УДК 004.056:004.773.3

ЗАГРОЗИ З ВИКОРИСТАННЯМ ЕЛЕКТРОННОЇ ПОШТИ

Патлан Є. О.
Науковий керівник – ст. викладач Олейнікова О.І.
Харківський національний університет радіоелектроніки, каф. КРіСТЗІ,
гурток «Основи інформаційної безпеки»,
м. Харків, Україна
e-mail: yehor.patlan@nure.ua

The work is devoted to the analysis of the most common e-mail threats. The main scenarios of the impact of threats are considered and the main recommendations for protecting information from threats, which are carried out by means of attacks on users' e-mails, are given.

Уже більше двох десятиліть електронна пошта – це основний інструмент для спілкування. Щодня пересилається понад 333 мільярди електронних листів по всьому світу. Цим користуються кіберзлочинці, які за допомогою атак на корпоративну електронну пошту, шкідливого програмного забезпечення, фішингових кампаній і багатьох інших методів викрадають цінну інформацію. Більшість кібератак (94%) починаються зі зловмисного електронного листа [1]. Захисту електронної пошти потребує будь-хто, хто використовує електронну пошту. Окремі користувачі, організації та компанії, які використовують електронну пошту, зазнають низки складних атак: від крадіжок облікових записів і порушень безпеки корпоративної електронної пошти до цільового фішингу й вішингу.

На сучасному етапі розвитку IT-індустрії без фішинг-листів не обходиться жодний витік персональних даних. Фішингові розсилання із відомостями, що викликають тривогу (наприклад, містять загрози щодо закриття банківських рахунків), пропонують неправдоподібно привабливі угоди, благають про пожертвування (наприклад, від імені благодійних організацій), обіцяють великі грошові вигоди з мінімальними зусиллями, насправді являють собою підготовчі кроки для нападу на клієнтів банків і електронних платіжних систем. Вийшовши на такий сайт користувач може надати зловмисникам цінну інформацію, яка дозволить їм отримати доступ до акаунтів і банківських рахунків. Головні правила, які має виконувати користувач, аби не стати жертвою фішингової атаки: не відкривати підозрілих посилань, отриманих навіть у повідомленнях від знайомих людей; не встановлювати й не запускати ігри та додатки, рекламовані у спам-розсиланнях; використовувати сучасне антивірусне програмне забезпечення. Порівняно новий різновид фішингу - вішинг. Атака спирається на використання системи попередньо записаних голосових повідомлень, мета яких – відтворити «офіційні дзвінки» від банківських та інших IVR (Interactive Voice Response) систем. Потенційна жертва отримує зазвичай запит (найчастіше через фішинг електронної пошти) про необхідність

зв’язку з банком для підтвердження або відновлення якоїсь інформації. При цьому система вимагає автентифікації користувача за допомогою введення PIN-коду або пароля. При цьому зачитується повідомлення, в якому потенційну жертву просять повідомити свої конфіденційні дані. При відповіді на дзвінок відбувається таке: автовідповідач попереджає споживача, що з його картою чиняться шахрайські дії, і дає інструкцію - передзвонити за певним номером негайно; коли за цим номером здійснено дзвінок, на іншому кінці проводу відповідає типово комп’ютерний голос, який повідомляє, що абонент має пройти звірення даних і ввести 16-цифровий номер карти з клавіатури телефону; тільки-но номер уведено, вішер стає власником всієї необхідної інформації (номер телефону, повне ім’я, адреса); далі, використовуючи цей дзвінок, можна зібрати й додаткову інформацію, таку як PIN-код, термін дії карти, дата народження, номер банківського рахунку тощо. Поряд із дуже небезпечними фішинговими та вішинговими атаками в мережі існує ще серйозніша загроза - фармінг - перенапрямлення жертви за помилковою (хибною) адресою. Для цього може використовуватися деяка навігаційна структура, скажимо файл hosts, система доменних імен. Механізм фармінгу має багато спільного зі стандартним вірусним інфікуванням. Жертва відкриває поштове послання або відвідує якийсь web-сервер, на якому виконується скрипт-вірус. При цьому спотворюється файл hosts. У результаті жертва потрапляє на один із помилкових сайтів. Механізмів захисту від фармінгу й досі не існує [2].

До найсерйозніших загроз для електронної пошти також належать ексфільтрація даних, підробка, шкідливе програмне забезпечення, спам. Ексфільтрація даних – це несанкціоноване передавання даних за межі організації вручну або за допомогою зловмисного програмного забезпечення. Шлюзи електронної пошти допомагають компаніям уникнути надсилання конфіденційних даних без авторизації, що може призвести до витоку інформації. Підробка виникає, коли кіберзлочинці маскуються під надійну особу або організацію, щоб виманювати гроші або дані за допомогою електронної пошти.

Захистити свою організацію від ураження електронної пошти можна за допомогою вбудованих засобів безпеки електронної пошти, які здатні автоматично переривати кібератаки та збільшувати продуктивність роботи системи захисту.

Список використаних джерел:

1. Що таке захист електронної пошти? Microsoft. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-email-security#:~:text (дата звернення: 16.02.2024).

2. Інформаційна та кібербезпека: соціотехнічний аспект/ В.Л. Бурячок та ін. Київ : ДУТ, 2015. 288 с.