ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи

на тему:

«ТЕХНОЛОГІЯ ЗАХИСТУ ВІД СПАМУ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ»

Виконав: студент 6 курсу, групи БСДМ-61
Спеціальності 125 Кібербезпека
Освітньо-професійної програми
«Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Роде О.О.
(прізвище та ініціали)
Керівник Кожухівський А.Д
(прізвище та ініціали)
Рецензент _____
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.

КИЇВ – 2020

РЕФЕРАТ

Текстова частина магістерської роботи: 52 сторінки, 22 рисунки, 7 джерел.

Об'єкт дослідження – процес дослідження та розробки технологій захищенності інформаційно-комунікаційних систем.

Предмет дослідження – види реагування програмного та технічного забезпечення на спам, або спам-атаки.

Мета роботи – дослідження засобів ефективного захисту інформаційних систем від спаму та спам-атак.

Методи дослідження – спосіб практичного аналізу та теоретичне застосування простих способів захисту інформаційно-комунікаційних систем.

В роботі приведено основні відомості про захист інформаційно-комунікаційних систем від небажаного спаму або спам-атак.

Приведено теоретичні відомості про спам, та його види. Сформульовано основні технології та способи захисту комунікаційних систем від спаму та спам атак. Розглянуто вплив спаму на діяльність та роботу корпоративної мережі. На практичному прикладі розроблено технологію протидії та показано, як спам може впливати на роботу мережі та яким способом можна захиститись від спам-атак.

Галузь використання – інформаційно-комунікайційні системи

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНА СИСТЕМА,СПАМ,СПАМ-АТАКА,КОРПОРАТИВНА МЕРЕЖА, ТИПИ СПАМ АТАК, НЕСАНКЦІОНОВАНИЙ ДОСТУП, ВРАЗЛИВІСТЬ КОРПОРАТИВНОЇ МЕРЕЖІ, DMARC, SPF,DKIM.

ЗМІСТ

ВСТУП

Для стабільної роботи і успішного розвитку комерційного або не комерційного web-проекту, власник інформаційно-комунікаційної системи повинен приділяти значну увагу питанням безпеки і захисту. На жаль, багато власників до сих пір не замислюються про те, що інтернет став набагато «агресивніше», ніж кілька років тому: кошти для злому стають доступнішими, а сам злом практично нічого не коштує, як наслідок зростає число цільових і нецільових атак на корпоративні мережі.

Якщо ваш ресурс безперебійно функціонував протягом останніх п'яти років і ви не робили для цього ніяких спеціальних дій (не посилювали "обороноздатність"), це не означає, що злом інтернет-ресурсу не може статися в будь-який момент сьогодні.

Об'єктом дослідження в роботі є процес дослідження захищенності інформаційно-комунікаційних систем. А також забезпечення ефективного загисту інформаційній системі або корпоративній мережі

Захист мережі критично важливий для будь-яких проектів в інтернеті - незалежно від галузі, в якій працює компанія, і розмірів бізнесу. Під прицілом хакера може виявитися будь-яка інформаційно-комунікаційна система, навіть зовсім маленька. Мета зловмисника - заробити гроші, а способів монетизації корпоративних,наприклад, дуже багато.

Метою даної роботи буде дослідження особливо важливих засобів ефективного захисту інформаційних систем від спам атак та розробки технології, для забезпечення ефективного захисту корпоративної мережі

Предмет дослідження в роботі є різні види реагування програмного та технічного забезпечення на спам, або спам-атаки.

Замислитися над питаннями захисту сайту ніколи не пізно. Якщо ви вже зіткнулися зі спам-атакою, то недостатьо просто ігнорувати, або кидати в «чорний список» відправника. Це допоможе, але не недовго. Потрібно розробити стабільні, та ефективні способи захисту вашої мережі, від постійних атак. І не тільки спам атак. Адже вони будуть завжди. Йдеться про проактивниі заходи, спрямовані на підвищення стійкості мережі до несанкціонованих вторгненнь ззовні. Дешевше захистити мережу превентивно.

Методом дослідження буде спосіб практичного аналізу та теоретичне застосування простих способів захисту інформаційно-комунікаційних систем на прикладі простого програмного забезпечення, а також за допомогою спеціалізованного технічного способу DMARC

1 БЕЗПЕКА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ В СУСПІЛЬСТВІ

Технології володіння та обміну інформацією як ресурсом завжди визначали основні вимоги до якості інформаційно-комунікаційного простору будь-якої країни. З появою першого комп’ютера із низкою новітніх інформаційно-комунікаційних технологій, та після першого впровадження такого компьютера до корпоративної мережі виникло досить багато незначних проблем їх безпеки, виявилось багато проблем та прорахунків в організації. Все це змушує постійно переглядати сенс суспільно політичних процесів та більш глибоко аналізувати факти інформаційної безпеки таких систем у суспільстві.

Протягом багатьох років спам швидко стає основною загрозою безпеці - каталізатором потенційного фінансового зливу або крадіжки інтелектуальної власності - для організацій у всьому світі.

1.1 Роль інфомаційно-комунікайних технологій в суспільстві

Інфомаційно-комунікаційні технології змінили параметри отримання інформації за допомогою комунікаційних технологій (газети, радіо і телебачення) шляхом розвитку Інтернету і нових технологічних пристроїв, таких як комп'ютер, планшет і смартфон. Інформація в цьому контексті відноситься до трансляції даних інноваційним чином, що включає текст, зображення і звук.

Під комунікацією розуміються інструменти, які дозволяють одержувачу правильно розшифрувати повідомлення.

Говорячи про інфомаційні технології, можна посилатися на різні критерії в залежності від контексту вживання терміна.

А саме:

1.Мережі. Йдеться як про радіо- і телевізійних мережах, так і про стаціонарних і мобільних мережах.

2.Термінали і обладнання. Маються на увазі всі типи пристроїв, через які працюють інформаційні та комунікаційні мережі. Наприклад, комп'ютери, планшети, мобільні телефони, аудіо- та відеотехніка, телевізори, ігрові приставки і т.д.

3.Послуги. Йдеться про широкий спектр послуг, пропонованих за допомогою вищевказаних ресурсів. Наприклад, поштові служби, хмарне сховище, дистанційне навчання, електронний банкінг, онлайн ігри, розважальні сервіси, віртуальні спільноти та блоги.

Інформаційно-комунікаційні технології є невід'ємною частиною сучасної робочого середовища. Вони полегшують зберігання складних баз даних, як на локальних серверах, так і в хмарних сервісах.

Інформаційні технології необхідні також для розвитку онлайн торгівлі, електронного банкінгу, пошуку інформації, інвентарного контролю, виробництва інформаційних матеріалів і безпосередньо ефективного зв'язку. Все це може позитивно вплинути на продуктивність праці і конкурентоспроможність бізнесу.

Однак інформаційно-комунікаційні технології також можуть створювати певні проблеми, оскільки їх все більш часте використання змушує працівників відволікатися від виконання своїх завдань.

1.2 Боротьба за контроль

Будь яка країна, після появи комп’ютера, який революційно змінів усі засоби і технології комунікації, досить важно і невпевнено почала контролювати фунціонування інформаційного контенту в своєму інформаційному полі. Відразу всі почали запозичувати один від одного різноманітні віртуальні продукти, витісняючи чужі на переферію й захищаючи власні інтереси в інформаційно-

комунікаційній сфері. Досить часто це траплялось не лише в м'якій формі, а і в жорсткій. За володіння сучасними перспективами інформаційно-комунікаційної сфери почалася боротьба в економічній, військовій, науково-освітній діяльності держави. На сьогоднішній день така боротьба має два принципово різні прояви – інформаційно-технічна й інформаційно-гуманітарна. Прикладом інформаційно-технічної є звичайна кібератака на ресурс або мережу. Прикладом інформаційно-гуманітарної – операція впливу.

І основою є підпорядкованість цих двох меделей завданням управління свідомістю людини різними засобами. Зараз рівень освіти та технічні уявлення про складні процеси комп'ютерної доби почали диктувати зовсім нові та іноваційні принципи захисту джерел інформаціх від витоку інформації.

1.3 Проблеми захисту комп'ютерної інформації

Термінами «інформаційна війна» і «інформаційна зброя» в останній час ми почали доволі активно оперувати та часто використовувати. Ми все частіше чуємо такі терміни по телебаченню, в інтеренеті, або навіть від знайомих. Цим ми пояснюємо безліч дій та операцій вливу проти України, які без сумніву направлені на право володіння нашими інформаційними ресурсами. І основну небезпеку для функціонування інформаційних систем представляє несанціонований доступ до комп'ютерної інформації. (під яким слід розуміти доступ до комп'ютерної інформації, здійснюваний з порушенням встановлених правил розмежування доступу) Небезпека несанкціонованого доступу полягає в тому, що воно, будучи само по собі комп'ютерним правопорушенням, створює передумови для здійснення більш тяжких правопорушень — розкрадання комп'ютерної інформації, шпигунства тощо.

Все це давно стало одним із видів бойових дій направлених на ту або іншу країну, та ,в сучасному світі, є ключовим об'єктом впливу на них. Отже основним

завданням спеціалістів по інформаційнії безпеці є убереження таких систем від несанкціонованого доступу, та модифікації цих систем згідно нинішніх реалій. В рідких випадках систему простіше знижити повністю, ніж намагатися її врятувати. У зв'язку з цим одним з основних питань ефективного функціонування інформаційних систем є захист комп'ютерної інформації, що зберігається в них, яка державну та іншу охоронювану законом таємницю.

Таким чином, проблеми інформаційно-комунікаційної безпеки починають посідати одне з ключових місць у системі забезпечення реалізації всіх політико-правових проблем, стають життєво важливими при реалізації інтересів усіх без винятку осіб, суспільств і країн.

1.4 Основні поняття та принципи

Електро́нна по́шта або е-пошта — це простий спосіб обміну текстовою, або будь якою іншою інформацією (текстові документи, аудіо-, відеофайли, архіви, програми) з іншими користувачами за допомогою компьютерів або інших пристроїв, з яких можливий вихід в Інтернет.

Електронною поштою можна надсилати не лише текстові повідомлення, але й документи, графіку, аудіо-, відеофайли, програми тощо. Через електронну пошту можна отримати послуги інших сервісних мереж.

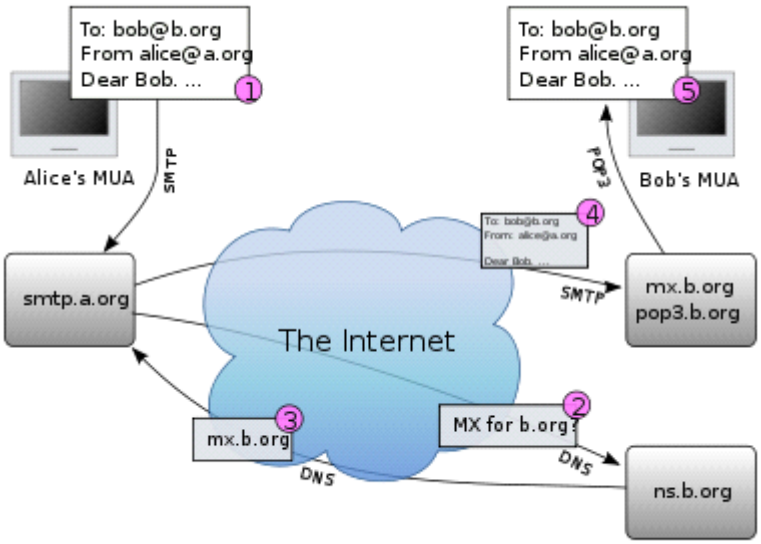


Рис. 1.1 Прицнип роботи електронної пошти

Електронна пошта — типовий сервіс відкладеного зчитування (off-line). Після відправлення повідомлення, як правило, у вигляді звичайного тексту, адресат отримує його на свій комп'ютер через деякий період часу, і знайомиться з ним, коли йому буде зручно.

Електронна пошта схожа на звичайну пошту. Звичайний лист складається із конверта, на якому зазначена адреса отримувача і стоять штампи поштових відділень шляху слідування, та вмісту — власне листа. Електронний лист складається із заголовків, які містять службову інформацію (про автора листа, отримувача, шлях проходження листа), які служать, умовно кажучи, конвертом, та власне вміст самого листа. За аналогією зі звичайним листом, відповідним методом можна внести в електронний лист інформацію якого-небудь іншого роду, наприклад, фотографію тощо. Як і у звичайному листі можна поставити свій підпис. Звичайний лист може не дійти до адресата або дійти з запізненням, — аналогічно і електронний лист. Звичайний лист доволі дешевий, а електронна пошта — найдешевший вид зв'язку.

Отже, електронна пошта повторює переваги реального листу (простоту, дешевизну, можливість пересилання нетекстової інформації, можливість підписати і зашифрувати лист) та недоліки (негарантований час пересилки, можливість доступу для третіх осіб під час пересилки, неінтерактивність) звичайної пошти. Проте у них є і суттєві відмінності. Вартість пересилки звичайної пошти у значній мірі залежить від того, куди вона повинна бути доставлена, її розміру та типу. У електронної пошти такої залежності або немає, або вона досить невідчутна. Електронний лист можна шифрувати та підписувати надійніше та зручніше, ніж лист на папері — для останнього, власне, взагалі не існує загальноприйнятих засобів шифровки. Швидкість доставки електронних листів набагато вища, ніж паперових, та мінімальний час проходження незрівнянно менший. Загалом в залежності від розміру листа та швидкості каналу зв'язку доставка електронного листа триває в середньому від кількох секунд до кількох хвилин.

1.5 Спам в останні роки

Щодня надсилається майже 200 мільярдів спаму, що свідчить про приблизний стократний приріст порівняно з 2,4 мільярдами спаму на день у 2019 році. Близько 95 відсотків цих повідомлень надсилаються ботами, зміст яких зазвичай затуманений і неоднозначни

1.6 Об’єм спаму

Глобальний обсяг спаму в першій половині 2019 року показує різну кількість перехопленого спаму щотижня. Спам виявився дорогим з точки зору таких ресурсів, як пропускна здатність, пропускна здатність сервера, мережева інфраструктура та сховище. Це коштує компанії величезних технологічних витрат через такі елементи, як кількість обробної потужності сервера електронної пошти, необхідної для подолання потоку, і кількість часу, який повинен витратити персонал IT-служби на боротьбу з проблемою. Незалежно від техніки - використання ботнетів або зловживання безкоштовними послугами електронної пошти - представлений нижче

глобальний обсяг спаму показує різні стани шкідливої діяльності на основі даних зібраних датчиків розвідки Trend Micro.

1.7 Види спаму

1.7.1 Реклама

Цей різновид спаму трапляється найчастіше. Деякі компанії рекламують свої товари чи послуги за допомогою спаму. Вони можуть розсилати його самостійно, але частіше замовляють це тим компаніям (чи особам), які на цьому спеціалізуються. Привабливість такої реклами в її порівняно низькій вартості і досить великому охопленню потенційних клієнтів.

Донедавна зовсім не було законів, які б забороняли чи обмежували таку діяльність. Тепер робляться спроби розробити такі закони, але це досить важко зробити. Складно визначити в законі, яка розсилка законна, а яка ні. Найгірше, що компанія (чи особа), що розсилає спам, може знаходитися в іншій країні. Для того, щоб такі закони були ефективними, необхідно погодити законодавство багатьох країн, що в найближчому майбутньому майже нереально. Проте в США, де такий закон уже прийнятий, є спроби притягнення спамерів до суду.

1.7.2 Нігерійські листи

Іноді спам використовується для того, щоб виманити гроші в одержувача листа. Найпоширеніший спосіб одержав назву «нігерійські листи», тому що дуже багато таких листів приходило з Нігерії. Такий лист містить повідомлення про те, що одержувач листа може одержати якимось чином велику суму грошей, а відправник може йому в цьому допомогти. Потім відправник листа просить перерахувати йому трохи грошей: наприклад, для оформлення документів чи відкриття рахунку. Виманювання цієї суми і є метою шахраїв.

1.7.3 Фішинг

Інший спосіб шахрайства за допомогою спаму одержав назву «фішинг». В цьому

разі спамер намагається виманити в одержувача листа номер його кредитних карток чи паролі доступу до систем онлайнових платежів тощо. Такий лист, зазвичай, маскується під офіційне повідомлення від адміністрації банку. У ньому говориться, що одержувач повинен підтвердити відомості про себе, інакше його рахунок буде заблоковано, і наводиться адреса сайту, який належить спамерам, із формою, яку треба заповнити. Серед даних, що потрібно повідомити, є й ті, котрі потрібні шахраям.

1.8 Інші види спаму

- Розсилання листів **релігійного змісту**.

- Масове розсилання для **виведення поштової системи з ладу** (Відмова сервісу).

- Масове розсилання **від імені іншої особи**, з метою викликати до неї негативне ставлення.

- Масове розсилання листів, що містять **комп'ютерні віруси** (для їхнього початкового поширення).

Є також два типи масових розсилань, які часто не відносять до категорії спаму, оскільки вони здійснюються ненавмисно. Однак вони створюють такі самі (або навіть серйозніші) проблеми для адміністраторів мереж і кінцевих користувачів.

- ***Комп'ютерні віруси*** *певного типу (поштові хробаки) поширюються за допомогою електронної пошти. Заразивши черговий комп'ютер, такий хробак шукає в ньому e-mail адреси й розсилає себе за цими адресами.*

- ***Поштові хробаки*** *часто підставляють випадкові адреси (зі знайдених на зараженому комп'ютері) у поле листа «Від кого». Недосконалі антивірусні програми на інших комп'ютерах відсилають на цю адресу повідомлення про знайдений вірус. У результаті десятки людей одержують повідомлення про те, що вони нібито*

розсилають віруси, хоча насправді вони не мають до цього жодного стосунку.

1.9 Способи поширення

1.9.1 Електронна пошта

Найбільший потік спаму поширюється через електронну пошту (e-mail). Станом на 2016 рік потік спаму в загальному трафіку електронної пошти становить близько 65% за даними Cisco Systems.

Спамери збирають **e-mail адреси** за допомогою спеціального робота або вручну (рідко), використовуючи веб-сторінки, конференції Usenet, списки розсилок, електронні дошки оголошень, гостьові книги, чати тощо. Такі програми-роботи здатні зібрати за годину тисячі адрес і створити з них базу даних для подальшого розсилання на них спаму. Деякі компанії займаються тільки збором адрес, а бази потім продають. Деякі компанії продають спамерам e-mail адреси своїх клієнтів, що замовили в них товари чи послуги електронною поштою.

Для розсилання спаму використовуються підключені до інтернету погано захищені комп'ютери. Це можуть бути:

- ***Сервери**, які помилково сконфігуровані так, що дозволяють вільне пересилання пошти (open relay, open proxy).*

- ***Webmail сервіси**, які дозволяють анонімний доступ чи доступ з простою реєстрацією нових користувачів (яку можуть виконати спеціальні програми-роботи).*

- ***Комп'ютер-зомбі**. Деякі спамери використовують відомі уразливості в програмному забезпеченні чи комп'ютерні віруси для того, щоб захопити керування великою кількістю комп'ютерів, підключених до інтернету і використовувати їх для розсилання спаму.*

Для ускладнення автоматичної фільтрації спаму повідомлення часто

спотворюються — замість букв використовуються схожі цифри, латинські букви замість кирилиці,тощо.

Застосовуються різні хитрощі для того, щоб переконатися, що повідомлення отримане й прочитане. Серед них:

•***Підтвердження про доставку***. *Деякі поштові клієнти можуть відправляти його автоматично.*

•***Листи з зображеннями***, *які завантажуються із сайтів, контрольованих спамерами.*

•***Посилання на веб-сторінки***, *на яких пропонується одержати додаткову інформацію.*

•***Пропозиція відмінити підписку на цю розсилку***, *послявши листа на вказану адресу.*

Якщо спамери одержують підтвердження, що поштова адреса дійсно використовується, потік спаму може багаторазово збільшитися.

1.9.2 Usenet

Багато груп новин Usenet, особливо немодеровані, втратили користувачів і зараз містять переважно рекламу, часто навіть не за темою. Замість інших були створені модеровані конференції.

1.9.3 Миттєві повідомлення

З розвитком служб миттєвих повідомлень, таких як ICQ, AI та ін., спамери почали використовувати їх для своїх цілей. Багато з цих служб надають список користувачів, який можна використати для розсилання спаму.

1.9.4 Блоги, Вікі

Останнім часом з'явилися веб-сайти, які можна вільно редагувати — блоги й вікі.

Наприклад, Вікіпедія створена за цією технологією. Оскільки ці сторінки відкриті для вільного редагування, на них може розміщуватися спам.

1.9.5 Підміна інтернет-трафіку

Відомі випадки коли деякі недобросовісні провайдери інтернет-зв'язку завдяки можливості підміни на льоту користувацького http-трафіку самовільно змінювали відображуваний користувачеві вміст отриманої ним з мережі веб-сторінки стороннього ресурсу або підмінювали її власною заради більшої реклами яких-небудь своїх додаткових послуг, що можна розглядати як сучасний різновид спаму.

1.9.6 SMS-повідомлення

Спам може поширюється не тільки через Інтернет. Рекламні SMS-повідомлення, які надходять на мобільні телефони особливо неприємні тим, що від них важче захиститися, і одержувач іноді повинен платити за кожне повідомлення. Це може бути досить велика сума, особливо якщо абонент використовує роумінг.

1.9.7 Телефонні дзвінки

Деякі компанії можуть масово здійснювати велику кількість телефонних дзвінків з доволі агресивною рекламою завдяки поступовому перебору телефонних номерів, випадковій вибірці номера з певного діапазону або використанню готових баз даних, придбаних на чорному ринку чи завдяки доступу до телефонної інфраструктури — своїх власних (наприклад, мобільні оператори). Відомим прикладом такого спаму в Україні є компанія «Київстар».

1.10 Небезпека спаму

1.10.1 Приклад: Шахрайство з банківським переказом

Не слід думати, що фішинг-шахрайство працює лише на непростих людей, які не мають технічного досвіду? Ну, запитайте себе наступне: як найкмітливіші корпоративні офіцери у світі стали жертвою вишуканої версії афери з банківськими переказами? У цих випадках, замість того, щоб викрадену здобич виміряти сотнями

або тисячами доларів, ФБР виміряло її мільйонами.

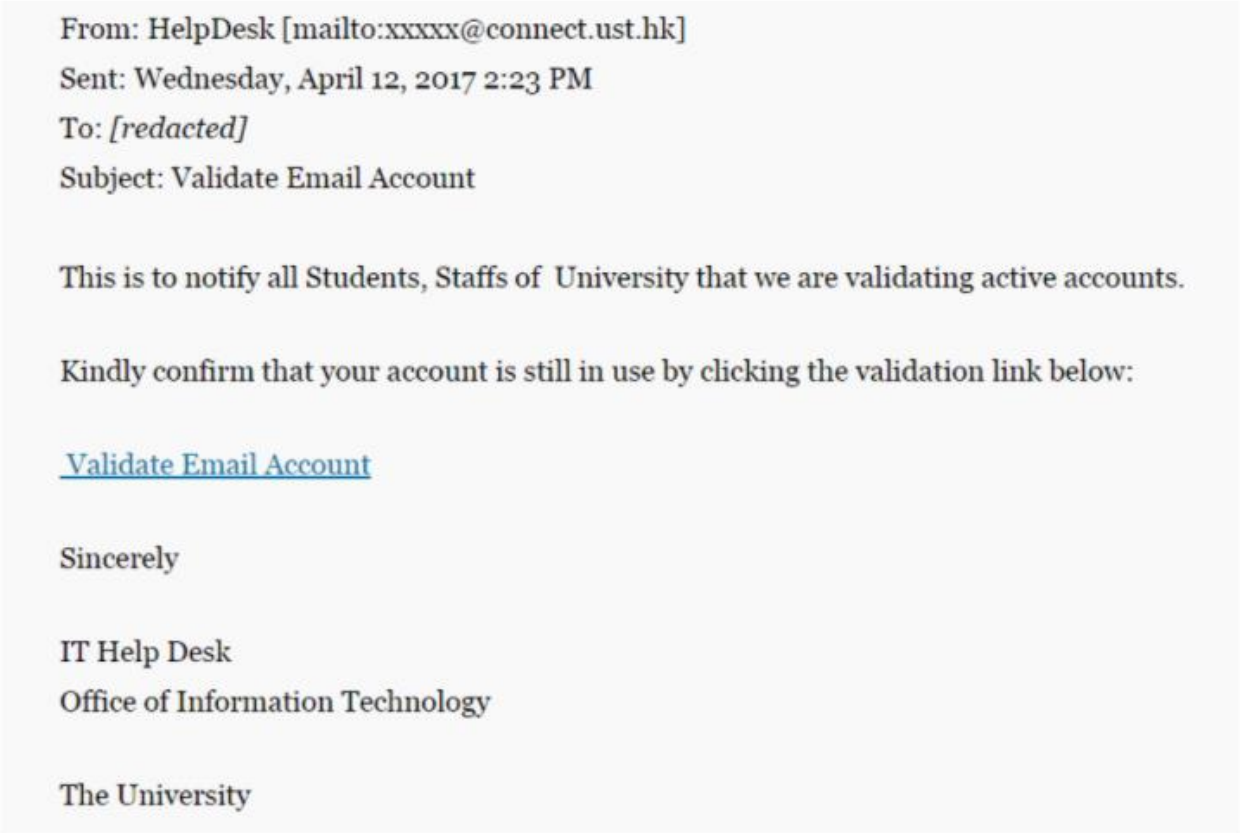
Google та Facebook втратили більш ніж 100 мільйонів долларів, коли шахрай встановив програмне забезпечення бухгалтеріях компаній для вивчення їх типових транзакцій. Потім підставив одного зі своїх підрядників і виставив рахунки на мільйони способом розсилки спам листів від імені Google та Facebook. (Обидві компанії стверджують, що виявили шахрайство і за допомогою правоохоронних органів повернули викрадені кошти.) Деякі з найбільших компаній у світі були обдурені таким чином. (У 2016 році 3 мільярди доларів було вкрадено за допомогою шахрайських схем переказу грошей «за допомогою» великих компаній. Більша частина грошей зникла безпортоно.

1.10.2 Інші приклади небезпечних листів

1.10.2.1 Шкідливі веб посилання

Посилання, також відомі як URL-адреси, поширені в електронних листах загалом, а також у фішинг-листах. Шкідливі посилання перенаправлять користувачів на веб-сайти-самозванці або на сайти, заражені шкідливим програмним забезпеченням, також відомим як шкідливе програмне забезпечення . Шкідливі посилання можуть маскуватися, щоб виглядати як довірені посилання, і вбудовуються в логотипи та інші зображення в електронному листі.

Ось приклад електронного листа, отриманого користувачами з Корнельського університету, американського коледжу. Це просте повідомлення, в якому вказано відправника як "Довідкову службу" (хоча електронне повідомлення не надходило з довідкової служби університету, а з домену @ connect.ust.hk). За інформацією IT-команди Корнелла, посилання, вбудоване в електронне повідомлення, перенесло тих, хто натиснув на посилання, на сторінку, яка виглядала як сторінка входу в Office 365. Цей фішинг-лист намагався викрасти облікові дані користувача.



From: HelpDesk [mailto:xxxxx@connect.ust.hk]
Sent: Wednesday, April 12, 2017 2:23 PM
To: *[redacted]*
Subject: Validate Email Account

This is to notify all Students, Staffs of University that we are validating active accounts.

Kindly confirm that your account is still in use by clicking the validation link below:

Validate Email Account

Sincerely

IT Help Desk
Office of Information Technology

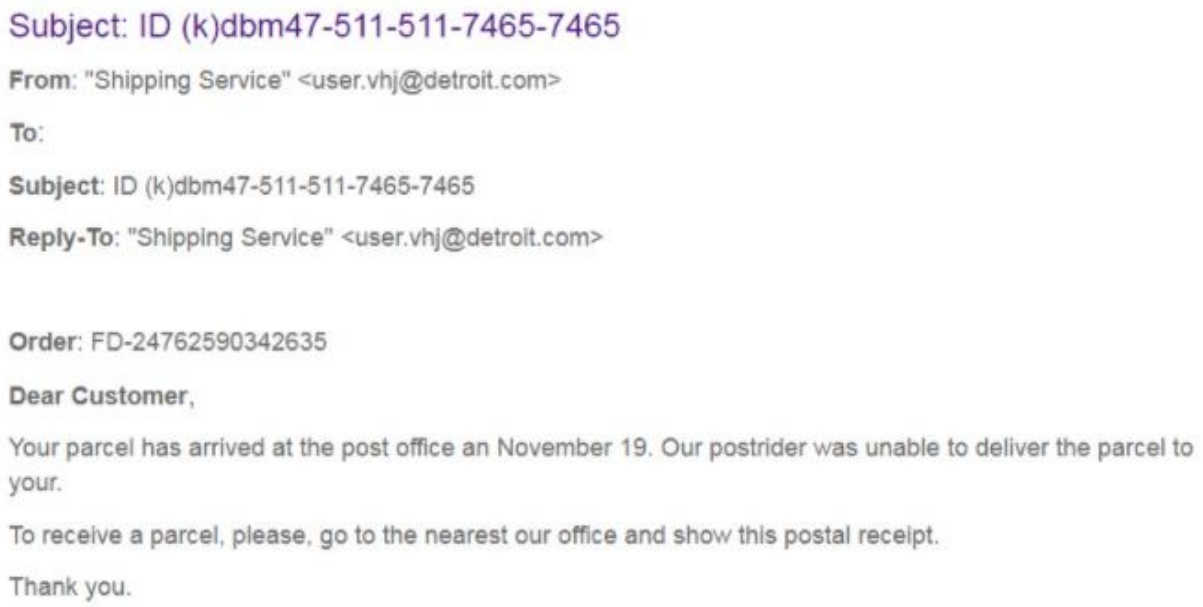
The University

Рис. 1.2 Приклад шкідливого веб посилання

1.10.2.2 Шкідливі вкладення

Вони виглядають як законні вкладення файлів, але насправді заражені шкідливим програмним забезпеченням, яке може скомпрометувати комп'ютери та файли на них. У випадку з вимогами - різновидом шкідливих програм - усі файли на ПК можуть стати заблокованими та недоступними. Або можна встановити реєстратор натискань клавіш для відстеження всього, що вводить користувач, включаючи паролі. Важливо також усвідомити, що інфекції-вимагателі та шкідливі програми можуть поширюватися з одного ПК на інші мережеві пристрої, такі як зовнішні жорсткі диски, сервери та навіть хмарні системи.

Ось приклад фішинг-тексту електронного листа, який міжнародний вантажовідправник FedEx розміщує на своєму веб-сайті. Цей електронний лист закликав одержувачів роздрукувати копію вкладеної поштової квитанції та віднести її у пунк отримання посилок від FedEx, щоб отримати посилку, яку неможливо доставити. На жаль, у додатку містився вірус, який заражав комп'ютери одержувачів. Варіації цих типів шахрайських відправлень особливо поширені під час різдвяного сезону покупок, хоча вони спостерігаються цілий рік.



Subject: ID (k)dbm47-511-511-7465-7465

From: "Shipping Service" <user.vhj@detroit.com>

To:

Subject: ID (k)dbm47-511-511-7465-7465

Reply-To: "Shipping Service" <user.vhj@detroit.com>

Order: FD-24762590342635

Dear Customer,

Your parcel has arrived at the post office an November 19. Our postrider was unable to deliver the parcel to your.

To receive a parcel, please, go to the nearest our office and show this postal receipt.

Thank you.

Рис. 1.3 Приклад шкідливого вкладення

1.10.2.3 Шахрайскі форми введення данних

Ці електронні листи пропонують користувачам заповнити конфіденційну інформацію, таку як ідентифікатори користувачів, паролі, дані кредитної картки та номери телефонів. Після того, як користувачі подають цю інформацію, кіберзлочинці можуть використовувати її для власної вигоди.

Ось приклад фальшивої цільової сторінки, якою користуються на веб-сайті gov.uk. Після натискання посилання у фішинг-листі користувачі переходять на цю шахрайську сторінку, яка, як видається, є частиною агенції збору податків HMRC. Користувачам повідомляють, що вони мають право на повернення коштів, але вони повинні заповнити форму. Цей тип особистої інформації може використовуватися кіберзлочинцями для цілого ряду шахрайських дій, зокрема викрадення особистих даних.

Рис. 1.4 Приклад щахрайскої форми

1.11 Ботнет Rustock

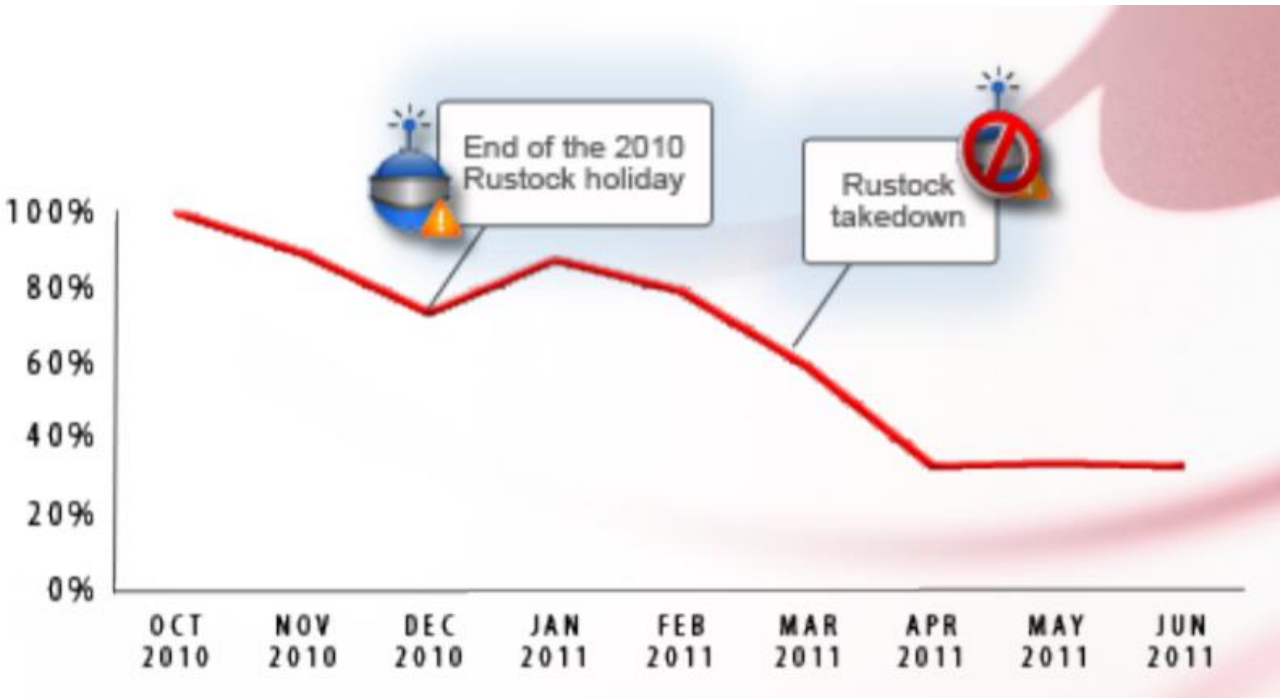


Рис 1.5 Глобальний обсяг спаму з жовтня 2010 по червень 2011 року

100-відсотковий рівень являє собою пік спам-активності ботнета Rustock (тобто одного з найвідоміших спам-ботів), який спостерігався протягом другої половини 2010 року. Дослідники вважають, що спад активності спаму можна віднести до ліквідації Рустока. Вони розробили підпис для ідентифікації спаму, що походить з ботнету, і виявили, що за годину після його видалення обсяг трафіку, що відповідав підпису Рустока, впав на 99,97 відсотка.

За останні 100 днів роботи Рустока було понад 3 мільйони різних IP-адрес, які розсилали спам, що відповідають підпису ботнету. Кількість заражених систем була значно меншою, ніж ця, оскільки більшість вузлів Rustock розміщувались на динамічних IP-адресах. Ботнет мав під контролем приблизно 1 мільйон заражених систем, які могли розсилати мільярди спаму щодня.

З моменту відкриття спам-бота в 2006 році, Русток зміг скомпрометувати тисячі систем і розіслати мільярди фармацевтичного спаму.

Видалення Рустока сильно зменшило обсяг спаму майже до мінімальних кількостей, ніж тих, що раніше фіксували під час свят 2010 року. Це показує, що загальний обсяг спаму щомісяця впав приблизно на 40 відсотків порівняно з найвищим числом у жовтні 2010р. До спаду в грудні 2010 році обсяг спаму залишався відносно стабільним з незначними варіаціями зростання протягом першої половини 2010р. Оскільки на спам-бота припадає половина загального обсягу спаму, зменшення його активності автоматично дало помітні результати. Поточний стан врешті-решт зміниться, особливо, оскільки спамери зараз зосереджуються на створенні більш цілеспрямованих повідомлень, націлених на "якість над кількістю".

1.12 Чи можлива стабілізація після видалення ботнетів?

Обнадійливо думати, що протягом декількох місяців після видалення Рустока обсяг спаму все ще не збільшувався, на відміну від видалення McColo у 2008 році. McColo виникла як основна послуга хостингу в США для міжнародних фірм та синдикатів, які беруть участь у віддаленому управлінні мільйонами скомпрометованих систем продажу фальшивих фармацевтичних та дизайнерських товарів, а також підроблених продуктів безпеки електронною поштою. Після видалення McColo загальний обсяг спаму продовжував робити невеликі стрибки, оскільки спамери продовжували використовувати інші ботнети, не розміщені на спам-боті.

1.13 Найпопулярніші спам-мови

На даний момент компанія Trend Micro контролює 38 мов та діалектів, які часто використовуються у спамі. У першій половині 2010 року вони виявили, що понад 95 відсотків зібраних нами зразків спаму було написано англійською мовою. Ця тенденція продовжилася і в 2011 році, оскільки англійська знову очолила список мов із 92-відсотковою часткою. Близько 22 відсотків неанглійського спаму було написано російською мовою.

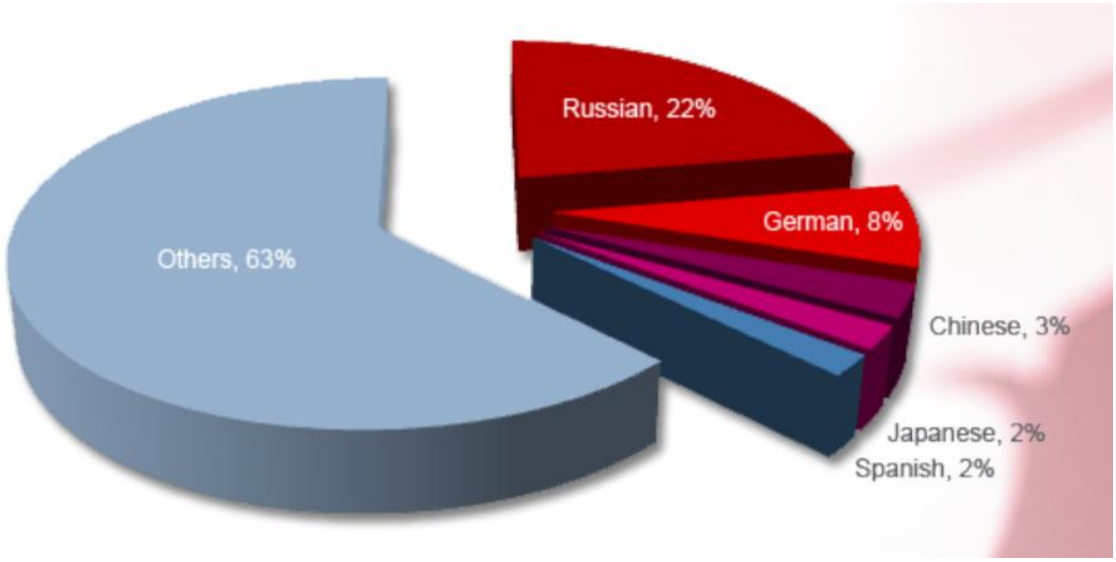


Рис. 1.6 Топ-5 неанглійських мов із спамом з січня по червень 2011 року

1.14 Топ країн «спамерів»

П’ять країн-відправників спаму в першій половині 2011 року становили одну третину від загального обсягу спаму. Однак жодна країна не домінувала у списку.

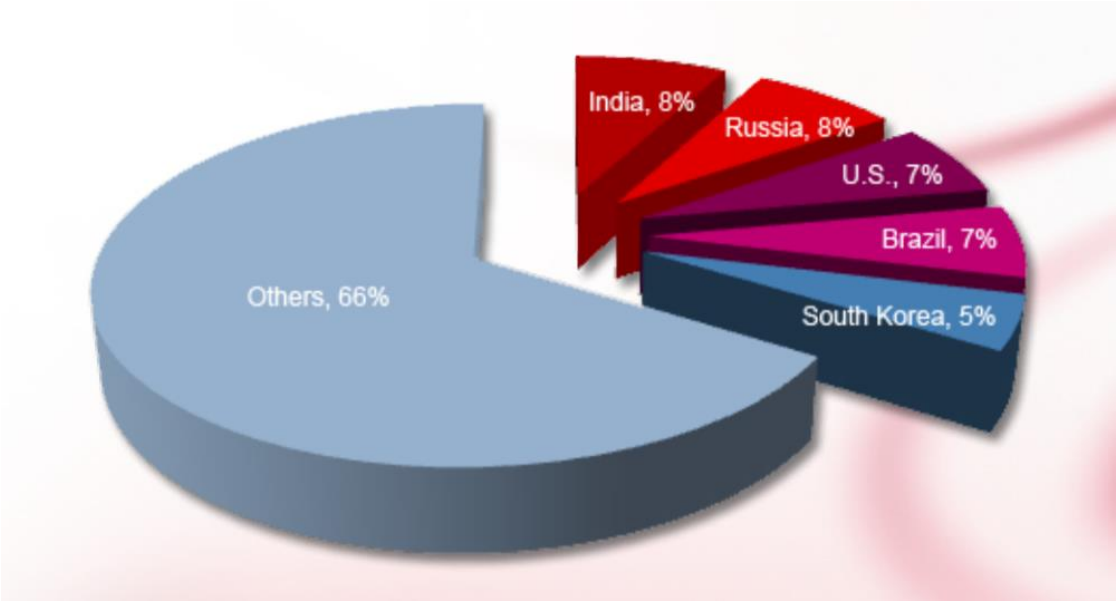


Рис. 1.7 5 найпопулярніших країн, що надсилають спам, з січня по червень 2011 *року*

Останніми роками цифри помітно змінилися порівняно з 2008-2011. Сполучені Штати очолили список країн-відправників спаму в першій половині 2010 року, але в першій половині 2011 року Сполучені Штати були на третьоміу місці. Цей спад збігся з ліквідацією Рустока в березні минулого року, що означає, що кілька спам-ботів, які були знесені базувалися в США.

1.15 Тенденції корпоративного спаму

Спам, що надсилається масовою поштою, стосується повідомлень, які здебільшого рекламують підроблені фармацевтичні або модні товари чи порнографічні предмети, призначені для комерційної вигоди. Спосіб подальшого запуску типового спаму не змінювався протягом тривалого часу, але це все ще створює проблеми для підприємств у вигляді збільшення пропускної здатності та навантаження поштового сервера.

Окрім обслуговування різних рекламних цілей, спам-програми також покладаються на методи соціальної інженерії для здійснення зловмисних намірів.

Зрештою, соціальна інженерія - це простіший і підступніший спосіб для кіберзлочинців отримати доступ до систем користувачів. Атаки соціальної інженерії пристосовані для збігу з широко відомими випадками, святами, а також новинами та іншими темами. Як правило, спамери використовують тактику соціальної інженерії для передбачуваних сповіщень провайдерів послуг Інтернету та електронної пошти. Ці кампанії, як правило, передбачають таємну інсталяцію шпигунського програмного забезпечення чи іншого шкідливого програмного забезпечення або обманюють користувачів передавати свої паролі та іншу конфіденційну фінансову чи особисту інформацію.

1.16 Боротьба з цілеспрямованими атаками

З точки зору підприємства, нові тренди спаму виходять за рамки звичайного напливу небажаних електронних листів. Ці тенденції включають фідерний фішинг, який зараз широко використовується кіберзлочинцями для отримання доступу до конкретних організаційних цілей. Атаки з допомогою фішингу націлені на певних користувачів, часто на керівників величезних корпорацій та високопоставлених державних службовців, які мають доступ до конфіденційної інформації, такої як дані про власні компанії та корпоративні банківські дані.

Спершу фішери проводять дослідження цільової установи, щоб визначити, як найкраще провернути фішинг-атаку. Для цього «фішери» можуть, наприклад, розсилати спам багатьом обліковим записам електронної пошти в цільовій компанії.

Певною мірою така поведінка, як проведення досліджень конкретних цілей з метою проникнення в організації, що є очевидним у підробному фішингу, також є типовою для найбільш цілеспрямованих атак.

У декількох випадках фішинг може бути навіть першою точкою контакту для здійснення цілеспрямованої атаки, в якій злоумисники агресивно переслідують конкретні цілі, часто за допомогою соціальної інженерії, з метою підтримання стійкого контролю всередині мережі з метою вилучення чутливої інформації та отримання доступу до внутрішніх мереж компанії.

Така справа була у квітні 2011 року. RSA, розкрила подробиці про атаку, яка використовувала два різні фішинг-повідомлення, надіслані своїм співробітникам із темою "План набору на 2011 рік". Зловмисники надіслали згаданий електронний лист двом невеликим групам працівників RSA. Ці повідомлення були написані досить добре, щоб обманути когось із співробітників і щоб ті відкрити вкладений файл Excel, що містив експлойт нульового дня, який встановлював програму для бэкдора.

Дані, отримані кіберзлочинцями від RSA, озброїли їх достатнім ноу-хау для здійснення наступних цілеспрямованих атак на клієнтів компанії, таких як Міжнародний валютний фонд (МВФ).

Через пару тижнів після проникнення на RSA, Epsilon, спіткала та сама доля, оскільки імена та адреси електронної пошти його клієнтів потрапили в коло кіберзлочинців. Ці конкретні інциденти, можливо, полегшили зловмисникам розробку та, отже, все далі підбурурювали їх до атак методом фішингу.

Організації, незалежно від галузі промисловості, такі як два відділи канадського уряду, Національна лабораторія Оук-Ридж та Тихоокеанська північно-західна національна лабораторія Міністерства енергетики США (PNNL) пішли по слідами RSA та Епсілона, піддаючись на майже паралізуючі атаки фішингу.

Ще одним ризиком, який спричиняє фішинг, є серйозні фінансові втрати. Більшість цілеспрямованих атак, які проводяться, спрямовані і спираються на звичайну слабкість - соціальну інженерну хитрість, - коли людину обманюють.

1.17 Битва проти спаму триває

Традиційний спам може зменшуватися в обсязі, але старі методи все ще використовуються для підбурювання сьогоднішніх спам-атак, тому битва продовжується. Напади на сайти соціальних мереж часто використовують тактику соціальної інженерії, якою кіберзлочинці користуються з тих пір, як використання веб-пошти набуло широкого поширення. Тепер користувачі отримують більше небажаних повідомлень за різною тематикою, тоді як підприємства продовжують відбивати численні кібератаки на свою IT-інфраструктуру.

В даний час методи розсилки спаму просунулися до такої міри, що перелік чорних списків IP та власна фільтрація вмісту вже недостатні. Спамери рухаються до використання законних поштових серверів провайдерів у зловмисних цілях, що може вимагати більш комплексних процесів щодо блокування спаму.

Висновок до розділу 1

В данному розділі були приведені теоретичні відомості про те, як інформаційно-комунікаційні системи впливають на життєдіяльність людей та країн. Розібраний спосіб комунікації за допомогою електронної пошти. Приведені різні способи та види спаму в сфері електронної пошти, та наведені найбільш небезпечні загрози при передачі електронного листа. Також було розібрано гучні шахрайства з використанням спаму за останні 10 років та приведена загальна статистика в області розсилки спаму.

2 МЕТОДИ ПРОТИСТОЯННЯ СПАМУ В ІНФОМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

Існує два види інформаційних атак — непряма і пряма. Наприклад, побудувати макетну копію військового об’єкта, та розмістити там макети техніки й імітувати діяльність щодо її технічного обслуговування, і це буде непрямою інформаційною атакою. А можна за допомогою сучасних засобів ІКТ впровадити неправдиву або сплановану інформацію прямо в сховища інформації супротивника, щоб він при прийнятті командних рішень оперував неправдивими даними, і це буде прямою інформаційною атакою. Інформація, таким чином, виступає і як мета впливу, і як зброя, а ІКТ при цьому розглядаються як зброя першого удару, руйнуючи або спотворюючи інформацію без видимих пошкоджень її носіїв.

Спам відноситься до другого типу. Ці повідомлення використовуються для реклами продуктів та послуг для фішингових цілей або для залучення одержувачів на скомпрометовані або шкідливі веб-сайти з метою передачі даних або крадіжки грошей. Вони пройшли довгий шлях з часу свого першого втілення у вигляді текстових рядків. На початку вони, як правило, були нешкідливими для одержувачів, які знають про безпеку, але зараз продовжують створювати загрози, оскільки спам став цільовим та, отже, більш небезпечними. Платформи Web 2.0 продовжують відкривати безмежні можливості для спілкування в Інтернеті, що, на жаль, також перетворюється на нові шляхи для кіберзлочинності. Спам зберігається навіть на платформах Web 2.0. Недавнє дослідження повідомило, що ці повідомлення коштують європейським компаніям приблизно 2,8 мільярда доларів втрат продуктивності, тоді як американські компанії повідомляють про втрати в 20 мільярдів доларів.

2.1Розпізнавання email спаму

Кібератаки стають все більш поширеними, не залежно від країни. Одним з найпоширеніших способів нападу на бізнес є спам. Спам - це електронний лист, який надсилається фізичній особі і зазвичай містить посилання на товар чи послугу. Потім посилання переведе вас на шкідливий веб-сайт, де шкідливе програмне забезпечення автоматично завантажується на ваш комп'ютер і отримує доступ до конфіденційної інформації.

Існує багато способів розпізнати та уникнути спаму. Ось декілька:

- Якщо відправник невідомий, спробуйте з'ясувати, хто це і чому він або вона зв'язується з вами, перш ніж відкрити електронний лист. Це можна зробити методом перевірки адреси, з якої вам надісланий лист. Методом пошуку адреси серед всіх ваших листів. Ви могли просто забути про цю людину або компанію.
- Якщо в листі присутні орфографічні помилки – слід замислитись. Іноді особа, яка надсилає спам, зробить це, щоб пройти повз фільтри спаму.
- Вам раніше хтось надсилав лист з цього адресу, але зараз електронний лист виглядає кардинально інакше. Це може бути шахрай, який видається за цю особу чи компанію, тому що знає що йому довіряють.
- Слід з обережністю ставитись до листів, які виглядають занадто добрими та вигідними. Таким способом шахраї просто намагаються втертись вам в довіру та заволодіти вами персональними данними.

2.2 Основі кроки, при виявленні спаму

Якщо ви помітили, що ваша компанія, здається, отримує багато спаму, ви можете зробити щось для боротьби з цим:

- Налаштуйте програму, яка фільтрує спам.
- Список електронної пошти співробітників завжди повинен бути конфіденційним. Якщо хтось за межами компанії потребує вашої адреси електронної пошти, надішліть йому більш загальний електронний лист, який ви використовуєте, не пов’язаний з електронною адресою вашої компанії та інформацією, що зберігається в ній.
- Встановіть у своєму офісі політику користування Інтернетом для співробітників. Це один з найкорисніших кроків у захисті вашої компанії від спаму та подальших кібератак. Політика повинна містити вказівки щодо таких речей, як загальна безпека, прийнятне використання Інтернету, використання особистого обладнання та безпека офісних служб. Переконайтеся, що всі співробітники підписують копію політики користування Інтернетом і щороку переглядають її.

2.3 Нові можливості у світі електронної пошти

DMARC вводить нові можливості у світ електронної пошти і спрямований на вирішення проблеми, яка мучить електронну пошту з самого початку:

Не існує надійного способу визначити, чи є електронна пошта справжньою чи просто справді гарною підробкою.

Ця проблема вв’язує електронну пошту користувача, або компанії у всілякі проблеми: спам, фішинг, поширення вірусів та шкідливих програм. Електронна пошта використовується для продовження багатьох шахрайств просто тому, що важко визначити, чи надіслана електронна пошта є справжньою. З іншого боку, законні відправники повинні переходити за деякими досить складними фільтрами проти спаму - фільтрами, призначеними для блокування небажаної електронної пошти - лише для того, щоб доставити їх електронні листи. Робити це є досить великою проблемою, оскільки існує ціла галузь “доставки електронної пошти”, яка допомагає організаціям постійно відправляти електронну пошту.

Пошта в Інтернеті не змінилася за ці роки просто тому, що на основне питання *"чи справжня?"* відповісти було непросто.

Основні технології, які пов'язують домен з електронною поштою, існують вже давно, і люди намагалися з усіх сил у різних контекстах, щоб зробити ці технології корисними.

SPF - це спосіб публікації списку серверів, яким дозволено надсилати електронну пошту від імені домену - існує з 2003 року.

DKIM - метод додавання захищеної від втручання доменної печатки до частини електронної пошти – існує з 2005 року

І замість того, щоб покладатися на одну технологію, DMARC об’єднує послідовність налаштування цих існуючих технологій, щоб при отриманні частини електронної пошти можна було виконати просту перевірку, чи справді електронна пошта надходить із домену, про який вона повідомляє, що надходить.

Мета цієї технології полягає в тому, щоб електронну пошту легко було ідентифікувати, але це не дуже корисно, якщо неможливо ідентифікувати **всю** електронну адресу домену. Якщо легко ідентифікувати лише частину електронної пошти домену, то людям все одно доведеться докласти максимум зусиль, щоб з’ясувати, чи решта частин справжні, чи вони просто виглядають справжніми, але насправді є фішинговими листами, які в підсумку спричиняють багато проблем.

2.4 Технологія DMARC

Щоб вирішити цю цілком реальну проблему, нові функції DMARC полегшують ідентифікацію електронної пошти. Це робиться шляхом створення зв’язку між доменом та електронною поштою. (Домен - це все після знаку «@» в електронній адресі.) Усі функції DMARC спрямовані на те, щоб зробити цю відправку можливою для всіх доменів електронної пошти в Інтернеті, незалежно від

того, належить цей домен якийсь окремій людині чи ні. Це може бути компанія «Fortune 500» або окремий громадянин.

Щоб зробити всі електронні листи домену легкими для ідентифікації, DMARC надає власникам доменів уявлення про те, як їх домени використовуються в Інтернеті. Ця видимість надається у формі звітів про зворотний зв'язок, які створюються організаціями, які обробляють вхідну пошту. Звіти надсилаються власникам доменів, коли роблять запит на них. Аналізуючи ці звіти, власники доменів можуть ідентифікувати всі свої джерела електронної пошти, що дає змогу застосовувати базові технології у всіх законних потоках електронної пошти. Без цих звітів власник домену повинен був би якось перевірити свою організацію, щоб з'ясувати, хто з працівників «зливає» електронну пошту - завдання, яке займає багато часу і майже гарантовано буде неповним. За допомогою цих звітів власник домену може швидко і точно виконати роботу.

Отже, коли власник домену впевнений, що він ідентифікував підробку, він може законно вимагати заблокувати її. (наприклад це можу бути фальшивий сайт компанії або підробка адресу електронної пошти)

Сьогодні DMARC використовується для блокування багатьох фальшивих електронних листів, що дуже добре.

Однак, навіть незважаючи на те, що блокування фальшивої електронної пошти носить масовий характер, видимість та всеосяжність, яку DMARC надає власникам доменів, корисна сама по собі. Люди використовують DMARC, щоб перевірити, чи не зловживають їхніми доменами в Інтернеті. Організації використовують DMARC, щоб зрозуміти, як вони та їх партнери надсилають електронну пошту за допомогою своїх доменів, а також чи всі надсилають електронну пошту правильно. Це перетворює DMARC на інструмент дотримання вимог, який організації використовують, щоб переконатись, що вони роблять все можливе, щоб зменшити ризик шахрайства для себе та своїх клієнтів, а також переконатись, що будь-яка

відповідальність за дотримання найкращих практик захисту користувачів на активи зменшуються.

Мабуть, найкраще, що DMARC робить для електронної пошти, - це «змінює» електронну пошту з моделі «дозволяємо не допускати поганих речей» на «дозволяє спиратися на нашу здатність ідентифікувати справжню електронну пошту». Отримувачам електронної пошти стає кардинально простіше працювати з поштою та її обробкою. І це досить велика справа для будь-якої організації, яка отримує та покладається на електронну пошту протягом робочого дня.

2.5 Основні принципи роботи DMARC

DMARC - це технічна специфікація, яка описує, як відправники електронної пошти можуть полегшити ідентифікацію своєї електронної пошти за допомогою існуючих безкоштовних та відкритих технологій. Електронна пошта, сумісна з DMARC, дуже проста в обробці, і основні одержувачі електронної пошти вже прийняли DMARC як звичайний спосіб з’ясувати основну ідентичність електронного листа.

DMARC базується на двох існуючих технологіях, які використовуються для асоціювання частини електронної пошти з доменом. SPF, що розшифровується як Sender Policy Framework, і DKIM, що позначає DomainKeys Identified Mail, працюють різними, але взаємодоповнюючими способами, щоб створити зв'язок між електронною поштою та доменом.

SPF та DKIM - це окремі технології, які існують вже багато років і можуть використовуватися незалежно від DMARC. Самі по собі SPF та DKIM можуть пов’язати електронну пошту з доменом. Мовою DMARC SPF та DKIM генерують «автентифіковані ідентифікатори».

DMARC намагається пов’язати результати SPF та DKIM - автентифікованих ідентифікаторів - із вмістом електронної пошти: конкретно з доменом, знайденим у заголовку електронної пошти «Від кого».

Рис. 2.1 SPF та DKIM ідентифікатори

Домен, знайдений у заголовку електронної пошти «Від кого» це сутність, яка пов'язує всю обробку DMARC.

Зараз, оскільки кожен може придбати домен і поставити SPF і DKIM на робочу систему (включаючи злочинців!), Результати обробки SPF і DKIM - тобто автентифікованих ідентифікаторів - повинні бути пов'язані з доменом, який знаходиться в заголовку «Від кого» ,який в свою чергу пов'язаний з DMARC. Ця концепція називається «вирівнювання ідентифікатора». Отримання ідентифікаторів для вирівнювання закінчується великою частиною роботи з розгортання DMARC.

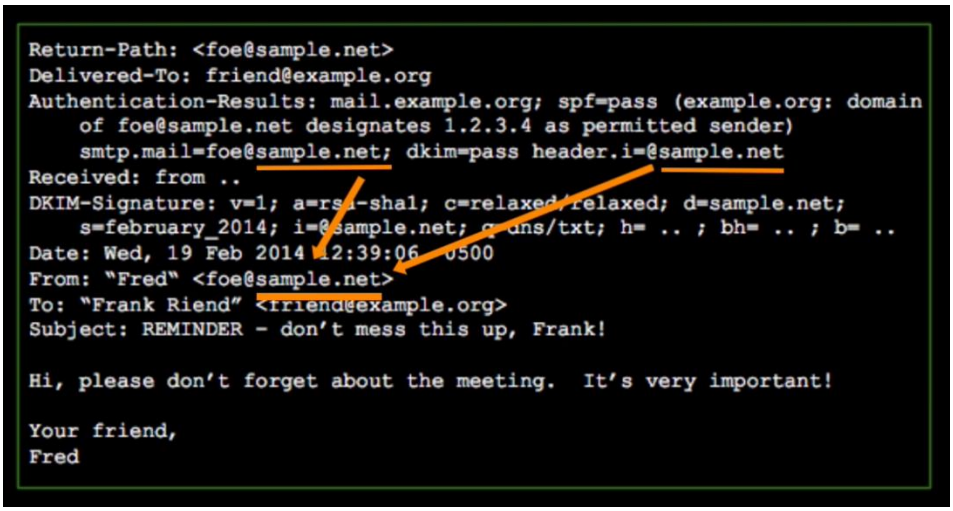


Рис. 2.2 Метод «вирівнювання ідентифікатора»

Щоб зробити можливим для когось, хто володіє доменом електронної пошти, точно розгортати SPF та DKIM, DMARC описує, як можна надіслати відгук власнику домену щодо того, як їх електронний домен використовується в Інтернеті. Цей відгук може бути у двох формах: звіти, що забезпечують вичерпне уявлення про весь трафік домену (як це бачить організація, яка створює звіт), та звіти, які є відредагованими копіями окремих електронних листів, які не на 100% відповідають DMARC.

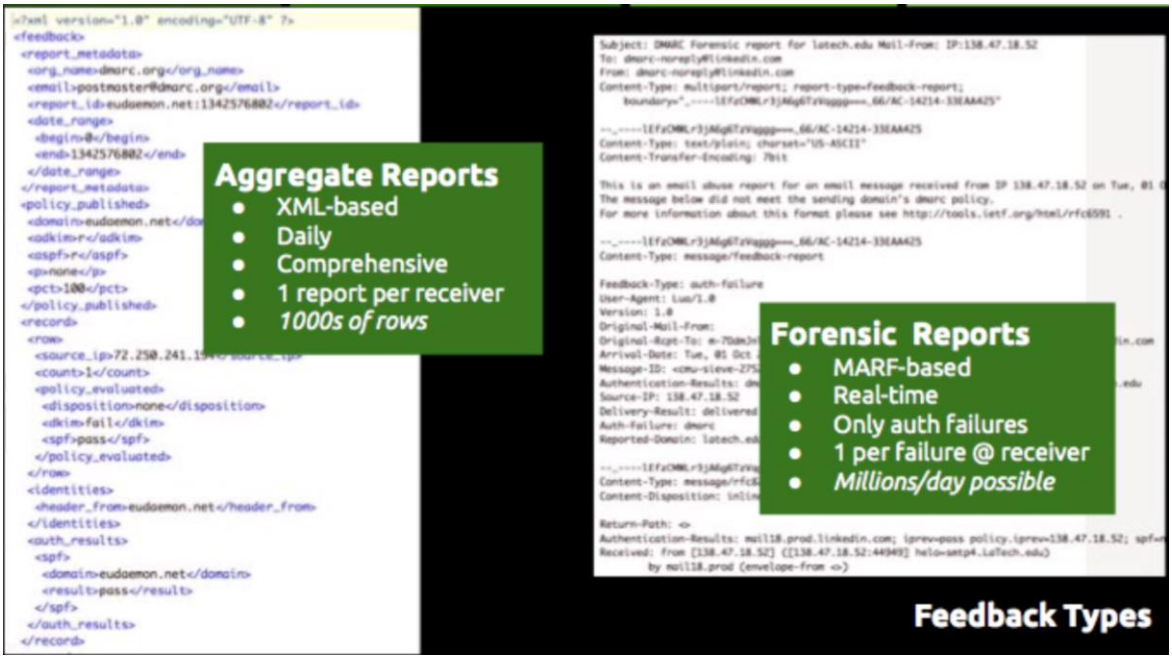


Рис. 2.3 Типи відгуків

Вичерпні звіти засновані на XML і включають таку інформацію, як кількість повідомлень, IP-адреси та результати обробки SPF та DKIM. Хоча деякі люди та більшість андроїдів можуть читати XML безпосередньо, *dmarcian* спеціалізується на обробці цих звітів та визначенні кроків, які потрібно вжити, щоб люди змогли запровадити технологію DMARC, не стаючи експертами з автентифікації електронної пошти.

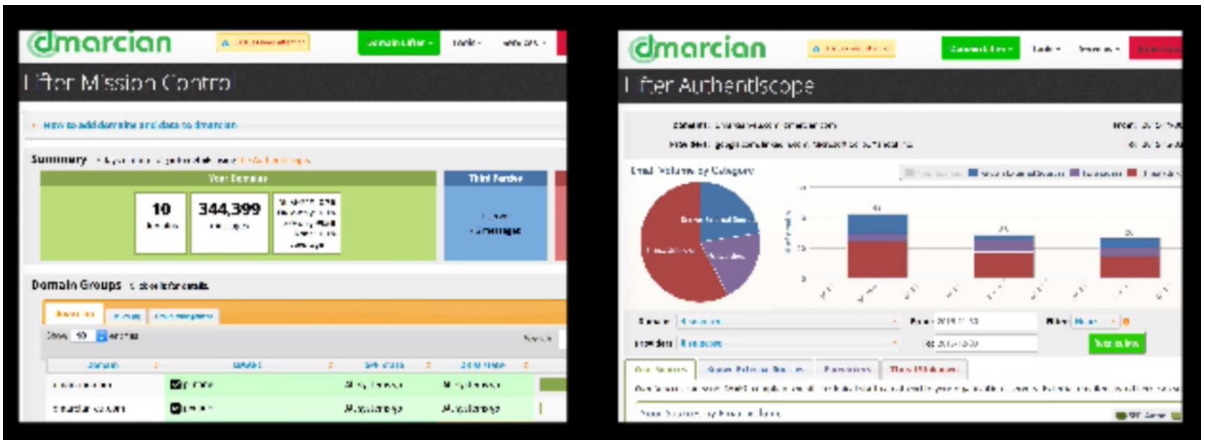


Рис. 2.4 Обробка звіту за допомгою dmarcian

Звіти, які є відредагованими копіями окремих електронних листів, створюються не всіма одержувачами електронної пошти, які беруть участь у DMARC. Причина, через яку одержувач електронної пошти може не генерувати такий звіт, охоплює три великі області:

1. Проблеми конфіденційності, оскільки окремі електронні листи можуть містити особисту інформацію,
2. Звіти можуть бути надзвичайно великими за обсягом,
3. Мати звіти іноді приємно, але виявилось, що їм не потрібно працювати під час розгортання DMARC.

Нарешті, досить багато організацій навіть не хочуть отримувати такі звіти, оскільки хочуть уникнути будь-якої потенційної відповідальності у сфері конфіденційності. Проте ці звіти можуть пролити світло на конкретні типи зловживань, з якими може зіткнутися домен.

Видимість, яку забезпечують звіти про зворотний зв'язок при обробці такими інструментами, як dmarcian дає власнику домену можливість розгортати SPF та DKIM з дуже високим ступенем точності. Після того, як власник домену електронної пошти впевнений, що він розгорнув SPF і DKIM на всіх своїх потоках електронної пошти, власник домену може змусити діяти проти електронної пошти, яка не відповідає DMARC. Дія, яку можна вжити - або, точніше, політика, яку може опублікувати власник домену, - це або поставити карантин, або відхилити електронну

пошту. Карантин зазвичай означає надсилання електронної пошти в папку зі спамом, яка не вдається перевірити DMARC, але якщо оператор не реалізує традиційну папку зі спамом, оператор може підсилити агресивність фільтрації спаму під час обробки невідповідної електронної пошти. Відхилити, однак, означає повністю заблокувати будь-яку електронну пошту, яка не проходить перевірку DMARC.

Власники доменів, як правило, прагнуть дійти до політики відхилення, оскільки це забороняє несанкціоноване використання домену, що в підсумку є досить сильним заходом проти фішингу. Однак, що важливіше для більшості, електронну пошту, сумісну з DMARC, набагато легше обробляти, що різко робить DMARC вимогою для кожного, хто хоче надійно доставити свою електронну пошту.

Саме за такою методикою працює технологія DMARC. І саме так вона використовує домени, щоб полегшити ідентифікацію електронної пошти.

2.6 Переваги технології DMARC

DMARC - це не продукт, це швидше доступна технічна специфікація, яка додає нові функції до електронної пошти. Зараз DMARC широко підтримується в Інтернеті, що дозволяє кожному, хто володіє доменом електронної пошти, скористатися перевагами функцій DMARC. Коли люди говорять про розгортання DMARC, вони говорять про:

- використання функцій DMARC для виявлення всіх законних джерел електронної пошти,
- впевненість що кожне, або окреме джерело надсилає електронні листи, що відповідають методу DMARC
- оприлюднення звіту про те, що кожне, або окреме джерело відповідає стандартам DRARC, та його можна використовувати по всьому світу

Розгортання DMARC виграє дві сфери, одна технологічна та одна, пов’язана з технологічними процесами.

З технологічної точки зору, DMARC полегшує ідентифікацію електронної пошти, забезпечуючи загальний спосіб прив’язки домену до електронного листа. Людям, які надсилають електронні листи, повідомляється, як саме ідентифікувати їх, щоб ті, хто отримує електронну пошту, могли виконувати просту послідовну перевірку кожного листа, який вони отримують.

Переваги спрощення ідентифікації електронної пошти потрапляють у 3 випадки використання високого рівня:

- захист від шахрайства,
- спрощена доставка
- репутація домену.

Первинним варіантом використання DMARC була боротьба з фішингом. Якщо ви розгорнете DMARC і зробите всю вашу законну електронну адресу легкою для ідентифікації, ви можете повідомити про відхилення електронної пошти, яка, як стверджується, надходить з вашого домену, але її не вдається перевірити DMARC. Це ефективно створює доменний канал, який забороняє несанкціонований доступ. Це потужний антифішинг-контроль, який використовувався для боротьби з величезною кількістю шахрайства на основі електронної пошти.

Метод DMARC для спрощення ідентифікації електронної пошти породив другий і, можливо, більший варіант використання - спрощення доставки електронної пошти. Проблема, з якою стикаються відправники електронної пошти - особливо відправники, які створили бізнес на основах до вимог надійної та своєчасної доставки електронної пошти, - полягає в тому, що електронну пошту в історії ніколи не було легко визначити надійним способом.

Це змусило одержувачів електронної пошти вкладати величезні витрати часу, грошей та людських годин у розробку технології, яка відфільтровує погану або небажану електронну пошту. Ці фільтри ефективні проти великої кількості спаму, менш ефективні проти невеликих партій спаму і не надто ефективні проти окремих небажаних повідомлень, таких як фішинг. Найгірше що, приймачі електронної пошти

зазнають серйозних санкцій, якщо механізм боротьби зі спамом помилково видаляє частину законного електронного листа.

Надсилання електронної пошти, сумісної з DMARC, дозволяє одержувачам радикально спростити правила фільтрації. Замість того, щоб змушувати свою електронну пошту переміщатися лабіринтом динамічно генерованих та постійно змінюваних правил фільтрації, можна просто зробити свою електронну пошту легкою для ідентифікації та надсилання електронних листів іншими людьми. Замість того, щоб грати у гру намагання відфільтрувати погані речі та змусити одержувачів намагатись визначити різницю між експертом-злочинцем та законним відправником за допомогою недбалої практики, DMARC дозволяє одержувачам легко розпізнавати та доставляти потрібні електронні листи.

Ця перевага перетворює DMARC на «обов'язкове» рішення для кожного, хто потребує надійної доставки електронної пошти. Якщо ви не надсилаєте електронну пошту, сумісну з DMARC, ви змагаєтесь із злочинцями у дедалі важчій гонці за вхідними повідомленнями.

З цим тісно пов'язаний третій варіант використання DMARC: репутація домену електронної пошти.

Репутація домену - це те, що відбувається, коли одержувачі електронної пошти будують рішення щодо доставки та фільтрації на основі домену, який зв'язаний з частиною електронної пошти, на відміну від IP-адреси сервера, який намагається доставити електронну пошту, або те, чи є вміст електронної пошти безпечним чи ні. Іншими словами, DMARC привносить в електронну пошту стабільні ідентифікатори на рівні домену і дозволяє отримувачам електронної пошти замінити складності набагато простішою моделлю - доставляти електронну пошту, сумісну з DMARC, яку хочуть люди.

Захист від шахрайства, спрощена доставка та репутація домену - це 3 великі технологічні переваги розгортання DMARC. Однак є додаткові переваги, які отримує процес розгортання DMARC.

Розглядаючи розгортання DMARC як проект, організація може отримати користь від роботи з розгортання на додаток до технологічних переваг, щойно описаних. Переваги проекту включають створення функції управління доменом та використання DMARC як способу забезпечення дотримання практики електронної пошти в організації - у тому числі у постачальників та партнерів, які можуть надсилати електронні листи від імені організації.

Перевага створення та встановлення функції управління доменом виходить за рамки DMARC. Ця функція - це лише адміністративний процес відстеження реєстрації та обслуговування доменів. Функція управління доменом в кінцевому підсумку створює портфель доменів, який використовується для відстеження використання доменів, відповідальності за будь-який даний домен та встановлення всіх відповідних елементів керування у всіх доменах. Елементи керування можуть включати DMARC, сертифікати SSL для веб-сайтів, незалежно від того, чи активно використовується домен, чи зареєстрована дата. Ця функція впорядковує розгортання DMARC і в кінцевому підсумку приносить користь організації завдяки оперативній ефективності та покращенню видимості портфеля доменів організації.

Останньою перевагою, яку приносить DMARC, є нове: уявлення про те, як домени електронної пошти використовуються у всій організації та її партнерах. Тепер можна виміряти відповідність, пов’язану з використанням SPF, DKIM та DMARC, якщо трафік переходить через правильні домени та якщо партнери правильно надсилають електронну пошту від імені організації. Ця нова функціональність піднімає електронну пошту як засіб спілкування до того, що можна контролювати як частину поточного організаційного управління.

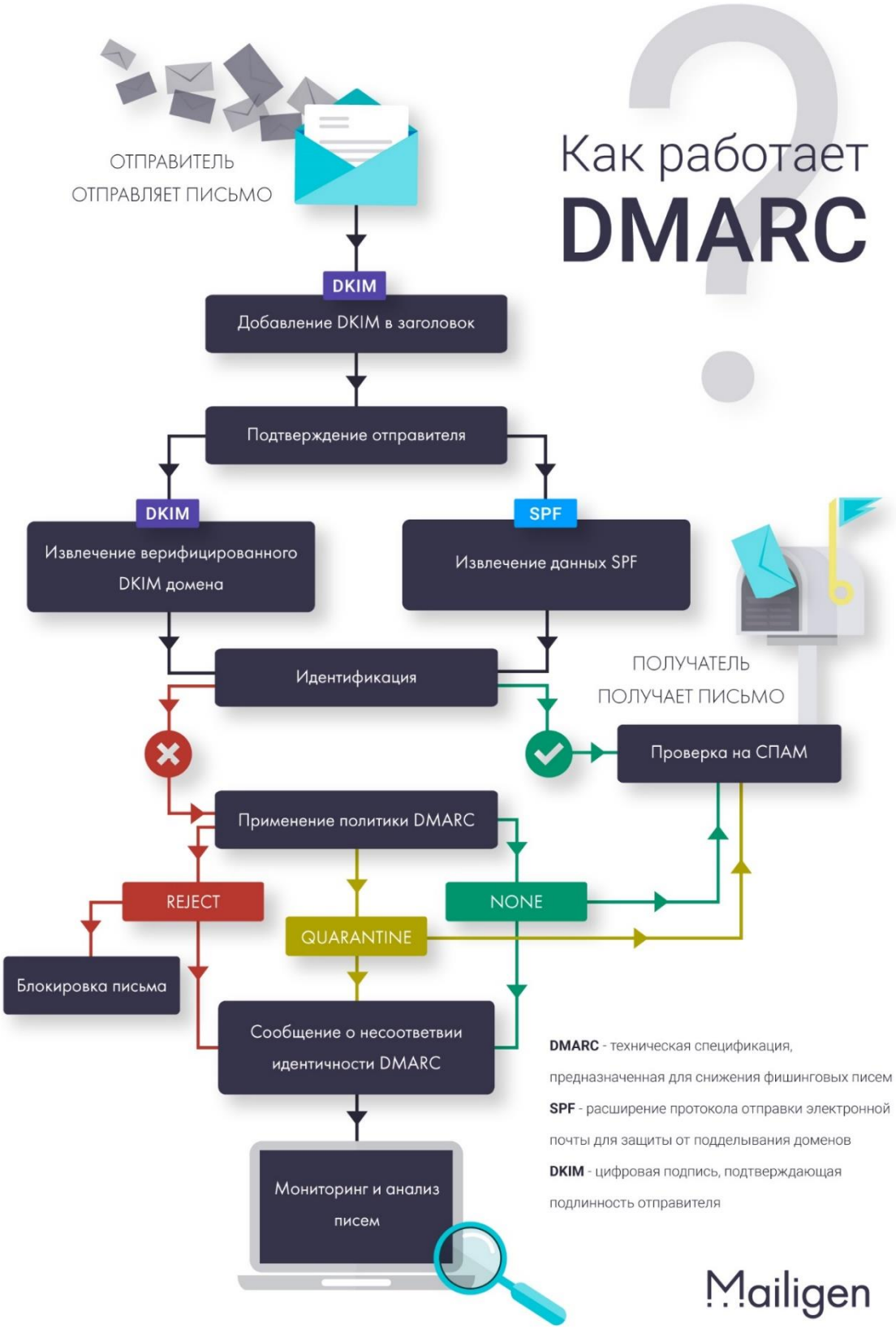


Рис. 2.5 Принцип роботи DMARC

Висновок до розділу 2

В даному розділі було розглянуто основні способи розпізнавання спаму, та основні способи протидії типовим випадкам спаму. Також розглянуто комплексний підхід до захисту інформаційно-комунікаційних систем за допомогою технічної специфікації DMARC. Приведені основні відомості про даний спосіб протидії спаму, наведені приклади видів ідентифікації електронної пошти, приклади звітів, та інше. Розглянуто основні переваги такого підходу в сучасному світі та побудовано цільну картину про те як працює DMARC.

3 ПРАКТИЧНИЙ ТЕСТ ТЕХНІЧНОЇ СПЕЦИФІКАЦІЇ DMARC НА СПАМ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІЙ СИСТЕМІ

DMARC намагається створити зв'язок між вмістом електронної пошти та доменом за допомогою SPF або DKIM.

Вміст електронної пошти, яким займається DMARC, - це домен, знайдений у заголовку «Від кого». Заголовок «Від кого» - це майже єдиний шматок інформації, який вказує, хто або звідки надходить електронний лист, який повинен бути в тому, що вважається "добре сформованим електронним листом". Саме тому DMARC знаходить домен в заголовку «Від кого».

DMARC не знаходить жодного іншого заголовка, включаючи заголовок «Відправник». Виявляється, дозволення декількох ключів політики викликає багато плутанини і навіть може підірвати корисність самого DMARC, і тому ключі DMARC знаходяться лише в домені, знайденого в заголовку «Від кого».

SPF і DKIM - це обидві технології, які виробляють стабільні ідентифікатори на рівні домену. SPF та DKIM - це вільно доступні технічні специфікації, які широко застосовуються у багатьох різних постачальників електронної пошти. Незважаючи на те, що вони займаються своїми справами по-різному, DMARC дбає лише про результати, які вони дають, і якщо ці результати мають якесь відношення до домену, знайденого в заголовку «Від кого». Результати, отримані SPF та DKIM, у світі DMARC називають «автентифікованими ідентифікаторами».

Ключовою концепцією DMARC є «Вирівнювання ідентифікатора». Це просто чудовий спосіб показати, що результати SPF та DKIM повинні бути пов’язані з доменом DMARC, щоб бути корисними. Основна причина цього полягає в тому, що одержувачам потрібен простий спосіб зрозуміти, чи результати SPF та DKIM мають відношення до домену, який має DMARC.

3.1 Приклад роботи DMARC

Отже ми зрозуміли, що DMARC працює за технікою «Вирівнювання ідентифікатора» результатів SPF та DKIM. І щоб більш наглядно зрозуміти як це працює, потрібно навести приклади різних комбінацій автентифікованих ідентифікаторів з метою продемонструвати, чому вирівнювання ідентифікаторів важливо з точки зору одержувача електронної пошти.

У цьому першому прикладі (рис3.1) одержувач електронної пошти отримав електронний лист, де домен DMARC (тобто домен, що міститься в заголовку «Від кого») – «bank.com». Крім того, перевірка SPF дала домен «bank.com». На електронному листі не було підпису DKIM, тому наш рядок позначено як «немає». Одержувач електронної пошти шукає будь-який позитивний сигнал про те, що електронну пошту можна простежити до домену «bank.com», і одержувачу електронної пошти байдуже, чи надходить цей сигнал від SPF або DKIM – головне, що сигнал є. У цьому прикладі автентифікованим ідентифікатором, який надійшов від SPF, було «bank.com», що точно відповідає домену DMARC, тому електронна пошта відповідає DMARC.

From:	SPF	DKIM
bank.com	bank.com	(none)

Рис. 3.1 Позитивна перевірка листа через SPF

У цьому наступному прикладі (рис. 3.2) все майже однаково, за винятком того, що автентифікований ідентифікатор, який надав SPF, є субдоменом bank.com - mail.bank.com. Для людини, що є необізнаною, ці два домени очевидно пов’язані. Однак виявляється, що в Інтернеті не існує стандартного способу з’ясувати, чи bank.com - це домен верхнього рівня, наприклад .com або .org, або домен другого рівня. Використовуючи деякі ресурси з Інтернету, зокрема список публічних суфіксів, який веде Фонд Mozilla, одержувач електронної пошти може з’ясувати цей банк. com

- це організаційний домен, а mail.bank.com - це субдомен, який використовує той самий організаційний домен, що і bank.com. У цьому випадку електронна пошта відповідає DMARC.

From:	SPF	DKIM
bank.com	bank.com	(none)
bank.com	mail.bank.com	(none)

Рис. 3.2 Автентифікований ідентифікатор є субдоменом

Третій приклад (рис. 3.3) показує щось цікаве. Замість того, щоб SPF надав автентифікований ідентифікатор bank.com або субдомен bank.com, автентифікованим ідентифікатором є banknewsletter.com. Наскільки нам відомо, banknewsletter.com - це реальний домен, який належить і управляється тим самим суб'єктом, який володіє bank.com. АБО banknewsletter.com належить і управляється злочинцями, які хочуть обдурити людей, щоб вони думали, що вони законні. Немає способу надійно підтримувати та передавати такі асоціації між доменами - або самими відправниками, які створюють бази даних асоціацій, або одержувачами, що підтримують свої власні - і те, і інше є завданнями, які можуть бути чреватими неточностями і в основному підривати корисність DMARC. Отже, цей електронний лист НЕ відповідає DMARC і на нього впливає політика DMARC.

From:	SPF	DKIM
bank.com	bank.com	(none)
bank.com	mail.bank.com	(none)
bank.com	banknewsletter.com	(none)

Рис. 3.3 Неточність в адресі відправника

В четвертому прикладі, (рис. 3.4) електронна пошта така сама, за винятком того, що ми вперше бачимо підпис DKIM. У цьому прикладі DKIM створив автентифікований ідентифікатор bank.com, що робить приклад сумісним із DMARC. Тобто отримувач електронної пошти переглядає автентифікований ідентифікатор, який надійшов від SPF, і бачить, що banknewsletter.com не має нічого спільного з bank.com, і просто ігнорує його. Оскільки приймач шукає будь-який позитивний сигнал про те, що повідомлення справді надійшло від bank.com, а DKIM надає такий сигнал, електронне повідомлення проходить перевірку DMARC.

From:	SPF	DKIM
bank.com	bank.com	(none)
bank.com	mail.bank.com	(none)
bank.com	banknewsletter.com	(none)
bank.com		bank.com

Рис. 3.4 Позитивна перевірка листа через DKIM

В п’ятому прикладі (рис 3.5) показує електронну пошту, яка повністю відповідає DMARC. І SPF, і DKIM дали автентифіковані ідентифікатори bank.com. Приймач піклується лише про пошук позитивного сигналу, тому наявність 2 позитивних сигналів подвійно хороший, але не означає нічого більше, ніж «позитивний сигнал»

From:	SPF	DKIM
bank.com	bank.com	(none)
bank.com	mail.bank.com	(none)
bank.com	banknewsletter.com	(none)
bank.com	banknewsletter.com	bank.com
bank.com	bank.com	bank.com

Рис. 3.5 Повна відповідність DMARC

Цей 6-й приклад (рис. 3.6) показує те саме що і приклад на рисунку 3.5, з тією різницею, що “news.bank.com” є автентифікованим ідентифікатором як для SPF, так і для DKIM. Це досить поширена практика для великих організацій делегувати субдомен провайдеру послуг електронної пошти, щоб постачальник послуг міг надсилати електронні листи від імені організації. У цьому прикладі власники bank.com могли делегувати субдомен «новини» своєму постачальнику маркетингу, щоб він міг надіслати електронний лист, сумісний з DMARC, за допомогою bank.com.

From:	SPF	DKIM
bank.com	bank.com	(none)
bank.com	mail.bank.com	(none)
bank.com	banknewsletter.com	(none)
bank.com	banknewsletter.com	bank.com
bank.com	bank.com	bank.com
bank.com	news.bank.com	news.bank.com

Рис 3.6 Домен та субдомен

Цей вигаданий приклад (рис 3.7) показує, що кожен може зареєструвати домени та встановити SPF та DKIM. Те, що SPF та DKIM передають і видають автентифікований ідентифікатор, ще не означає, що з електронною поштою все добре.

From:	SPF	DKIM
bank.com	bank.com	(none)
bank.com	mail.bank.com	(none)
bank.com	banknewsletter.com	(none)
bank.com	banknewsletter.com	bank.com
bank.com	bank.com	bank.com
bank.com	news.bank.com	news.bank.com
bank.com	crime.net	badguys.com

Рис. 3.7 Вигаданий приклад електронної пошти

Останній приклад (рис 3.8) показує, що SPF дав автентифікований ідентифікатор «bark.com». Це добре відома атака, яку деякі шахраї використовують для обману людей, які вручну перевіряють шматки електронної пошти для визначення законності. Швидкий погляд може обдурити око і змусити когось подумати, що відправник насправді є банком. Гірше того, можна скористатися деякими прийомами кодування символів, щоб відтворені гліфи виглядали точно так, як відображається домен. Але машину таким способом обхітрити не вийде, саме тому машини повинні виконувати перевірки вирівнювання ідентифікаторів, а не люди.

From:	SPF	DKIM
bank.com	bank.com	(none)
bank.com	mail.bank.com	(none)
bank.com	banknewsletter.com	(none)
bank.com	banknewsletter.com	bank.com
bank.com	bank.com	bank.com
bank.com	news.bank.com	news.bank.com
bank.com	crime.net	badguys.com
bank.com	bark.com	(none)

Рис. 3.8 Підробка способом «схожого слова»

3.2 Як DMARC формує звіти

Коли одержувач електронної пошти обробляє шматок електронної пошти в контексті DMARC, одержувач витягує домен, знайдений у заголовку «Від кого». Цей домен лежить в основі того, де приймач шукає будь-який відповідний запис DMARC. Приймач ляпає префікс underbar-dmarc домену і запитує DNS для запису TXT.

У наведеному тут прикладі витягнутим доменом є EUROPE.ENG.EXAMPLE.ORG. Одержувач додасть underbar-dmarc до цього домену та запитує DNS, щоб спробувати знайти запис TXT. Якщо запит відхилено або нічого не знайдено, то одержувач витягує організаційний домен із домену. В нашому

випадку EXAMPLE.ORG і повторює спробу знайти запис DMARC, додаючи under-dmarc перед доменом і запитуючи запис TXT.

Таким чином, виявлення записів DMARC обмежується лише 2 пошуками DNS. Це дає деякі чудові переваги. Ви можете опублікувати один запис DMARC на рівні організаційного домену, і він може охоплювати всі та будь-які піддомени. Не має значення, чи створює спамер власні субдомени, ви все одно можете опублікувати запис DMARC, який охоплює їх, не вимагаючи публікувати інші записи DMARC для всіх можливих субдоменів. (рис3.8) Інша чудова річ полягає в тому, що ви можете публікувати записи DMARC для всіх своїх реальних субдоменів, і ці записи DMARC замінять те, що публікується на рівні організаційного домену.

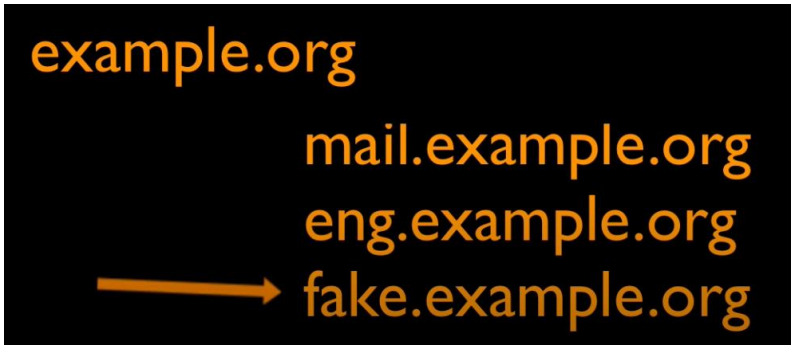


Рис. 3.9 Покриття субдоменів за допомогою одного домену

Записи DMARC - це прості списки пар тегів / значень. Це приклад домену, який опублікував запис DMARC. Ми точно можемо сказати що це DMARC-запис, оскільки він починається з «v = DMARC1;». Він має політику ap = none та просить надіслати всі зведені звіти на основі XML до report@example.org для обробки. DMARC був розроблений, щоб дозволити доменам збирати інформацію, не впливаючи на електронну пошту, і саме так це робиться – «вмикаючи» політику ap = none.

Усі записи DMARC повинні починатися з тегу версії протоколу. Після цього політику можна налаштувати. Можна налаштувати політику, яка застосовуватиметься до будь-яких субдоменів, наприклад: якщо ви знаєте, що ваш домен ніколи не використовує піддомени, ви можете задати політику sp = reject, збираючи дані лише у вашому організаційному домені, використовуючи p = none. Тег

pct схожий на повзунок, який переходить від 0 до 100, так що будь-яка опублікована політика може бути розгорнута повільно, наприклад: якщо ви задасте pct = 1, тоді лише на 1 із кожних 100 електронних листів вплине політика DMARC

Ви також можете налаштувати, чи повинні автентифіковані ідентифікатори, надані SPF та DKIM, точно відповідати домену DMARC. За замовчуванням "розслаблений" є переважним майже у всіх випадках, але в "суворому режимі" ви можете заборонити вирівнювання ідентифікатора, яке базується на піддоменах, можливо, якщо ви перебуваєте в середовищі, де у вас немає контролю над надісланим електронним листом використання делегованих субдоменів.

Наступні два теги, rua та ruf, використовуються, щоб повідомити світові, куди надсилати звіти для домену. Оскільки звіти різні, люди надсилають звіти на різні електронні адреси для збору та аналізу.

Останні теги стосуються налаштування форматів звітів, інтервалів та часу надсилання відредагованих копій окремих електронних листів, які не відповідають DMARC. Перші два теги мають лише 1 значення, тому вони трохи марні, і, як видається, остання опція вимикає генерацію звітів деякими постачальниками звітів через помилки програмного забезпечення, тому, можливо, залиште їх, якщо ви хочете їх зібрати.

3.3 Політика DMARC

Варіанти політики DMARC дуже прості. Ви можете опублікувати політику "жодного", що означає "будь ласка, надсилайте мені звіти, не діючи по електронній пошті, яка не проходить перевірку DMARC". Ви можете опублікувати політику "карантину", яка спрямовує одержувачів до папки зі спамом до будь-якого електронного листа, який не вдається перевірити DMARC. Якщо папка зі спамом не існує, одержувач може зробити все, що в їх силах, щоб поводитися з повідомленням із вищим ступенем підозри, наприклад, підсилюючи агресивність сканування проти спаму.

Останньою політикою, яку можна застосувати, є політика “відхилити”, яка спрямовує одержувачів блокувати - або відмовлятися приймати - електронну пошту, яка не проходить перевірку DMARC. На одному екрані ви побачите трохи більше про тег pct, і як, якщо ви використовуєте його разом із наявною політикою відхилення, тоді будь-який відсоток електронної пошти, який не відхилено через тег відсотків, замість цього бути на карантині.

Нарешті, дві форми звітів про зворотний зв'язок, які DMARC може надати, дуже різні. Сукупні звіти на основі XML генеруються протягом 24 годин та містять вичерпну статистику про те, як отримувач електронної пошти бачить, як використовується його домен, включаючи всю електронну пошту, яка повністю пройшла DMARC. Другий тип зворотного зв'язку складається з відредагованих копій окремих електронних листів, які не отримали підтвердження SPF, DKIM або їх обох. Ці звіти не завжди доступні через проблеми конфіденційності, проблеми з обсягом, або думку, що вони не потрібні для точного розгортання DMARC.

Option	Purpose	Example	Default
v	Protocol version	v=DMARC1	n/a
p	Policy for the domain	p=quarantine	(required)
sp	Policy for subdomains	sp=reject	p= value
pct	% of msgs subject to policy	pct=20	100
adkim	DKIM alignment mode	adkim=s	r
aspf	SPF alignment mode	aspf=r	r
rua	Aggregate reporting URI	rua=mailto:aggrep@example.org	n/a
ruf	Forensic reporting URI	ruf=mailto:fails@example.org	n/a
rf	Forensic reporting format	rf=afrf	afrf
ri	Aggregate reporting interval	ri=14400	86400
fo	Forensic reporting options	fo={0,1,d,s}	0

Рис. 3.10 Опції DMARC

Висновок до розділу 3

В даному розділі був проведений тест технічної специфікації DMARC та реагування її на різного роду поштові запити. На основі проведеного тесту, можна сказати, що DMARC є чудовим рішенням проблем спаму в корпоративній мережі. DMARC має гнучкі опції налаштуваннь та без проблем справляється з більшістю небажаних листів.

ВИСНОВКИ

В магістерській роботі приведені теоретичні відомості про інформаційні мережі, системи та корпоративні мережі. Також приведено приклади найбільш типових атак на такі мережі за допомогою поштового спаму. В роботі приведені основні і прості способи захистити будь яку мережу, або вашу особисту пошту, від спаму.

Крім того, детально досліджено найпопулярніші види спаму, не залежно від цілі злоумисника та його намірів. Розібрано найбільш гучні справи в сфері спаму в мережі.

Детально розібрано як працює ефективна технічна специфікація DMARC. Наведені плюси та мінуси даного виду захисту від спаму, а також показано як формуються звіти для детального аналізу.

Дані рекомендації можуть бути використані системними адміністраторами та адміністраторами безпеки при налаштуванні системи захисту корпоративних webресурсів або звичайними користувачами при налаштуванні домашньої системи захисту.

Варто зазначити, що створені рекомендації не дають сто відсоткової гарантії забезпечення необхідного рівня безпеки інформації. Створені рекомендації дозволяють збільшити тривалість проведених атак, а також унеможливити успішність атаки у випадку обмеженості технічних ресурсів порушника.

В наш час дуже важко сказати, які загрози ябо які способи захисту від цих загроз з’являться завтра. Прогрес йде настільки швидко, що наше покоління просто не встигає за цим, швидкоплинним процесом. Ще вчора ви користувалися телефоном, натискаючи на ньому кнопки. А вже завтра ви будете керувати їм за допомогою тільки ваших очей використовуючи eye-tracker. І слід розуміти, що це відноситься не тільки до сфери телефонів або якихось гаджетів.

ПЕРЕЛІК ПОСИЛАННЬ

1. «Основы веб-хакинга. Нападение и защита» / Юрій Жуков // Видавнитство – Пітер. 2012 - 208с
2. «Безпека веб сайтів або зворотній відлік до злому». [Електронный ресурс] – Режим доступу: World Wide Web. – URL: filandor.com
3. Список інструментів технічної специфікації DMARC
4. DMARC – загальні відомості [Електронный ресурс] – режим доступу: World Wide Web. – URL: wikipedia.com
4. Закон України "Про електронні документи та електронний документообіг" від 22 травня 2003 р. № 851-IV;
5. Закон України "Про захист інформації в автоматизованих системах"
6. Інформаційна сторінка технології DMARC. [Електронный ресурс] – Режим доступу: World Wide Web. – URL: dmarcian.com
7. «Anti-Spam Measures: Analysis and Design» [Книга] / Guido Schryen.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ
(ПРЕЗЕНТАЦІЯ)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНОРМАЦІЇ
КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Магістерська роботи

на тему

«ТЕХНОЛОГІЯ ЗАХИСТУ ВІД СПАМУ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ»

Виконав: Студент групи
БСДМ-61 Роде О.О.
Керівник: Кожухівський А.Д.

Об'єкт дослідження – захищеність інформаційно-комунікаційних систем.

Предмет дослідження – види реагування програмного забезпечення на спам, або спам-атаки

Мета роботи – дослідження засобів ефективного захисту інформаційних систем від спам

Актуальність – Одним із найважливіших напрямків розвитку ринку телекомунікацій України є формування та розвиток національного сегмента інформаційного суспільства і входження нашої країни до світової інформаційної спільноти. Робота присвячена одному з важливих напрямків розвитку телекомунікацій – захист корпоративних мереж від спаму. Тому тема магістерської роботи є актуальною завжди і своєчасною.

ЗАВДАННЯ РОБОТИ:

- Розібрати теоретичні відомості про інформаційно-комунікаційні системи та принципи їх роботи
- Розглянути основні типи атак та основні типи методи захисту від спаму в корпоративних мережах
- Розробити рекомендації щодо комплексного захисту мережі від спаму
- Провести практичний тест методів захисту мережі від спаму
- Зробити висновки

Інформаційно-комунікаційні системи

Говорячи про інфомаційні технології, можна посилатися на різні критерії в залежності від контексту вживання терміна.

А саме:
1.Мережі. Йдеться як про радіо- і телевізійних мережах, так і про стаціонарних і мобільних мережах.

2.Термінали і обладнання. Маються на увазі всі типи пристроїв, через які працюють інформаційні та комунікаційні мережі. Наприклад, комп'ютери, планшети, мобільні телефони, аудіо- та відеотехніка, телевізори, ігрові приставки і т.д.

3.Послуги. Йдеться про широкий спектр послуг, пропонованих за допомогою вищевказаних ресурсів. Наприклад, поштові служби, хмарне сховище, дистанційне навчання, електронний банкінг, онлайн ігри, розважальні сервіси, віртуальні спільноти та блоги.

Види спаму

- Види спаму
- Реклама
- Нігерійські листи
- Фішинг
- Інші види спаму
- Електронна пошта
- Usenet
- Миттєві повідомлення
- Блоги, Вікі
- Підміна інтернет-трафіку
- SMS-повідомлення
- Телефонні дзвінки

Захист від спаму в мережі

Якщо ви помітили, що ваша компанія, здається, отримує багато спаму, ви можете зробити щось для боротьби з цим:

- Налаштуйте програму, яка фільтрує спам.
- Список електронної пошти співробітників завжди повинен бути конфіденційним. Якщо хтось за межами компанії потребує вашої адреси електронної пошти, надішліть йому більш загальний електронний лист, який ви використовуєте, не пов'язаний з електронною адресою вашої компанії та інформацією, що зберігається в ній.
- Встановіть у своєму офісі політику користування Інтернетом для співробітників. Це один з найкорисніших кроків у захисті вашої компанії від спаму та подальших кібератак. Політика повинна містити вказівки щодо таких речей, як загальна безпека, прийнятне використання Інтернету, використання особистого обладнання та безпека офісних служб. Переконайтеся, що всі співробітники підписують копію політики користування Інтернетом і щороку переглядають її.

DMARC

DMARC - це технічна специфікація, яка описує, як відправники електронної пошти можуть полегшити ідентифікацію своєї електронної пошти за допомогою існуючих безкоштовних та відкритих технологій. Електронна пошта, сумісна з **DMARC**, дуже проста в обробці, і основні одержувачі електронної пошти вже прийняли DMARC як звичайний спосіб з'ясувати основну ідентичність електронного листа.

Зараз, оскільки кожен може придбати домен і поставити **SPF** і **DKIM** на робочу систему (включаючи злочинців!), Результати обробки **SPF** і **DKIM** - тобто автентифікованих ідентифікаторів - повинні бути пов'язані з доменом, який знаходиться в заголовку «Від кого» ,який в свою чергу пов'язаний з **DMARC**. Ця концепція називається ***«вирівнювання ідентифікатора»***. Отримання ідентифікаторів для вирівнювання закінчується великою частиною роботи з розгортання **DMARC**.

Робота DMARC

From:	SPF	DKIM
bank.com	bank.com	(none)

Позитивна перевірка листа через SPF

From:	SPF	DKIM
bank.com	bank.com	(none)
bank.com	mail.bank.com	(none)

Автентифікований ідентифікатор є субдоменом

Робота DMARC

From:	SPF	DKIM
bank.com	bank.com	(none)
bank.com	mail.bank.com	(none)
bank.com	banknewsletter.com	(none)

Неточність в адресі відправника

From:	SPF	DKIM
bank.com	bank.com	(none)
bank.com	mail.bank.com	(none)
bank.com	banknewsletter.com	(none)
bank.com		bank.com

Позитивна перевірка листа через DKIM

From:	SPF	DKIM
bank.com	bank.com	(none)
bank.com	mail.bank.com	(none)
bank.com	banknewsletter.com	(none)
bank.com	banknewsletter.com	bank.com
bank.com	bank.com	bank.com

Повна відповідність DMARC

From:	SPF	DKIM
bank.com	bank.com	(none)
bank.com	mail.bank.com	(none)
bank.com	banknewsletter.com	(none)
bank.com	banknewsletter.com	bank.com
bank.com	bank.com	bank.com
bank.com	news.bank.com	news.bank.com

Домен та субдомен

Робота DMARC

From:	SPF	DKIM
bank.com	bank.com	(none)
bank.com	mail.bank.com	(none)
bank.com	banknewsletter.com	(none)
bank.com	banknewsletter.com	bank.com
bank.com	bank.com	bank.com
bank.com	news.bank.com	news.bank.com
bank.com	crime.net	badguys.com

Вигаданий приклад електронної пошти

Робота DMARC

From:	SPF	DKIM
bank.com	bank.com	(none)
bank.com	mail.bank.com	(none)
bank.com	banknewsletter.com	(none)
bank.com	banknewsletter.com	bank.com
bank.com	bank.com	bank.com
bank.com	news.bank.com	news.bank.com
bank.com	crime.net	badguys.com
bank.com	bark.com	(none)

Підробка способом «схожого слова»

Опції DMARC

Option	Purpose	Example	Default
v	Protocol version	v=DMARC1	n/a
p	Policy for the domain	p=quarantine	(required)
sp	Policy for subdomains	sp=reject	p= value
pct	% of msgs subject to policy	pct=20	100
adkim	DKIM alignment mode	adkim=s	r
aspf	SPF alignment mode	aspf=r	r
rua	Aggregate reporting URI	rua=mailto:aggrep@example.org	n/a
ruf	Forensic reporting URI	ruf=mailto:fails@example.org	n/a
rf	Forensic reporting format	rf=afrf	afrf
ri	Aggregate reporting interval	ri=14400	86400
fo	Forensic reporting options	fo={0,1,d,s}	0

Висновки

- В даній роботі приведені теоретичні відомості про інформаційно-комунікаційні системи та те як вони працюють.
- Окремо розібраний спосіб комунікації через електронну пошту.
- Розібрані основні небезпеки при відправці , або отриманні електронного листа.
- На прикладах показано, які із сучасних способів захисту забезпечать комплексний захист від спаму в інформаційній системі.
- Проведений практичний тест DMARC.

Дякую за увагу