Сучасну систему кіберзахисту неможливо уявити без її невід'ємної складової – захисту електронної пошти. Згідно з Verizon 2019 Data Breach Investigations report більш ніж **92% шкідливого ПЗ отримується по Email**. Не незважаючи на заходи безпеки котрі вживаються компаніями **49% заражень шкідливим ПЗ відбувається саме через електронну пошту**. Чому так відбувається? Сучасні кіберзлочинці використовують різні методи, але всі вони як правило ґрунтуються на необережності та недосвідченості користувачів електронної пошти. Використовуючи так звану соціальну інженерію, кіберзлочинці створюють спеціальний контент орієнтований на користувачів з однаковими інтересами, на організацію чи на осіб у межах організації, вміст на основі інтересів або ролі конкретного користувача. Вони дуже часто створюють ілюзію «легітимності» вмісту, видаючи себе за керівника компанії або представників партнерів, банків тощо, що призводить до витоку конфіденційної інформації приватного або корпоративного характеру.

Сервіс infoMail розроблено саме для боротьби зі сучасними загрозами широкого спектру, що виникають в наслідок використання електронної пошти такими як віруси, шкідливе програмне забезпечення, спам, листи з посиланнями на ресурси що містять шкідливе ПЗ, виток конфіденційної інформації спричинений фішинг-технологіями, виток критичної інформації спричинений несанкціонованими помилковими або навмисними діями працівників компанії.

Сервіс infoMail має наступні компоненти та властивості

- **Антиспам / Антифішинг**
- **Антивірус**
- **Захист від нових загроз**
- **Захист від націлених атак**
- **Аналіз у «пісочниці»**
- **Забезпечення відповідності та захист даних**
- **Управління та звітність**
- **Гнучке розгортання**

- **Антиспам / Антифішинг.**

Простим, але в той же час найшвидшим та дієвим механізмом захисту від спаму та фішингових повідомлень є використання репутаційних баз даних. Під час отримання повідомлення по електронній пошті система перевіряє IP-адресу відправника та вміст на предмет наявності їх у такій базі. Якщо відповідний відправник має негативну репутацію то лист блокується. У разі якщо у базі даних немає ніяких відомостей про відправника система проводить додатковий аналіз, що базується на динамічній евристиці, аналізі заголовка, поведінки та проводить сканування на наявність шкідливого ПЗ. Після перевірки відправнику присвоюється позитивний або негативний рейтинг, котрий зберігається у репутаційній базі даних.

Ця технологія дозволяє ефективно боротися з масовими спам/фішинг-атаками так як репутаційна база постійно оновлюється у режимі реального часу. Будь-яка нова атака виявлена в одній країні автоматично блокується деінде.

- **Антивірус**

Сучасний захист не можливо уявити без надійного антивірусу. Сервіс infoMail налічує в своїй базі більш ніж **50 000 сигнатур** різних варіантів сімейств вірусів. Так само як і репутаційна база даних, база даних вірусних сигнатур постійно оновлюється у режимі реального часу. Під час перевірки антивірус аналізує вміст вкладень та за потреби проводить розпакування наявних архівів, розшифровує файли, видаляє активний вміст підозрілих файлів та HTML. Якщо система не може ідентифікувати код ні як безпечний ні як небезпечний вона проводить більш глибокий аналіз. Цей аналіз проводиться за допомогою хмарної «пісочниці» де відбувається емуляція коду та його поведінковий аналіз.

- **Захист від нових загроз**

Щоб ефективно боротися з новими кібернетичними загрозами аналітичний центр сервісу infoMail аналізує по всьому світу мільйони електронних листів на годину і може ідентифікувати новий небезпечний код за лічені хвилини. Усі підозрілі вкладення, виявлені в електронних листах блокуються для аналізу у лабораторіях інформаційної безпеки. Створена база даних постійно доповнюється та є спільним ресурсом **CYBER THREAT ALLIANCE**, який включає світових лідерів з кібербезпеки.

CYBER THREAT ALLIANCE

Check Point SOFTWARE TECHNOLOGIES LTD.

CISCO

FORTINET

paloalto NETWORKS

McAfee Together is power.

infocom

- **Захист від націлених атак**

– захист від переходу за посиланням

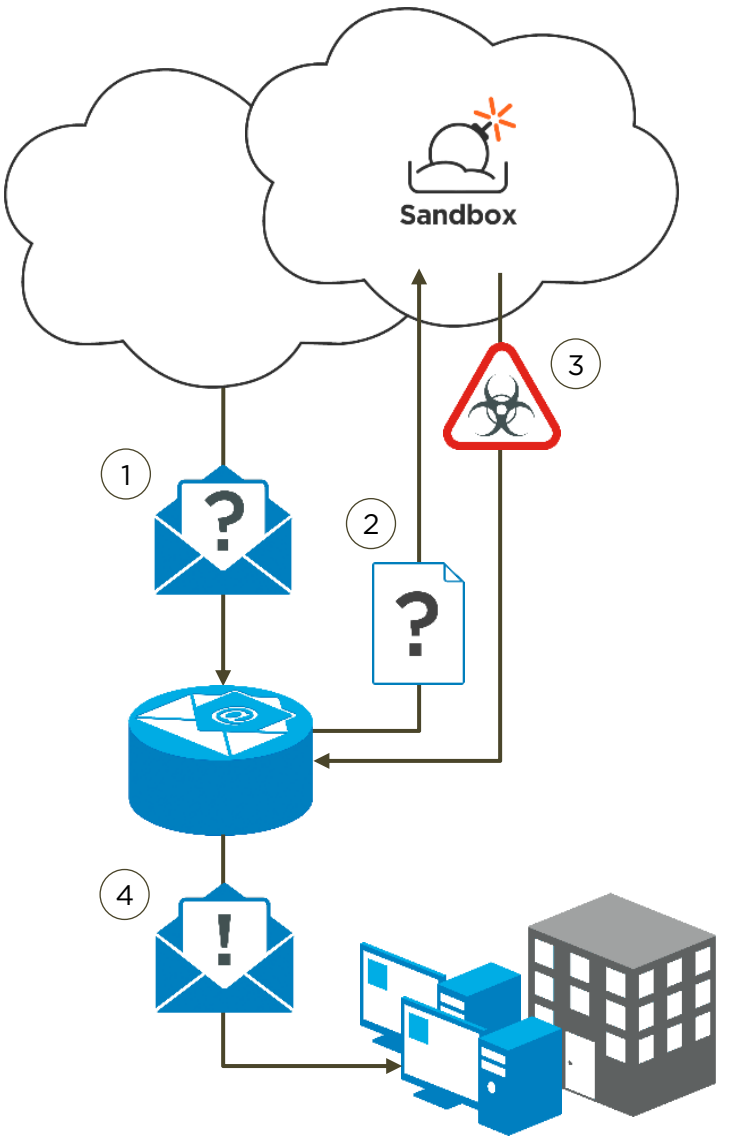
Сервіс infoMail використовує ефективну тактику боротьби проти зловмисників котрі використовуючи соціальну інженерію створюють повідомлення з посиланням на цілком безпечний ресурс, а з часом змінюють вміст ресурсу на шкідливий. Як правило такі повідомлення надсилаються вночі щоб мати час для зміни вмісту сайту до того як отримувач прочитає листа. Так як під час надсилання ресурс не несе жодної загрози таки листи без проблем проходять перевірку базовими системами безпеки. В свою чергу Сервіс infoMail робить підміну оригінального посилання та коли отримувач здійснює спробу переходу за цим посиланням повторно перевіряє його на наявність загроз і тільки після цього дає доступ до ресурсу або блокує його.

- «роззброєння» та реконструкція вмісту

Сервіс infoMail автоматично аналізує файли та видаляє підозрілий вміст, такий як макроси, посилання, вбудовані об'єкти (OLE, JavaScript тощо). Після видалення підозрілого вмісту файл реконструюється для того щоб виглядати якомога ближче до оригіналу та надсилається користувачеві. Оригінальний файл поміщається у карантин користувача та є доступним після повного аналізу на основі хмарного сервісу безпеки. У разі якщо файли зашифровані система може розшифрувати їх використовуючи попередньо завантажені паролі або паролі виявлені в тексті електронного листа. За потреби сервіс також дає можливість здійснювати категорійне або селективне видалення посилань з усіх повідомлень.

- **«Пісочниця» – захист від загроз нульового дня**

Сервіс infoMail перевіряє електронні листи та надсилає підозрілі файли та посилання у хмарну «пісочницю» для подальшого аналізу. У «пісочниці» створюється віртуальне середовище у якому підозрілий код запускається так ніби він потрапив у реальну систему отримувача. Під час цієї перевірки аналізуються дії підозрілого коду, чи намагається він зв'язатися для отримання інструкцій, чи запускає будь-які процеси котрі суперечать політиці безпеки, тощо. Після перевірки система призначає відповідний рейтинг згідно якому виконуються подальші дії такі як дозвіл на доставку отримувачеві, або видалення.



- **Забезпечення відповідності та захист даних**

Попередження втрати критичних даних досягається побудовою цифрових відбитків таких файлів за допомогою ручного завантаження у систему, або автоматичного сканування загальних тек Windows. Після цього система проводить аналіз усіх файлів що надсилаються на відповідність наявним цифровим відбиткам та у разі порушення політики безпеки блокує їх надсилання.

Система також має можливість здійснювати шифрування даних за протоколами TLS & S/MIME та за протоколом ідентифікаційного шифрування для якого не потрібна додаткова ліцензія та не здійснюється обмін ключами шифрування

- **Управління та звітність**

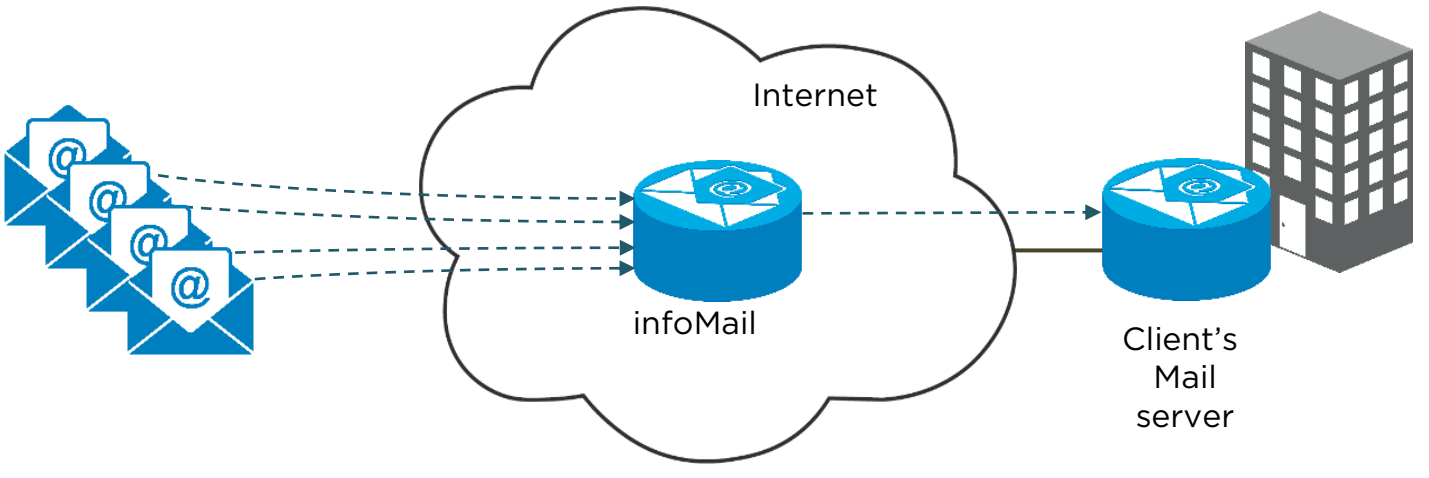
infoMail дає можливість переглядати статистику усіх користувачів надаючи вичерпну інформацію щодо загроз у реальному часі. Система дозволяє вести перехресний пошук подій з мілісекундною точністю по всім наявним журналам.

- **Гнучке розгортання**

Сервіс infoMail може бути розгорнуто у як у режимі шлюзу так і у прозорому режимі. У режимі шлюзу вся пошта надсилається на сервер infoMail та після перевірки переадресовується на клієнтський сервер. Таке підключення потребує змін у налаштуваннях клієнтського серверу.

Режим шлюзу

Пошта доставляється на infoMail, перевіряється на наявність загроз та передається на поштовий сервер клієнта.



У прозорому режимі обладнання Інфоком підключається безпосередньо перед поштовим сервером клієнта. Підключення у прозорому режимі не потребує ніяких змін у налаштуваннях.

Прозорий режим

Встановлюється як «врізка в провід». Не потрібно змінювати конфігурацію серверу.