо;
- Decision Manager підвищує захист від зомбі, мінімізує помилкові спрацьовування;
- багатий набір даних надається для кожної IP-адреси, включаючи:
- Рекомендована дія: заблокувати, придушити, дозволити;
- IP-клас — класифікує IP за дієвими класами;
- Рівень ризику IP-адреси – ймовірність того, що повідомлення буде небажаним: 0–100%;
- співвідношення та коефіцієнт спаму;
- класифікація рекламних компаній (наприклад, інформаційні бюлетені).

Технічні характеристики:

• Підтримує стандартні платформи Mail Transfer Agent (MTA).

• Розроблено для високої масштабованості — понад 4000 повідомлень/с

• Кілька варіантів розгортання: локальний домен для вбудованого кешування та відновлення після відмови (на базі Linux, FreeBSD, Solaris і Windows).

• Доступні інтерфейси HTTP, UDP і RBL/RBL+

• Доступ до хмари через UDP — встановлення програмного забезпечення не потрібно.

2.3. Способи та методи розпізнавання спаму

2.3.1. Технічні заходи

Серед усіх різноманітних методів боротьби зі спамом найефективнішими стали технічні заходи. Для фільтрації спаму використовується кілька підходів. У наступному розділі ми прокоментуємо деякі з найпопулярніших підходів.

Примітивний мовний аналіз або евристичний аналіз. Фільтрування вмісту

Найперші фільтри спаму використовували примітивні методи аналізу мови для виявлення небажаної електронної пошти. Ідея полягала в тому, щоб зіставити певні

тексти чи слова з тілом електронного листа чи адресою відправника. У середині 1990-х років, коли спам не був такою проблемою, як сьогодні, користувачі могли фільтрувати небажані електронні листи, скануючи їх, шукаючи фрази чи слова, які вказували на спам, наприклад «Віагра» або «Купити зараз». У ті часи спам повідомлення не були такими складними, як сьогодні, і цей дуже спрощений підхід міг фільтрувати ~80% спаму. Перші версії найважливіших поштових клієнтів включали цю техніку, яка деякий час працювала досить добре, перш ніж спамери почали використовувати свої хитрощі, щоб уникнути фільтрів. Те, як вони заплутували повідомлення, робило цю техніку неефективною. Іншим недоліком цього підходу був високий рівень хибно-позитивних результатів: будь-яке повідомлення, що містило «заборонені слова», відправлялося у кошик. Більшість із цих слів підходять для фільтрації спаму, але іноді вони можуть з'являтися в законних електронних листах. Цей підхід зараз не використовується через низьку точність і високий рівень помилок. Ця примітивна техніка аналізу насправді є формою аналізу вмісту, оскільки вона використовує вміст кожного електронного листа, щоб визначити, чи є він спамом або легітимним листом.

Білий і чорний списки

Білий і чорний списки є надзвичайно популярними методами фільтрації спаму. Білі списки вказують, повідомлення яких відправників ніколи не вважаються спамом, а чорні списки включають тих відправників, яких завжди слід вважати спамерами. Білий список містить адреси, які вважаються безпечними. Ці адреси можуть бути окремими електронними адресами, доменними іменами чи IP-адресами, і вони зареєструють окремого відправника або групу відправників. Цю техніку можна використовувати на стороні сервера та/або на стороні клієнта, і зазвичай її можна знайти як доповнення до інших більш ефективних підходів. У білих списках на стороні сервера адміністратор має перевірити адреси, перш ніж вони перейдуть до довіреного списку. Це може бути здійсненним у невеликій компанії або на сервері з невеликою кількістю облікових записів електронної пошти, але це може перетворитися на біль, якщо використовувати його на великих корпоративних серверах, де кожен користувач має власний білий список. Це тому,

що завдання перевірки кожного електронного листа, якого немає в списку, займає багато часу. Екстремальним використанням цієї техніки може бути відхилення всіх електронних листів від відправників, яких немає в білому списку. Це може здатися дуже нерозумним, але це не так. Його можна використовувати в обмежених доменах, наприклад у школах, де ви надаєте перевагу фільтруванню електронних листів від невідомих відправників, але хочете тримати дітей подалі від потенційно шкідливого вмісту, оскільки спам-повідомлення можуть містити порнографію чи інший вміст для дорослих. Насправді цей агресивний метод захисту від спаму використовувався деякими безкоштовними постачальниками послуг електронної пошти, як-от Hotmail, у якому можна встановити правило, яке запобігає потраплянню будь-яких повідомлень, що надходять від будь-якої іншої служби, до поштових скриньок їхніх користувачів. Білі списки також можна використовувати на стороні клієнта. Фактично, одна з перших технік, використаних для фільтрації спаму, полягала у використанні адресної книги користувача як білого списку, позначаючи як потенційний спам усі листи, які містили в полі FROM: адресу, якої не було в адресній книзі. Ця техніка може бути ефективною для тих людей, які використовують електронну пошту лише для спілкування з обмеженою групою контактів, як-от родина та друзі. Основною проблемою білих списків є припущення, що довірені контакти не надсилають небажаної електронної пошти, і, як ми побачимо, це припущення може бути помилковим. Багато спамерів використовують комп’ютери, які були скомпрометовані за допомогою троянських програм і вірусів, для надсилання спаму, надсилаючи його всім контактам адресної книги, щоб ми могли отримати спам від відомого відправника, якщо його комп’ютер був заражений вірусом. Оскільки ці контакти знаходяться в білому списку, усі повідомлення, що надходять від них, позначаються як безпечні. Чорні списки, найчастіше відомі як чорні списки DNS (DNSBL), використовуються для фільтрації електронних листів, які надсилаються з відомих спам-адрес або скомпрометованих серверів. Найпершим і найпопулярнішим чорним списком був торгова марка Realtime Blackhole List (RBL), керована Системою запобігання зловживанням поштою. Системні адміністратори, використовуючи інструменти

виявлення спаму, повідомляють про IP-адреси машин, які надсилають спам, і вони зберігаються в загальному центральному списку, яким можуть спільно користуватися інші фільтри електронної пошти. Більшість антиспамових програм мають певну форму доступу до таких мережевих ресурсів. Агресивні чорні списки можуть блокувати цілі домени або інтернет-провайдерів, які мають багато помилкових спрацьовувань. Спосіб вирішення цієї проблеми полягає в тому, щоб створити кілька розповсюджених чорних списків і порівняти інформацію про відправника з деякими з них перед блокуванням електронної пошти. Поточні чорні списки DNS є динамічними, тобто вони не тільки поповнюються новою інформацією, але й закінчуються, зберігаючи актуальне відображення поточної ситуації в адресному просторі.

Сірий список

Як доповнення до білих і чорних списків, можна використовувати сірі списки. Основою цього підходу є припущення, що небажана електронна пошта надсилається за допомогою спам-ботів, це спеціальне програмне забезпечення, призначене для надсилання тисяч електронних листів за короткий час. Це програмне забезпечення відрізняється від традиційних серверів електронної пошти та не відповідає стандартам електронної пошти RFC. Зокрема, електронні листи, які не досягли мети, не надсилаються повторно, як це робить реальна система. Це правильна функція, яку використовують сірі списки. Коли система отримує електронний лист від невідомого відправника, якого немає в білому списку, вона створює функцію «tupla». Коли в системі вперше виникає функція «tupla», електронний лист відхиляється, тому повертається відправнику. Сервер знову надішле цей електронний лист, тож коли система вдруге знайде «tupla», електронний лист буде позначено як безпечний і доставлено одержувачу. Сірі списки мають деякі обмеження та проблеми. Очевидними з них є затримка, яку ми могли б мати в отриманні деяких законних електронних листів, використовуючи цей підхід, тому що ми повинні чекати, доки електронний лист буде надіслано двічі, і марна пропускна здатність, яка виникає в процесі надсилання– відхилення– повторного надсилання. Інші обмеження полягають у тому, що цей підхід не

працюватиме, коли спам надсилається з відкритих ретрансляторів, оскільки вони є справжніми серверами електронної пошти, і для спамерів це простий спосіб обійти сірі списки, просто додавши нові функції до програмного забезпечення, дозволяючи йому знову надсилати відхилені електронні листи.

Цифрові підписи та контроль репутації

З появою криптографії з відкритим ключем і, зокрема, її застосування для кодування та підписання електронної пошти, найпомітніше представлене Pretty Good Privacy (PGP) і GNU Privacy Guard (GPG), існує можливість відфільтрувати непідписані повідомлення, а якщо вони підписані, ті, які надіслано ненадійними користувачами. PGP дозволяє підтримувати нетривіальну мережу/ланцюжок довіри між користувачами електронної пошти, таким чином, як ця довіра поширюється на мережу контактів. Таким чином, користувач може довіряти підписувачу повідомлення, якщо йому довіряє інший контакт одержувача електронної пошти. Основним недоліком цього підходу є те, що користувачі PGP/GPG рідкісні, тому досить ризиковано вважати, що електронні листи надходять лише від довірених осіб. Однак цю ідею можна поширити на сервери електронної пошти. Як ми бачили в попередньому розділі, багато фільтрів електронної пошти використовують білі списки для зберігання безпечних відправників, як правило, локальних адрес і адрес друзів. Отже, якщо спамери з'ясовують, хто наші друзі, вони можуть підробити FROM: заголовок повідомлення з цією інформацією, уникаючи фільтрів, оскільки відправники, які знаходяться в білих списках, ніколи не фільтруються. Структура політики відправника (SPF), ключі домену та ідентифікатор відправника намагаються запобігти підробці, реєструючи IP-адреси машин, які використовуються для надсилання електронної пошти, для кожного дійсного відправника електронної пошти на сервері. Отже, якщо хтось надсилає електронний лист із певного домену, але він не збігається з IP-адресою відправника, ви можете знати, що електронний лист підроблено. Повідомлення підписуються відкритим ключем сервера, що робить його запис SPF, DomainKeys або ідентифікатор відправника загальнодоступним. Оскільки все більше й більше постачальників послуг

електронної пошти (особливо безкоштовних, таких як Yahoo!, Hotmail або Gmail) оприлюднюють свої IP-записи, цей підхід ставатиме все ефективнішим. Підписи є базовою реалізацією більш складної техніки, якою є контроль репутації для відправників електронної пошти. Коли система отримує електронний лист від невідомого відправника, воно сканується та класифікується як законне або спам. Якщо електронна пошта класифікується як законна, репутація відправника підвищується та знижується, якщо класифікується як спам. Чим більше електронних листів надсилається з цієї адреси, тим позитивніше чи негативніше оцінюється відправник. Коли репутація переступає певний поріг, її можна перемістити до білого або чорного списку. Цей підхід можна поширити на весь IP-простір у мережі, оскільки поточні продукти захисту від спаму за допомогою функції IronPort під назвою SenderBase.

Поштові витрати

Однією з основних причин успіху спаму є низька вартість розсилки спаму. Відправникам не потрібно платити за надсилання електронної пошти, а витрати на пропускну здатність дуже низькі, навіть якщо надсилаються мільйони електронних листів.

Поштова оплата — це техніка, заснована на принципі, згідно з яким відправники небажаних повідомлень демонструють свою добру волю, сплачуючи якусь поштову оплату: або невелику суму грошей, сплачену в електронному вигляді, жертву кількох секунд людського часу для відповіді на просте запитання, або деякий час обчислення в машині відправника. Оскільки служби електронної пошти базуються на простому протоколі пересилання пошти, економічні поштові витрати потребують спеціальної архітектури в мережі або кардинальної зміни протоколу електронної пошти. Абаді та ін. описує клієнтсько-серверну архітектуру на основі квитків, яка забезпечує поштову оплату для уникнення спаму (хоча підходять інші програми).

Альтернативою є вимога до відправника відповісти на якесь запитання, щоб довести, що він насправді людина. Це свого роду тест Тьюринга, який був реалізований у багатьох веб-службах, вимагаючи від користувача введення прихованого слова на зображенні. Ці тести називаються CAPTCHA (повністю автоматизований публічний тест Тьюринга для розрізнення комп'ютерів і людей).

Такий підхід можна особливо ефективно використовувати для уникнення вихідний спаму, тобто запобігання зловживанню спамерами безкоштовними постачальниками послуг електронної пошти, такими як Hotmail або Gmail.

Третій підхід вимагає, щоб машина-відправник вирішила якусь обчислювально дорогу проблему, створюючи затримку і, таким чином, не дозволяючи спамерам надсилати мільйони повідомлень на день. Цей підхід є, безумовно, менш дратівливим із запропонованих методів поштової доставки, і, отже, найпопулярнішим.

Одноразові адреси

Одноразові адреси є технікою, яка використовується для запобігання спаму від користувача. Це не сама система фільтрації, а спосіб уникнути спамерів, щоб дізнатися нашу адресу. Щоб зібрати адреси електронної пошти, спамери сканують Інтернет, шукаючи адреси в Інтернеті, сторінки, форуми або групи Usenet. Якщо ми не публікуємо свою адресу в Інтернеті, ми можемо бути більш-менш захищені від спаму, але проблема полягає в тому, що ми хочемо зареєструватися на веб-сторінці чи в Інтернет-сервісі, і нам потрібно заповнити свою адресу електронної пошти у формі .

Більшість сайтів заявляють, що вони не використовуватимуть цю інформацію для надсилання спаму, але ми не можемо бути впевнені, і часто адреса потрапляє до списку, який продається третім компаніям і використовується для надсилання комерційних електронних листів. Крім того, до цих сайтів можуть отримати доступ хакери з метою збору дійсних (і цінних) адрес. Щоб уникнути цієї проблеми, ми можемо використовувати одноразові адреси електронної пошти. Замість того, щоб дозволяти користувачеві готувати власні одноразові адреси, йому

можна надати автоматичну систему для керування ними, як інфраструктура каналів АТТ. Адреси є тимчасовими обліковими записами, які користувач може використовувати для реєстрації у веб-службах. Усі повідомлення, надіслані на одноразову адресу, перенаправляються до нашого постійного безпечного облікового запису протягом налаштованого періоду часу. Коли тимчасова адреса більше не потрібна, вона видаляється, тому, навіть якщо цей обліковий запис отримує спам, він не перенаправляється.

Спільна фільтрація

Спільна фільтрація — це розподілений підхід до фільтрації спаму. Замість того, щоб кожен користувач мав власний фільтр, ціла спільнота працює разом. Використовуючи цю техніку, кожен користувач ділиться своїми судженнями про те, що є спамом, а що ні, з іншими користувачами. Мережі спільної фільтрації використовують проблему деяких користувачів, які отримують спам, щоб створювати кращі фільтри для тих, хто ще не отримував ці спам повідомлення.

Коли група користувачів в одному домені позначає електронний лист від спільного відправника як спам, система може використовувати інформацію в цих електронних листах, щоб навчитися класифікувати ці конкретні електронні листи, щоб інші користувачі в домені не отримували їх. Слабкість цього підходу полягає в тому, що те, що для когось є спамом, для іншого може бути законним вмістом. Ці спільні фільтри спаму не можуть бути більш точними, ніж особистий фільтр на стороні клієнта, але це чудовий варіант для фільтрації на стороні сервера. Іншим недоліком цього підходу є те, що спамери вносять невеликі варіації в повідомлення, не дозволяючи іншим користувачем ідентифікувати новий майбутній спам-лист як близьку варіацію одного одержувача раніше.

Пастки для приманки та електронної пошти

Відомо, що спамери зловживають такими вразливими системами, як відкриті ретранслятори електронної пошти та публічні відкриті проксі-сервери. Щоб виявити спам, деякі адміністратори створили програми honeypot, які імітують такі вразливі системи. Існування таких підроблених систем робить використання відкритих ретрансляторів більш ризикованим для спамерів і відкритих проксі для

розсилки спаму. Honeypotting — це поширена техніка, яка використовується системними адміністраторами для виявлення хакерських дій на їхніх серверах. Вони створюють підроблені вразливі сервери, щоб хакери їх ламали, захищаючи справжні сервери. Оскільки термін honeypotting більше підходить для середовищ безпеки, терміни «перехоплення електронної пошти» або «перехоплення спаму» можна використовувати замість посилань на ці методи, коли вони застосовуються для запобігання спаму. Спам-пастки можна використовувати для збору екземплярів спам-повідомлень із збереженням свіжої колекції спамерських методів (і кращої навчальної колекції в класифікаторах на основі навчання), для створення та розгортання оновлених правил фільтрації в евристичних фільтрах і для завчасного виявлення нових спам-атак , уникаючи їх досягнення, наприклад, корпоративної мережі зокрема.

Фільтри на основі вмісту

Фільтри на основі вмісту засновані на аналізі вмісту електронних листів. Ці фільтри можуть бути створеними вручну правилами, також відомими як евристичні фільтри, або отриманими за допомогою алгоритмів машинного навчання. Обидва підходи сьогодні широко використовуються у фільтрах спаму, оскільки вони можуть бути дуже точними, коли їх правильно налаштовано, і вони будуть детально проаналізовані в наступному розділі.

2.3.2 Фільтрація спаму на основі вмісту

Серед технічних заходів боротьби зі спамом одним із найпопулярніших є контентна фільтрація. Спам-фільтри, які аналізують вміст повідомлень і на основі цього приймають рішення, поширилися серед користувачів Інтернету, починаючи від окремих користувачів на домашніх персональних комп’ютерах і закінчуючи великими корпоративними мережами. Успіх фільтрів, заснованих на вмісті, настільки великий, що спамери здійснюють дедалі складніші атаки, щоб уникнути їх і досягти поштових скриньок користувачів. Евристична фільтрація важлива з історичних причин, хоча найпопулярніші сучасні евристичні фільтри мають певний компонент навчання. Фільтрування на основі навчання є основною тенденцією в цій галузі, можливість вчитися на прикладах спаму та легітимних

повідомлень дає цим фільтрам повну силу для персоналізованого виявлення спаму. Останні TREC конкурсні оцінки підкреслили важливість сімейства фільтрів на основі навчання, які використовують алгоритми стиснення; вони отримали найкращі результати з точки зору ефективності, тому заслуговують окремого розділу.

Евристична фільтрація

Починаючи з перших спам-повідомлень, користувачі (які водночас були своїми власними «адміністраторами мережі») мають закодовані правила або евристики, щоб відокремлювати спам від своїх легітимних повідомлень і уникати читання першого . Евристичний фільтр на основі вмісту – це набір закодованих вручну правил, які аналізують вміст повідомлення та класифікують його як спам або законне. Наприклад, правило може виглядати так (1.1)

$$\text{if}(\text{P`Viagra'} \in \text{M})\text{or}(\text{`VIAGRA'} \in \text{M})\text{then class}(\text{M}) = \text{spam} \quad (1.1)$$

Це правило означає, що якщо будь-яке зі слів «Viagra» або «VIAGRA» (які насправді є рядками різних символів) зустрічається в повідомленні M, його слід класифікувати як спам. У той час як перші користувачі Інтернету часто були привілейованими адміністраторами користувачів і використовували такий тип правил у контексті складних сценаріїв і командних мов, більшість сучасних поштових клієнтів дозволяють писати такі правила за допомогою простих форм. Наприклад, відображається простий спам-фільтр Thunderbird. У цьому прикладі користувачі підготували фільтр під назвою «спам», який видаляє всі повідомлення, у яких у заголовку «Тема» зустрічається слово «**спам**».

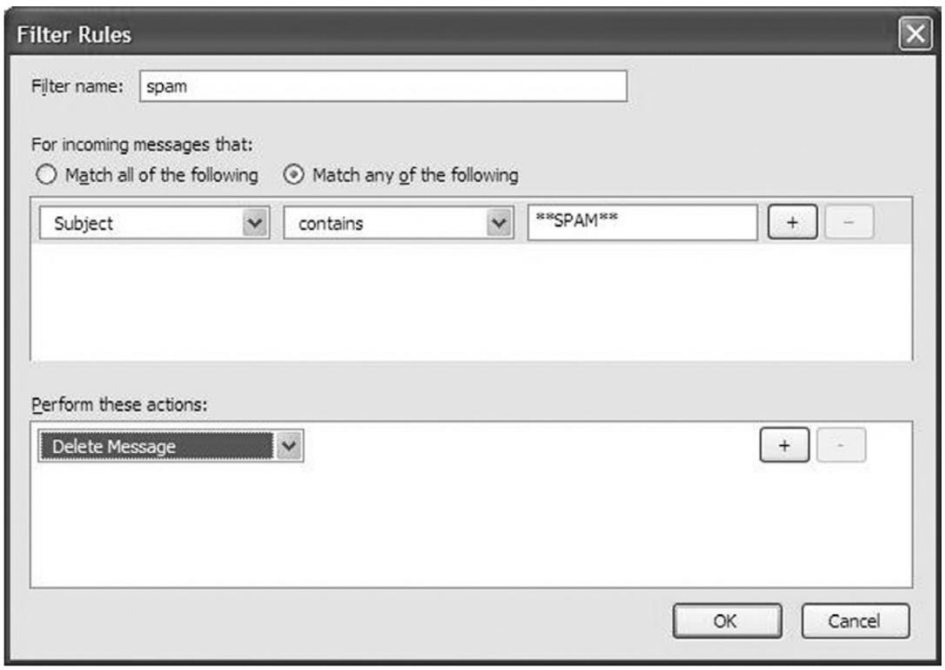

Рис 2.3. Складання правил у програмі Thunderbird

Однак ці утиліти фільтрації найчастіше використовуються для класифікації вхідних повідомлень у папки відповідно до відправника, теми чи списку розсилки, до якого вони належать. Їх також можна використовувати в поєднанні з рішенням фільтрації з поштового клієнта, який може позначати спам-повідомлення (наприклад, за допомогою рядка «**спам**» у темі або, будучи більш складним, додаючи спеціальний заголовок як, наприклад, звіт X-mail, який може включати простий тег або досить інформативний вихід із рівною оцінкою), який пізніше буде оброблено поштовим клієнтом шляхом застосування відповідних фільтрів і виконання бажаної дії. Розумно надсилати повідомлення, позначені як спам, до папки карантину, щоб уникнути помилкових спрацьовувань (легітимні повідомлення, класифіковані як спам). Має бути зрозуміло, що підтримка ефективного набору правил може бути досить трудомісткою роботою. Спам-повідомлення включають пропозиції аптечних товарів, порнорекламу, небажані позики, рекомендації щодо акцій та багато інших типів повідомлень. Не тільки їх зміст, але й стиль постійно змінюється. Насправді, важко знайти повідомлення, в якому б слово «» зустрічалося без змін (крім законних!). Іншими словами, є чимало технічних експертів, які дуже віддані тому, щоб фільтр вийшов з ладу: спамери. Ось чому фільтрація спаму вважається проблемою «змагальної класифікації». Ні

сучасний мережевий адміністратор, ні навіть просунутий користувач не будуть писати власні правила фільтрації спаму. Натомість список корисних правил може підтримуватися спільнотою досвідчених користувачів і адміністраторів, як це було зроблено в дуже популярному рішенні з відкритим вихідним кодом SpamAssassin або в комерційній службі Brightmail, наданій корпорацією Symantec.

2.3.3 Способи розпізнавання за допомогою штучного інтелекту

За останні 9 років виникла нова парадигма фільтрації спаму на основі вмісту. Байєсовські фільтри, або, загалом, фільтри на основі навчання, мають здатність вивчати потік електронної пошти та покращувати свою продуктивність з часом, оскільки вони можуть адаптуватися до фактичного спаму та легітимних електронних листів, які отримує конкретний користувач. Їхній вражаючий успіх демонструє глибокий вплив, який вони мали на спам-електронну пошту, оскільки спамерам доводиться дорого змінювати свої методи, щоб уникнути їх. Фільтри на основі навчання — це сучасний рівень фільтрації електронної пошти та головна проблема цього розділу.

Фільтрування спаму є прикладом більш загального завдання класифікації тексту під назвою Text Categorization. Категоризація тексту — це віднесення текстових документів до набору заздалегідь визначених класів. Важливо відзначити, що класи вже існують, а не генеруються на льоту (що відповідає завданням Text Clustering). Основним застосуванням категоризації тексту є присвоєння текстовим документам предметних класів. Тематичні класи можуть бути категоріями веб-каталогів (як у Yahoo!), тематичні дескриптори в бібліотеках (наприклад, предметні рубрики Бібліотеки Конгресу або, в окремих областях, медичні предметні рубрикиНаціональною медичною бібліотекою або дескрипторами Асоціації обчислювальної техніки ACM Computing Classification System, які використовуються в самій цифровій бібліотеці ACM), папки особистої електронної пошти тощо. Документами можуть бути веб-сайти чи сторінки, книги, наукові статті, новини, повідомлення електронної пошти тощо.

Категоризацію тексту можна виконати вручну або автоматично. Перший метод використовується в бібліотеках, де експерти-каталоги сканують нові книги

та журнали, щоб проіндексувати їх відповідно до використовуваної системи класифікації. Наприклад, у Національній медичній бібліотеці працює близько 95 штатних каталогізаторів, щоб індексувати наукові та новинні статті, що поширюються через MEDLINE. Очевидно, що це трудомістке та фінансове завдання, а кількість публікацій постійно зростає.

Зростаюча доступність даних з тегами дозволила застосувати до завдання методи машинного навчання. Замість того, щоб класифікувати документи вручну або створювати систему класифікації вручну, можна автоматично створити класифікатор за допомогою алгоритму машинного навчання на колекції класифікованих вручну документів, представлених належним чином. Адміністратору чи експерту не потрібно писати фільтр, але дозвольте алгоритму вивчити властивості документа, які роблять його придатним для кожного класу. Таким чином, традиційна експертна система «вузьке місце отримання знань» усувається, оскільки експерт може продовжувати робити те, що він або вона вміє найкраще (тобто, фактично, класифікувати), а система буде вчитися на його рішеннях.

Фільтрування спаму можна вважати прикладом (автоматизованої) категоризації тексту, у якому документами для класифікації є повідомлення електронної пошти користувача, а класами є спам і законна електронна пошта. Це можна вважати легким, оскільки це задача одного класу. Однак він демонструє особливі властивості, що робить його дуже складним завданням:

1. Як спам, так і додатковий клас (легітимна електронна пошта) не є тематичними, тобто вони можуть містити повідомлення, що стосуються кількох тем або тем. Наприклад, станом на 2021 рік 37% спаму становили листи «швидкого збагачення», 25% — порнографічна реклама, а 18% — пропозиції програмного забезпечення. Решта спаму включала рекламні оголошення веб-сайтів, інвестиційні пропозиції, (підроблені) товари для здоров'я, конкурси, свята та інше. Крім того, деякі типи спаму можуть збігатися з легітимними повідомленнями, як комерційними, так і зі списків розсилки. Хоча відсотки, безумовно, змінилися (пропозиції щодо здоров'я

та інвестицій зараз найбільш популярні), це демонструє, що поточні системи ТС, які спираються на слова та ознаки для класифікації, можуть мати серйозні проблеми, оскільки клас спаму дуже фрагментований.

2. Розповсюдження спаму постійно змінюється і часто спотворене. З одного боку, Класифікатори машинного навчання очікують такого ж розподілу класів, з якого вони вчилися; будь-яка зміна розподілу може вплинути на продуктивність класифікатора. З іншого боку, спотворені розподіли, такі як 90% спаму (досягнуті в 2020 році), можуть створити алгоритм навчання для створення тривіального акцептора, тобто класифікатора, який завжди класифікує повідомлення як спам. Це пов’язано з тим, що алгоритми Machine Leaning намагаються мінімізувати помилку або максимізувати точність, і тоді тривіальний акцептор має точність на 90%. І що ще гірше, рівень спаму може відрізнятися від місця до місця, від компанії до компанії та від людини до людини; у такій ситуації дуже важко побудувати придатний для всіх класифікатор.

3. Як і багато інших завдань класифікації, фільтрація спаму має незбалансовані витрати на неправильну класифікацію. Іншими словами, види помилок, які робить фільтр, є значними. Жоден користувач не буде задоволений фільтром, який вловлює 99% спаму, але видаляє легітимне повідомлення раз на день. Це пояснюється тим, що хибні спрацьовування (законні повідомлення, класифіковані як спам) коштують набагато дорожче, ніж хибні негативи (повідомлення зі спамом, класифіковані як законні, і, таким чином, потрапляють до папки "Вхідні"). Але знову ж таки, незрозуміло, яка пропорція правильна: користувач може прийняти фільтр, який робить хибний позитивний результат на 100 помилкових негативних результатів або на 1000 тощо.

Це залежить від смаку користувача, кількості спаму, який він або вона отримує, місця, де він або

вона живе, типу облікового запису електронної пошти (робоча чи особиста) тощо.

4. Можливо, найскладнішою проблемою з класифікацією спаму є те, що це приклад змагальної класифікації. Змагальна класифікаційна задача — це така, у якій існує супротивник, який змінює дані, що надходять до класифікатора, щоб зробити його

невдалим. Фільтрація спаму є, мабуть, найбільш репрезентативним прикладом змагальної класифікації, серед багатьох інших, таких як виявлення комп'ютерних вторгнень, виявлення шахрайства, боротьби з тероризмом або багато в чому пов'язане: виявлення веб-спаму. У цьому останньому завданні система повинна виявити, які веб- майстри маніпулюють сторінками та посиланнями, щоб підвищити свій рейтинг, після зворотного проектування алгоритму рейтингу. Хоча термін спам походить із сфери електронної пошти, він настільки поширений, що його використовують для багатьох інших проблем шахрайства: мобільний спам, спам у блогах, «спам» (спам через миттєві повідомлення), «плювок» (спам через Інтернет-телефонію), тощо. Що стосується фільтрації спаму, спамери незабаром навчилися їх обманювати, вставляючи в електронні листи слова «не спам», розділяючи «спамові» слова, як-от «Віагра», помилковими знаками пунктуації тощо. Щойно фільтри спаму були змінені для виявлення цих прийомів, спамери почали використовувати нові.

Ці проблеми роблять фільтрацію спаму дуже незвичайним випадком автоматичної категоризації тексту. Зважаючи на це, стандартна структура системи автоматизованої текстової категоризації підходить для проблеми фільтрації спаму.

2.3.4 Спам- та URLF-аналітики

Спам- та URLF-аналітики – спеціально навчений спеціаліст з кібербезпеки який займається фільтруванням посилань сайтів, для уникнення переходу кінцевого користувача на інфікований або заздалегідь шкідливий сайт. Фільтрування відбувається як автоматично так і вручну за допомогою внутрішніх сервісів компанії (якщо треба максимально швидко розблокувати випадково заблоковане посилання).

Почнемо з базового пояснення фільтрації URL-адрес. URL-адреси функціонують як веб-адреси та посилаються на веб-ресурс із зазначенням його розташування в комп'ютерній мережі. З різних причин певні URL-адреси можуть становити більший ризик, ніж інші, а деякі «безпечні» веб-сайти одного дня можуть бути скомпрометовані.

Фільтрування URL-адрес — це спосіб «блокування» завантаження певних URL-адрес у мережі компанії. Якщо співробітник спробує відвідати цю URL-адресу, ввівши її вручну або натиснувши посилання в пошуковій системі, він буде перенаправлений на сторінку зі сповіщенням про те, що цей вміст заблоковано.

Фільтрування URL-адрес базується на фільтрації баз даних, які класифікують URL-адреси за темами; кожна тема в цій системі «заблокована» або «дозволена». Ця система була в основному розроблена з міркувань продуктивності, дозволяючи роботодавцям блокувати веб-сайти, які були невідповідними для роботи або які були розроблені для марнування часу.

Адміністратори можуть створювати списки блокування для окремих URL-адрес, блокуючи конкретні веб-сайти, які, на їхню думку, є небезпечними чи шкідливими. У більш широкому плані адміністратори можуть блокувати цілі категорії URL-адрес, додаючи до списку блокування цілі групи веб-сайтів одночасно.

Існує кілька ключових переваг фільтрації URL-адрес, зокрема:

- Мінімізація ризиків безпеки. Перша і найпомітніша перевага полягає в тому, що ви зменшите вразливі місця в системі безпеки, з якими стикається ваша організація. Ви будете менш сприйнятливі до загроз в Інтернеті.
- Покращення відповідності. Ви також можете уникнути зобов'язань і залишатися сумісними. Залежно від вашої галузі вам, можливо, доведеться дотримуватися суворіших стандартів кібербезпеки та операцій.
- Підвищення продуктивності. Як додатковий бонус, фільтрування URL-адрес може допомогти вам контролювати, які сайти відвідують ваші співробітники, що зрештою призведе до підвищення продуктивності в цілому.

Ви також можете розглянути можливість впровадження фільтрації DNS. DNS-фільтрація та фільтрація URL-адрес – це обидва типи веб-фільтрації, але вони виконують різні окремі функції. DNS-фільтрація блокує веб-вміст на основі DNS-запитів, а не конкретних URL-адрес; іншими словами, це дозволяє блокувати цілі домени.

Більшість організацій намагаються використовувати комбінацію фільтрації URL-адрес і фільтрації DNS, щоб отримати вигоду з переваг обох.

До недавнього часу фільтрування URL-адрес було майже повністю ручним процесом. Адміністратори ретельно вибирали список категорій URL-адрес і конкретних URL-адрес для блокування та додавали нові, коли отримували більше інформації. Але зараз багато служб фільтрації URL-адрес використовують машинне навчання, щоб дізнаватися про нові загрози, визначати можливості для вдосконалення та автоматизувати розгортання нових фільтрів.

Фільтрування URL-адрес — потужний спосіб заблокувати доступ до певних веб-сторінок, але це не ідеальна система й не забезпечить організації комплексний захист. Натомість фільтрування URL-адрес найкраще використовувати як одну з кількох функцій безпеки, призначених для захисту від загроз в Інтернеті. Наприклад, фішингові сайти можна виявити за допомогою IPS або ізольованого програмного середовища, але відсутність зв’язку між вашим ізольованим програмним середовищем, IPS і системами фільтрації URL-адрес може запропонувати вам неповний захист.

Далі буде розглянутий процес роботи типового URLF/Spam-аналітика:

Зазвичай такі спеціалісти працюють у двох сервісах:

1) CRM система. У нашому випадку це Jira від Atlassian та система Salesforce Вони дозволяють безпосередньо контактувати між собою клієнта і аналітика. Якщо, наприклад, посилання заблоковано FP, то перший створює у цій системі тікет, описавши проблему та вказавши посилання яке треба пофіксити. У свою чергу аналітик дивиться та аналізує за допомогою різних сервісів та тулзів чи дійсно це FP та при потребі розблоковує цей лінк.

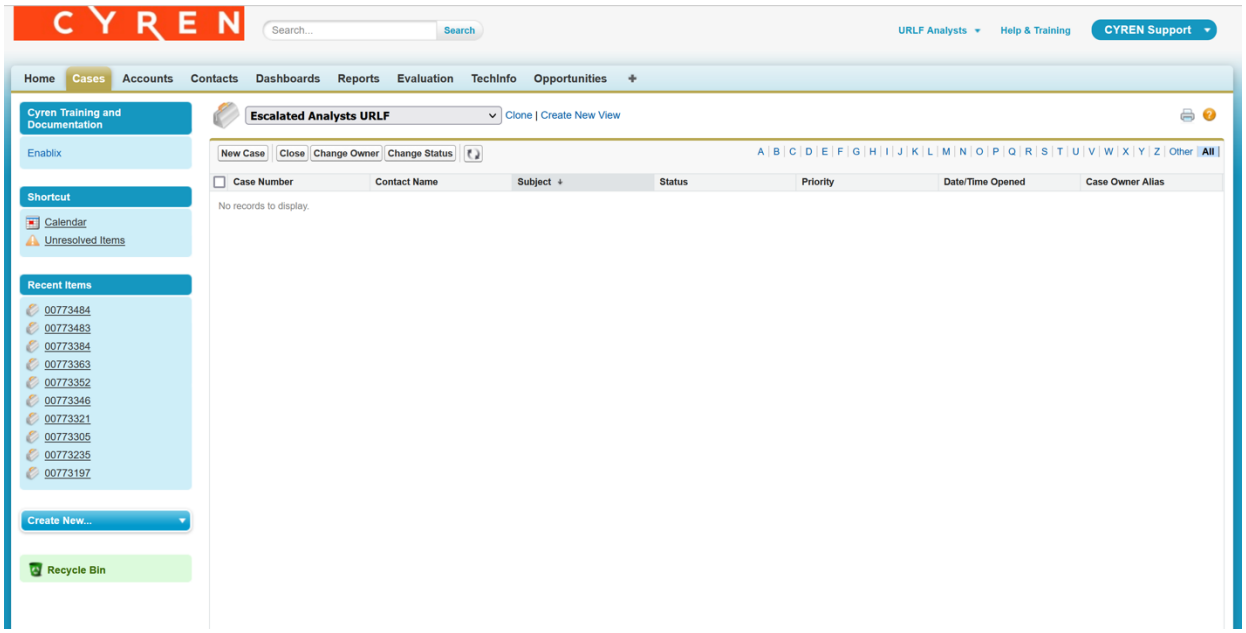

Рис 2.5 Інтерфейс CRM-системи Salesforce

2) Інша система в якій працює URLF-аналітик це Miscat Station. Вона створена для корегування категорій посилань та надавання їм нових категорій. Всього їх є 168 (18 security-категорій(spam, phishing, spyware…), 38 parental control-категорій(pornography, nude…), 102 common(business, computers, education…) та internal(для класифікації всередині компанії))

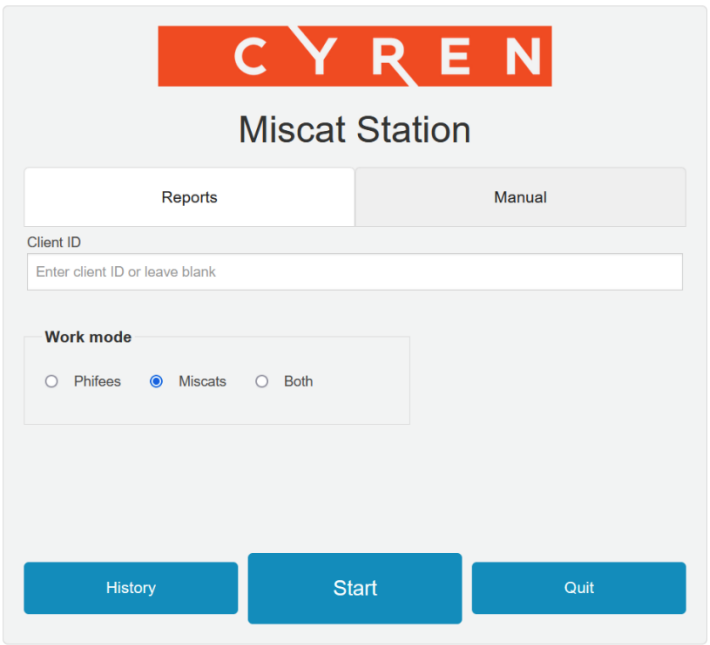

Рис. 2.6. Стартова сторінка Miscat Station

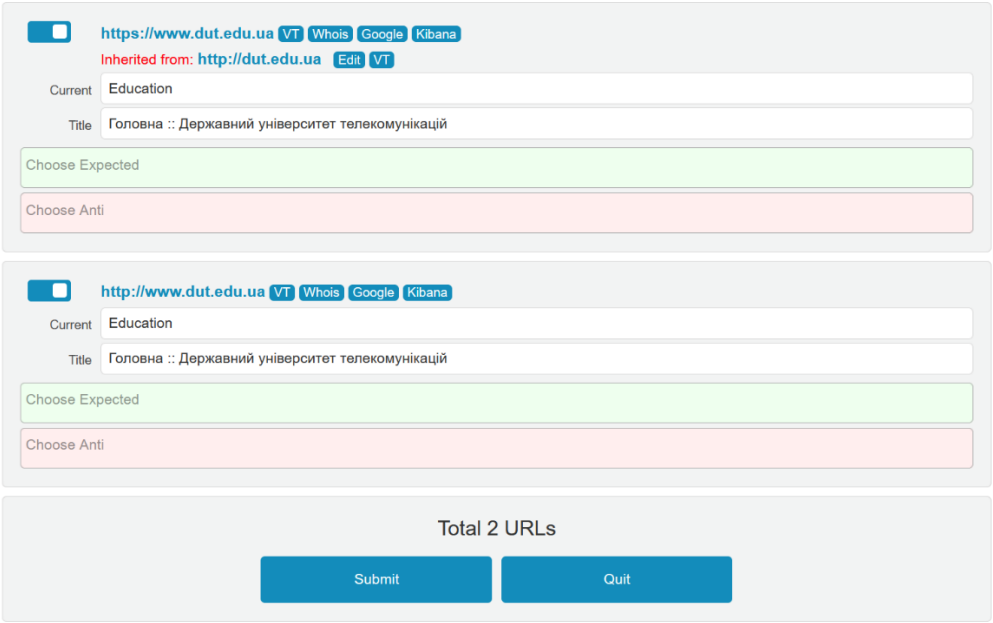

Рис. 2.7. Приклад категоризації сторінки Державного Університету Телекомунікацій

2.4. Порівняння з іншими антиспам системами

2.4.1. Spam Assassin

«Хоча легко перемогти одного адміністратора мережі, важче перемогти спільноту». Це дух одного з найпоширеніших евристичних фільтраційних рішень: SpamAssassin. Його особливість полягає в тому що це open-source проект, тому він є безкоштовним та будь-хто може додавати правила або підлаштовувати його під себе. Він є одним із найстаріших фільтрів, які все ще діють на ринку, і його головною особливістю є вражаючий набір правил або евристик, створених десятками адміністраторів і перевірених проектом.

Поточна версія (3.2) має набір правил (названиих «тести» в SpamAssassin) містить 746 тестів. Деякі з них є адміністративними, а деякі з них не є справді «контентними», оскільки вони, наприклад, перевіряють адресу відправника чи IP-адресу за загальнодоступними білими списками. Наприклад, тест під назвою "RCVD_IN_DNSWL_HI" перевіряє, чи внесено відправника в білий список DNS. Звичайно, це механізм білого списку, і він майже не аналізує сам вміст повідомлення. З іншого боку, правило під назвою «FS_LOW_RATES» перевіряє, чи містить поле «Тема» слова «низькі ставки», які дуже популярні в спам-повідомленнях, пов’язаних із кредитами чи іпотекою. Багато тестів SpamAssassin

вирішують варіативність введення за допомогою досить складних регулярних виразів.

Типове правило зіставлення вмісту SpamAssassin має структуру, наведену в наступному прикладі:

```
body DEMONSTRATION_RULE /test/
score DEMONSTRATION_RULE 0.1
describe DEMONSTRATION_RULE This is a simple test rule
```

Правило починається з рядка, який описує тест, який потрібно виконати, продовжується рядком, який представляє оцінку, і має останній рядок для опису правила. Зразок назви правила – "DEMONSTRATION_RULE", і воно перевіряє (з урахуванням регістру) слово "test" у розділі тіла вхідного повідомлення електронної пошти. Якщо умова є

AREA TESTED	LOCALE	DESCRIPTION OF TEST	TEST NAME	DEFAULT SCORES *(local, net, with bayes, with bayes+net)*
header		Envelope sender listed in bl.open-whois.org.	DNS_FROM_OPENWHOIS	0 2.431 0 1.130
body		Provision for income taxes	DOS_PROVISION4	1.5
body		Report of financial income	DOS_REPORT_FIN_INC	0.5
body		Pump and dump stock spam	DOS_STOCK_CDYV_GENERIC	2.5
uri		Found an asterisk in a URI	DOS_URI_ASTERISK	1
header		Subject =~ /\bhoodia\b/i	DRUGS_HDIA	2.529 2.501 2.483 2.697
body		Add / Gain inches	FB_ADD_INCHES	2.999 2.999 2.620 2.131
body		It's almost sex, but not!	FB_ALMOST_SEX	3.099 3.096 2.841 2.110

Рис. 2.8. Зразок правил перевірки або фільтрації у SpamAssassin

Область, що перевіряється, може бути заголовком, основним текстом тощо, і кожен тест забезпечується одним або кількома балами, які можна використовувати для встановлення відповідного порогу та зміни чутливості фільтра.

Якщо умову задоволено, тобто слово зустрічається, тоді оцінка 0,1 додається до загальної оцінки повідомлення. Оцінка повідомлення може бути збільшена за іншими правилами, і повідомлення буде позначено як спам, якщо загальна оцінка перевищить порогове значення, встановлене вручну або автоматично. Звичайно, чим вищий бал правила, тим більше воно впливає на рішення позначити повідомлення як спам.

Тести, які виконуються в правилах, можуть охоплювати всі частини повідомлення та вимагати попередньої обробки чи ні. Наприклад, якщо правило починається з "заголовка", перевірятимуться лише заголовки:

заголовок DEMONSTRATION_SUBJECT Тема =- /test/

Насправді символи «=~» перед тестом разом зі словом «Тема» означають, що тестуватиметься лише заголовок теми. У цьому випадку ім’я поля теми нечутливе до регістру.

Виконані тести дозволяють складати складні вирази, написані за допомогою синтаксису регулярних виразів Perl (Regex). Трохи складнішим прикладом може бути:

заголовок DEMONSTRATION_SUBJECT Тема =- /\btest\b/i

У цьому прикладі вираз «/ \btest\b/i» означає, що слово «test» шукатиметься як одне слово (а не як частина інших, як-от «testing»), оскільки воно починається й закінчується на знак розриву слова '\b', і тест буде нечутливим до регістру через кінцевий знак '/i'.

Вручну призначати бали правилам не дуже гарна ідея, оскільки кодувальник правил повинен мати точне та загальне уявлення про всі бали в усіх інших правилах. Замість цього потрібен автоматизований метод, який повинен мати можливість переглядати всі бали та набір тестових повідомлень і обчислювати бали, які мінімізують помилку фільтра. У версіях 2.x оцінки правил призначалися за допомогою генетичного алгоритму, тоді як у (поточних) версіях 3.x оцінки призначалися за допомогою нейронної мережі, навченої зворотному розповсюдженню помилок (персептрон). Обидві системи намагаються оптимізувати ефективність правил, які виконуються з точки зору мінімізації кількості помилкових спрацьовувань і помилково негативних результатів.

Оцінки оптимізовано на основі реальних прикладів, наданих волонтерами. Група SpamAssassin фактично випустила корпус спам-повідомлень під назвою SpamAssassin Public Corpus. Цей корпус включає 6047 повідомлень, з коефіцієнтом спаму ~31%.

2.4.2 Symantec BrightMail Solution

Кілька років тому Brightmail виник як постачальник рішень для захисту від спаму на основі оригінальної бізнес-моделі на ринку захисту від спаму. Замість того, щоб надати кінцеву програмну програму з можливостями фільтрації, вона зосередилася більше на сервісі та взяла модель роботи від антивірусних корпорацій: аналітики 24 години на добу працюють над новими атаками та часте надання нових правил захисту. Модель вдалася, і 21 червня 2004 року корпорація Symantec придбала компанію Brightmail Incorporated разом із її рішенням і клієнтами. Зараз Symantec стверджує, що Brightmail Anti-spam захищає понад 500 мільйонів користувачів і фільтрує понад 15% електронних листів у всьому світі.

Рішення Brightmail Anti-spam працює на шлюзі клієнтів, скануючи вхідні повідомлення до корпорації та вирішуючи, чи є вони спамом чи ні. Рішення приймається на основі набору правил фільтрації, наданих експертами в операційному центрі Symantec під назвою BLOC (Brightmail Logistics Operations Center).

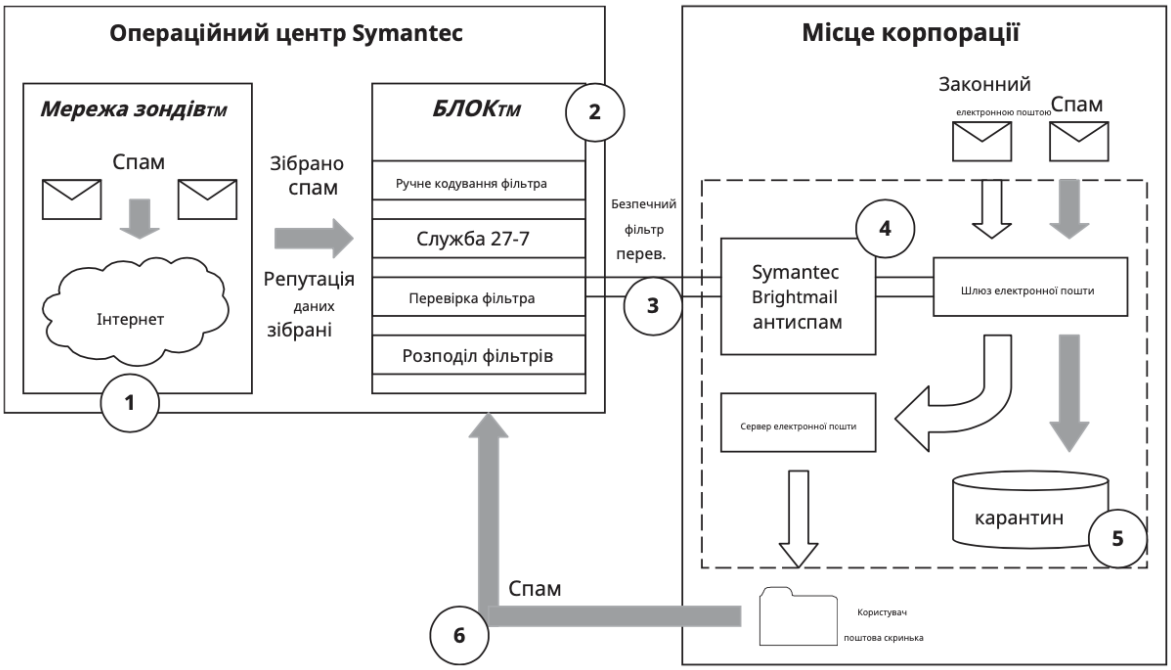

Рис 2.10. Операційна структура рішення Symantec Brightmail Anti-spam.

Цифри в кружечках позначають описані процеси

1. Probe Network (TM) — це мережа підроблених скриньок електронної пошти («пасток для спаму» або «приманок»), створених лише з метою отримання

спаму. Ці адреси електронної пошти можуть бути зібрані лише автоматично, як спамери і, як наслідок, вони можуть отримувати лише спам. Зібраний спам надсилається до BLOC.

2. У BLOC групи експертів і, нещодавно, автоматичні засоби аналізу контенту

створюють, перевіряють і розповсюджують антиспам-фільтри серед корпоративних клієнтів Symantec.

3. Кожні 10 хвилин програмне забезпечення Symantec завантажує найновішу версію фільтрів із BLOC, щоб підтримувати їх якомога оновленішими. 4. Програмне забезпечення фільтрує вхідні повідомлення за допомогою фільтрів Symantec і налаштованих користувачем фільтрів.

5. Адміністратор електронної пошти визначає найбільш прийнятний режим адміністрування для відфільтрованої електронної пошти. Найчастіше електронний лист (виявлений як спам) зберігається в карантині, де користувачі можуть перевірити, чи фільтр помилково класифікував законне повідомлення як спам (хибний результат).

6. Користувачі можуть повідомляти Symantec про непомічений спам для подальшого аналізу.

Процеси в BLOC колись були ручними, але постійно зростаюча кількість спам- атак поступово унеможливила підхід до створення фільтрів як до рукотворного завдання. Останнім часом експерти зі спаму в BLOC фактично змінили свою роль на адаптери фільтрів і тюнери, оскільки фільтри створюються за допомогою автоматичних інструментів на основі навчання.

2.5 Основні плюси та мінуси Cyren Email Security Engine

Як і будь-який продукт, Cyren Email Security Engine, має свої недоліки та переваги.

Плюси:

- хмарна система. Актуальність баз та списків будь де та будь коли, не потребує адаптації чи складної інсталяції;

- просунутий, створений для адміністрування електронної пошти та облегшення досвіду користовача;

- пропонує детальний чорний список за IP-адресою, діапазоном IP-адрес, країною та DNS, Використовує серверну базу даних аналізу загроз, щоб знаходити та зупиняти нові та нові загрози;

- захист від хибного застосування. Електронна пошта пройшла через 23 різні фільтри, перш ніж потрапити до папки "Вхідні";

- універсальність. Підтримує кілька мов, добре для міжнародного використання;

- може переглядати поточну статистику електронних листів, як-от обсяг, коефіцієнт спаму та кількість заблокованих спроб спаму. Адміністратори можуть переглядати елементи на карантині, що мінімізує перешкоди для кінцевих користувачів;

- може аналізувати спам, який приходить, ШІ щоб система могла навчитися його ідентифікувати в майбутньому;

- дозволяє налаштування за допомогою налаштувань і сценаріїв ;

- не потребує архітектурних змін для встановлення;

- Інтеграція з Microsoft 365 і Google Workspace

- Створений для масштабування, може підтримувати великі середовища з кількома клієнтами або корпоративні мережі з кількома доменами, розташуваннями та поштовими серверами;

- допомагає виявляти та зупиняти фішингові атаки, а також зловмисне програмне забезпечення на основі файлів;

Мінуси:

- Не безкоштовно назавжди

- Дорого в порівнянні з аналогічними засобами

- Плагін Outlook може спричинити повільне відкриття Outlook або збій

- Створений для великих організацій, не ідеальний для домашніх користувачі.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КОРИСТУВАЧІВ КОРПОРАТИВНИХ МЕРЕЖ ВІД СПАМ АТАК

Як і інші небезпечні тактики соціальної інженерії та шкідливого ПЗ, спам атаки в основному спрямовані на використання людського фактору. Організації можуть і повинні займати проактивну позицію проти спаму, але й кінцеві користувачі повинні бути пильними та слідкувати за трендами і своєю безпекою в Інтернеті.

3.1 Рекомендації для фахівців з кібербезпеки

Щоб зменшити вразливість вашого бізнесу до спамних атак, ви повинні визначити свої активи та ключових користувачів. Нам потрібно проаналізувати можливості реалізації різних типів атак і способи їх реалізації. Наприклад, ресурси (електронна пошта, месенджери, соціальні мережі), де можна отримати конфіденційну інформацію всередині компанії. Крім того, розраховуючи захист від спам атак, слід враховувати не тільки своїх співробітників, але й клієнтів, які можуть стати жертвами атаки. Необхідно визначити, які працівники знаходяться в групі ризику (топ-менеджери, фінансові співробітники, IT-адміністратори).

Адміністраторам та Хелпдеску слід використовувати тільки ліцензійне програмне забезпечення та перевіряти оновлення для нього якомога частіше, для того щоб мінімізувати можливий виток інформації та використання експлойтів нульового дня. Окрім цього оновлення актуалізує бази даних шкідливих IP-адрес, білих та чорних списків, що дозволяє перевіряти листи навіть без підключення до мережі Інтернет.

Крім того, вам слід визначити всі веб-ресурси, які шахраї можуть зламати для розміщення спам сторінок. Одним із найкращих способів захистити свій бізнес є навчання фішингу і спам атакам. Переконайтеся, що ваші співробітники навчені використовувати найновішу тактику та поточні тенденції зловмисників – один із найкращих способів боротьби зі спам атаками. Важливо, щоб працівники компанії використовували надійні паролі. Протягом цього часу фахівці з кібербезпеки повинні стежити за списком зламаних облікових записів і паролів і заздалегідь

повідомляти користувачів про те, що їхні паролі потрібно змінити. Це особливо вірно, якщо обліковий запис користувача зламано. Cyren Email Security Engine дозволяє адміністраторам безпеки відстежувати статуси електронних листів, чи були вони прочитані чи проігноровані, подивитись репутацію відправника та чи є він в блеклісті. Таким чином ви можете побачити, скільки шкідливих електронних листів було відкрито та відпралено під час аналізу конкретної спам атаки. Крім того, співробітники повинні знати, як створювати надійні паролі для захисту своїх облікових записів. По можливості, багатофакторну аутентифікацію слід впроваджувати для всіх співробітників компанії. Співробітники повинні знати та відрізняти легітимні листи від шкідливих та не переходити по усіх посиланнях від невідомих відправників. Рекомендовано використовувати методи запобігання злому веб-додатків, атакам ботів, запобіганню шахрайству, а також використовувати спам-фільтри. Cyren Email Security Engine пропонує професіоналам унікальну можливість легко знаходити та блокувати електронні листи за допомогою однієї чи кількох найпоширеніших тенденцій спаму. Наприклад, враховуючи інформацію про заголовки електронних листів та найпоширеніші домени, що використовують зловмисники, можна провести швидкий пошук за всіма електронними листами користувачів, що надходили на протязі двох тижнів, та заблокувати їх.

3.2 Рекомендації для кінцевих користувачів

Незалежно від того, на що йдуть компанії, щоб захистити свій бренд і своїх клієнтів, кінцевий користувач завжди буде об'єктом атак спаму та соціальної інженерії. Так само, як і антивіруси повинні бути в курсі можливої атаки, споживачі теж мають володіти актуальною інформацією.

Користувачі можуть позначити електронний лист як спам, тим самим заблокувавши відправника, щоб уникнути спамних повідомлень і у інших ресіпієнтів. Ви можете видалити небажані листи вручну, але це не завадить спамерам надсилати вам більше небажаних листів у майбутньому. І це не захистить вас від вірусів чи інших типів зловмисного програмного забезпечення, прихованого

в небажаних електронних листах — для цього вам знадобиться засіб для видалення зловмисного програмного забезпечення.

Щоб ефективно блокувати спам, вам потрібно повідомити про нього, оскільки це допоможе вашому поштовому клієнту дізнатися, яку адресу електронної пошти блокувати та як фільтрувати спам у більш загальному плані.

Ось як повідомити про спам у пошті Gmail і Outlook:

Як повідомити про спам у Gmail:

1) Відкрийте Gmail.

2) Поставте прапорець на спамний лист, про який ви хочете повідомити.

3) Потім натисніть кнопку «Повідомити про спам» (піктограма «Зупинка») на панелі інструментів поштової скриньки.

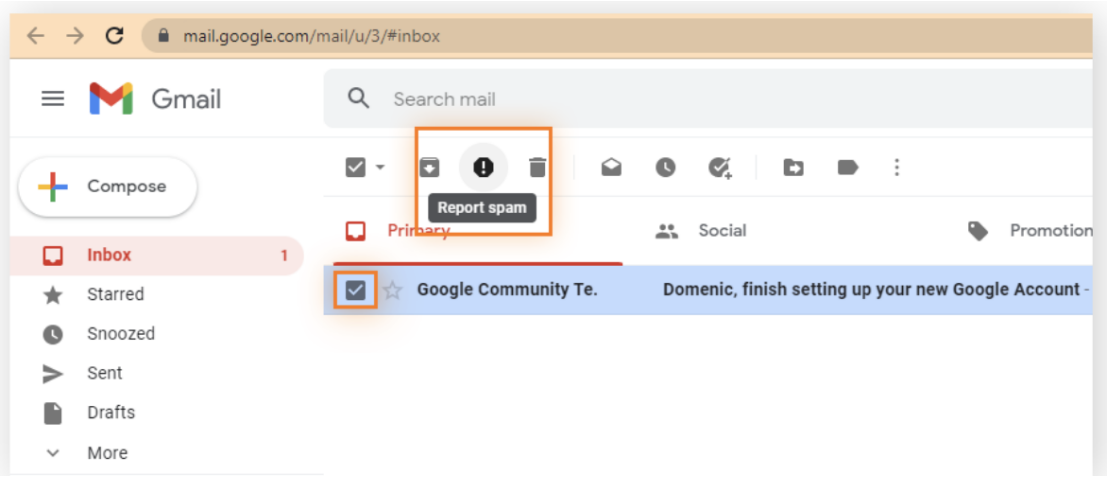

Рис 3.1. Спосіб репорту спаму у Gmail

Як повідомити про спам в Outlook:

1) Відкрийте Outlook.

2) Клацніть правою кнопкою миші спам, про який потрібно повідомити.

3) Перейдіть до параметрів безпеки та натисніть Позначити як небажане.

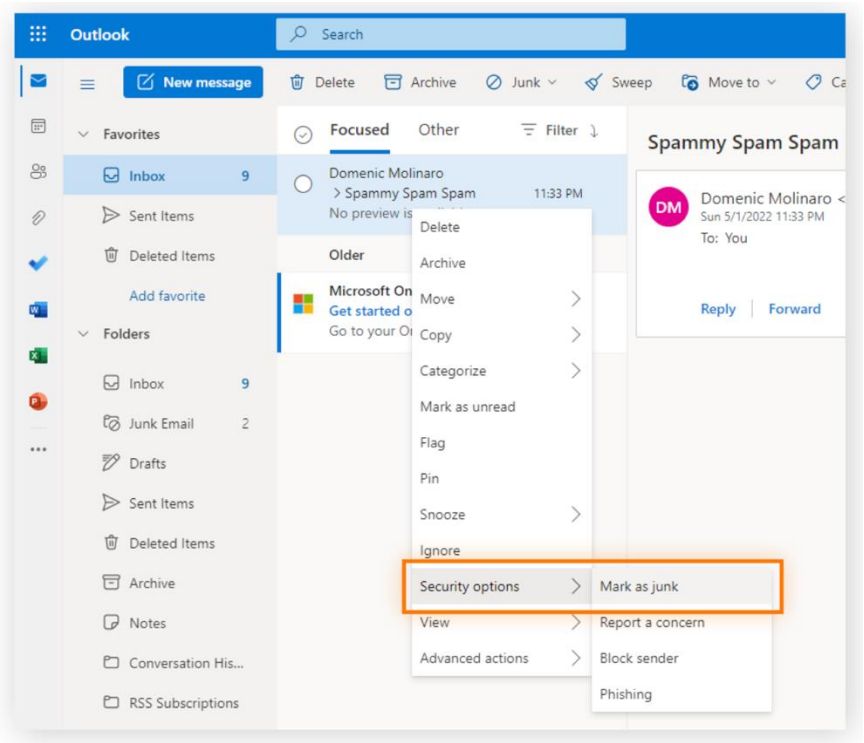

Рис 3.2. Спосіб репорту спаму в Outlook

Після того, як ви почнете навчати свою електронну пошту розпізнаванню та зупиненню спаму, навчіть себе самостійно виявляти фішингові листи Amazon та інший спам. Спамери можуть знати, як не потрапити під фільтри електронної пошти, але їм не вдасться обдурити добре навчене око.

Фільтруючи адреси деяких спам-листів, ви повинні прямо блокувати адреси електронної пошти, які є постійними, небезпечними або підробленими. І не забувайте повідомляти про будь-яке інтернет-шахрайство, на яке ви натрапляєте, як-от фішинг Apple ID та інші загрози.

Блокуйте спам-електронні адреси

Блокування небажаних електронних листів назавжди запобігає надходженню спаму на цю адресу електронної пошти, але будьте обережні, як ви це робите, оскільки відкриття деяких спам-листів може призвести до потоку небажаних листів з інших облікових записів спаму.

Змініть налаштування конфіденційності електронної пошти

Зупинити спамерів заповнювати вашу папку "Вхідні" небажаними небажаними електронними листами – це добре, але ще краще змінити

налаштування конфіденційності електронної пошти — і свої звички — щоб зменшити ризик спаму.

Завжди зберігайте свою електронну пошту максимально конфіденційною. Це означає бути обережним щодо людей і організацій, яким ви надаєте свою адресу. Використовуйте двофакторну автентифікацію, щоб ще більше захистити свою папку "Вхідні".

Ось як налаштувати параметри конфіденційності електронної пошти, щоб уникнути спаму та запобігти доступу рекламодавців та інших третіх осіб до вашої адреси.

Змініть налаштування Gmail

1) Відкрийте Gmail і натисніть значок свого облікового запису у верхньому правому куті.
2) Потім натисніть Керувати обліковим записом Google.

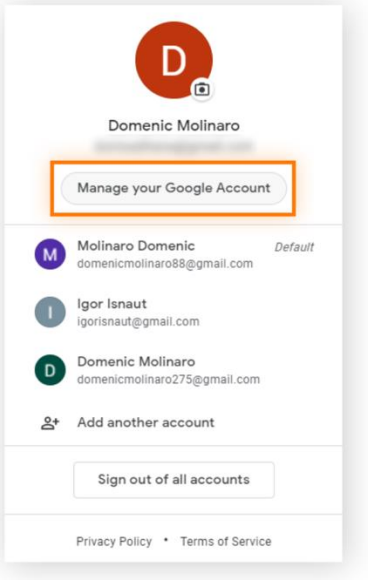

Рис 3.3. Управління акаунтами

3) Меню облікового запису Google

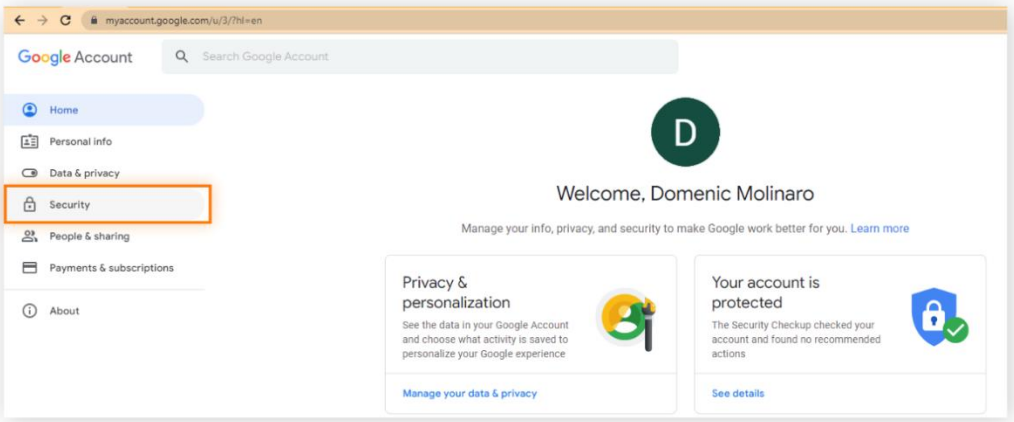

Рис 3.4. Налаштування акаунта

4) У лівому навігаційному меню натисніть Безпека.

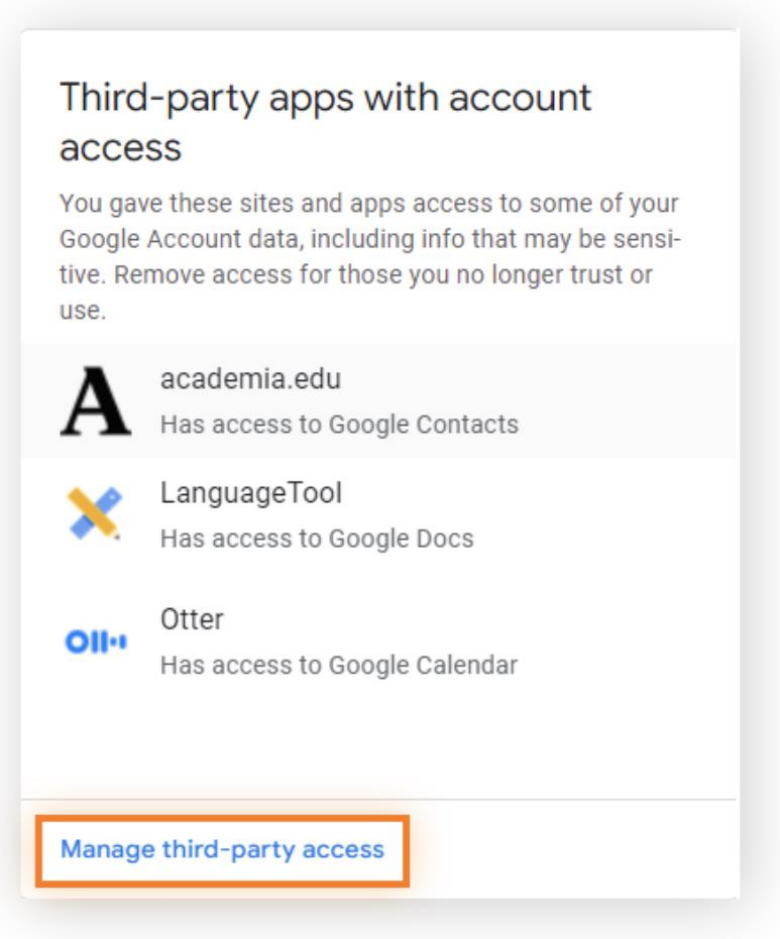

Рис 3.5. Інтерфейс «Безпека акаунту»

5) Виділення опції «Безпека» в розділі «Керування обліковим записом Google» у Gmail.

Перегляньте свої поточні налаштування та змініть ті, які потрібно оновити. Ми рекомендуємо скасувати доступ до вашого облікового запису для будь-яких третіх сторін, які надсилають вам небажаний спам.

Ще одна причина, чому ви можете отримувати спам, полягає в тому, що ви дійсно підписалися на його отримання — свідомо чи ні. Видалення вашої адреси електронної пошти зі списків підписки на спам – це чудовий спосіб розрідити сміття у вашій папці "Вхідні".

Для початку відкрийте свою електронну пошту та введіть скасування підписки в рядку пошуку електронної пошти. Це призведе до появи всіх інформаційних бюлетенів і списків розсилки, на які ви можете скасувати підписку, оскільки всі ці електронні листи матимуть варіанти скасування підписки, приховані в нижній частині їхніх електронних кампаній.

Тепер ви можете вибрати електронні листи зі спамом, які ви ніколи не відкриваєте та не читаєте, або ті, які більше не бажаєте отримувати, і натиснути посилання для скасування підписки внизу листа. Багато інформаційних бюлетенів і рекламних кампаній, навіть тих, що проводяться авторитетними службами, ускладнюють пошук кнопки скасування підписки. Але якщо ви уважно прокрутите, ви знайдете його. Якщо ні, ви завжди можете повідомити про електронний лист як про спам, що автоматично скасує вашу підписку.

Використовуйте додаткову електронну адресу

Створення додаткового облікового запису електронної пошти – ще один спосіб захистити вашу поштову скриньку від спаму. Електронні адреси, які використовуються для покупок, реєстрації на події або завантажень, часто потрапляють у списки спаму. Використання однієї адреси електронної пошти для роботи, друзів і родини та іншої для всього іншого може значно очистити вашу папку "Вхідні".

Щоб отримати додаткові поради щодо конфіденційності в Інтернеті, як-от шифрування папки "Вхідні" за допомогою засобу шифрування електронної пошти або використання анонімної електронної пошти, щоб захистити та приховати вашу поштову скриньку, перегляньте інші наші посібники.

Використовуйте фільтр електронної пошти третьої сторони

Навіть найкращий фільтр небажаної пошти не може перехопити кожну небажану електронну пошту. Використання фільтра електронної пошти третьої

сторони разом із звичайним фільтром електронної пошти посилить захист від спаму. Існує багато потужних сторонніх фільтрів електронної пошти, які допоможуть вам запобігти спаму, зокрема від Cyren, Mailwasher, SpamSieve, Zerospam, Spambrella та SpamTitan.

Видаліть підозрілі листи

Не надсилайте підозрілих електронних листів і не натискайте посилання в спамі. Це може призвести до збільшення кількості спаму або навіть наразити вас на шахрайство чи зловмисне програмне забезпечення. Спам-лист може навіть містити фальшиве посилання для скасування підписки, через що ви отримуєте ще більше спаму.

Деякі небажані електронні листи призначені для того, щоб змусити вас відкрити електронний лист, щоб вони знали, що ваш обліковий запис активний. Тоді вони можуть націлити на вас більше сміття. Якщо щось виглядає дещо не так, це, ймовірно, так. Для безпеки просто видаліть електронний лист — якщо він важливий, відправник, швидше за все, зв’яжеться з вами іншим способом.

І не забувайте час від часу очищати папку зі спамом. Електронні листи, які ви позначили як спам, зазвичай зберігаються у вашій електронній пошті протягом певного періоду часу, якщо ви захочете скасувати своє рішення. Щоб переконатися, що ваша папка "Вхідні" залишається чистою, або навіть якщо ви хочете звільнити місце, очистіть папку спаму.

Методи захисту від шкідливого спаму

Спам та інші небажані повідомлення можуть надходити звідки завгодно, і фільтрування їх із папки «Вхідні» може виглядати як гра в «удар по кроту». На щастя, всеосяжне програмне забезпечення безпеки та конфіденційності, як-от Cyren Email Security Engine, може захистити вашу електронну пошту та всю вашу мережу від будь-яких зловмисних загроз, які намагаються проникнути через неї.

Cyren Email Security Engine створено на основі відзначеного нагородами детектора загроз на двигуні, а також має ряд інших функцій безпеки та конфіденційності, як-от інструмент захисту електронної пошти, який автоматично

блокує шкідливі посилання та вкладення. Завантажте Cyren Email Security Engine сьогодні для надійного онлайн-захисту.

ВИСНОВКИ

Темою магістерської дипломної роботи було дослідження та розробка рекомендацій протидії спаму у бізнес-інформаційних системах на базі продукту Cyren Email Security Engine

Для цього було проведено аналіз проблеми спам атак на корпоративні інформаційні системи та аналіз впливу спаму на КІС.

Війна у країні та останні новини стосовно коронавірусу привернуло увагу до поширення спам атак. Тому було вирішено дослідити, як забезпечити захист інформаційних систем від спам атак.

Визначено загальні методи створення спам сайтів та життєвий цикл атаки з метою надання відповідних рекомендацій щодо фзахисту корпоративних інформаційних систем. Було проведено дослідження характеристик мережі та географії спамерів.

Під час роботи була розглянута технологія Cyren Email Security Engine та розглянуті найпоширеніші атаки, які виявляються за допомогою продукту. Переглянуто призначення та ключові функції рішення Cyren Email Security Engine. На основі Cyren Email Security Engine визначено логіку, завдяки якій спам сайти автоматично розпізнаються системою.

За результатами проведеної роботи надано рекомендації щодо захисту фахівців з кібербезпеки від спам атак. Оскільки спамери використовують вразливі місця людини, для кінцевих користувачів було розроблено рекомендації щодо боротьби зі спам атаками.

ПЕРЕЛІК ПОСИЛАНЬ

1. Закон України «Про захист інформації в автоматизованих системах»: Закон України від 05.10.94 № 80/94-ВР // Відомості Верховної Ради України. – 1994. – № 31. – Ст. 286.

2. Закон України «Про інформацію» // Відомості Верховної Ради (ВВР), 1992. – № 48. – ст. 650.

3. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»;

4. ISO/IEC 17799: Information technology – Code of practice for Information security management, 2000.

5. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТЗІ СБ України від 26.07. 99 р. № 22.

6. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.99 р. № 22.

7. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі. Затверджено наказом ДСТЗІ СБ України від 04.12.2000 р. № 53.

8. НД ТЗІ 3.3-001-07 «Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації».

9. ISO/IEC 18043 «Information technology – Security techniques – Selection,deployment and operations of intrusion detection systems»

10. Бурячок В.Л. Політика інформаційної безпеки: підручник. / В.Л. Бурячок, Р.В. Грищук, В.О. Хорошко / За заг. ред. докт. техн. наук, проф. В.О. Хорошка. – К.: ПВП «Задруга», 2014. – 222 с.

11. Бурячок В.Л. Особливості реалізації кібернетичних атак та заходи щодо послаблення їх деструктивного впливу // Вісник воєнної розвідки, 2013, № 32. – С. 46 – 53.

12. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка.– К.: ДУТ, 2015.– 288 с.

13. How to get rid of spam [Електронний ресурс]. Режим доступа: https://us.norton.com/blog/how-to/spam-spam-go-away#

14. What is spam? [Електронний ресурс]. Режим доступа: https://www.cisco.com/c/en/us/products/security/email-security/what-is-spam.html

15. URL Filtering [Електронний ресурс]. Режим доступа: https://www.checkpoint.com/cyber-hub/network-security/what-is-url-filtering/#:~:text=URL%20filtering%20is%20a%20way,that%20this%20content%20is%20blocked.

16. Spam emails [Електронний ресурс]. Режим доступа: https://www.avast.com/c-how-to-stop-spam-emails

17. Enrique Peurtas Sans. 2017 p. Spam filter

18. Email Spam Filtering:A systematic review [Електронний ресурс]. Режим доступа: https://www.nowpublishers.com/article/Details/INR-006

19. Software development: Machine learning [Електронний ресурс]. Режим доступа: https://www.sciencedirect.com/science/article/abs/pii/S0065245808006037

20. Spam is bad [Електронний ресурс]. Режим доступа: https://www.malwarebytes.com/spam.

21. Cyren Ransomware Infographic bad [Електронний ресурс]. Режим доступа: https://www.cyren.com/files/downloads/Cyren-Ransomware-Infographic-profile-v3-LTR.pdf

22. Spam reports [Електронний ресурс]. Режим доступа: https://docs.sendgrid.com/ui/analytics-and-reporting/spam-reports

23. Malware URL intelligence reports [Електронний ресурс]. Режим доступа: https://www.cyren.com/tl_files/downloads/Cyren_Malware%20URL%20Intelligence_Datasheet_12282020_Web.pdf

24. Phishing and spam reports [Електронний ресурс]. Режим доступа: https://cybercalm.org/novyny/fishyng-ta-spam-yak-rozpiznaty-internet-shahrajstva-pov-yazani-z-covid-19/

25. Ukraine: Spam websites [Електронний ресурс]. Режим доступа: https://www.bbc.com/news/technology-60697261

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)