УДК 002.513

Л. М. Ткачук
К. Ю. Василенко

АТАКА «САЛЯМІ» (SALAMI ATTACK) ЯК КІБЕРЗЛОЧИН В ЕЛЕКТРОННОМУ БАНКІНГУ

Вінницький національний технічний університет

Анотація

Проаналізовано кіберзлочин, відомий як атака «салямі», застосування даної техніки в електронному банкінгу, збиранні інформації. Розглянуто можливість виявлення та запобігання даній атаці.

Ключові слова: атака салямі, грошові рахунки, кіберзлочин, фінанси, банк, транзакції.

Annotation

Cybercrime, known as the "salami" attack, the use of this technique in electronic banking, information gathering, is analyzed. The possibility of detecting and preventing this attack is considered.

Keywords: salami attack, money accounts, cybercrime, finance, bank, transactions.

Вступ

Інформаційні системи стають однією з найбільш уразливих сторін сучасного банку, притягаючи до себе зловмисників як з числа персоналу банку, так і з інших сторін. В даний час доступ до послуг банків став можливий з різних віддалених точок, включаючи домашні термінали, любі гаджети, службові комп'ютери. Враховуючи те, що зараз інформація накопичується та обмінюється з досить високою швидкістю, яка перевищує нашу здатність уважно стежити, зловмисниками була розроблена атака «Салямі» для позбавлення частинок транзакцій, яка має жахливі наслідки на електронного банкінгу.

Результати дослідження

Атака «салямі» - це форма кіберзлочинності, яка зазвичай використовується з метою вчинення фінансових злочинів, коли злочинці крадуть гроші або ресурси як дрібну частинку за раз з фінансових рахунків у системі[1-2].

Дані атаки найбільше характерні для систем, що обробляють грошові рахунки і, отже, для банків є особливо актуальними [3].

Різні дрібні атаки, що поєднуються і утворюють масштабні атаки, які можуть вплинути на повсякденну діяльність організації, відомі як атаки салямі.

Існує два основних типи атак салямі [1]:

- Внутрішні атаки.

Це найпоширеніший тип атак салямі, який відбувається, а саме, коли особа, що працює в організації і знає про систему безпеки в організації, намагається вкрасти в організації кошти, завдаючи серйозної шкоди.

- Зовнішня атака.

Як випливає з назви, зовнішня атака є різновидом атаки салямі, яка відбувається поза організацією. В цьому випадку зловмисник використовує отриману інтернет-базу даних для вилучення інформації клієнтів, тобто даних банківських / кредитних карток або гаманців електронних платіжних систем, вставивши на сервер створену програму [4].

Найбільш типовою схемою, зображеною нападом салямі, є та, яка передбачає автоматичну модифікацію фінансових систем та їх даних. Наприклад, цифри, що представляють валюту на комп’ютерах банку, можуть бути змінені таким чином, щоб значення завжди округлялися нижче необхідного. Оскільки ці округлення вниз призводять до накопичення частки копійок, їх потрібно

перерахувати в інше місце обережно, щоб не став очевидним чистий збиток для системи рахунків [3-2-5]. Це робиться шляхом простого переведення коштів на баланс, що належить злочинцю. Остаточні суми можуть бути дуже привабливими, завдяки "шматочкам", особливо коли вираховуються кошти протягом довгого періоду.

Суть цього механізму полягає в його стійкості до виявлення. Власники рахунків рідко обчислюють свої залишки до тисячних або десятитисячних відсотків і, як наслідок, нічого не запідозрюють. Навіть якщо розбіжності помічені, більшість людей швидше збережуть свою гордість, ніж скаржитимуться на помилкову цифру в якомусь далекому знаку після коми.

Назва ж “салямі” пішла від ковбаси з такою назвою, яка виготовляється з різних сортів м’яса. Таким саме чином рахунок зловмисника поповнюється за рахунок різних вкладників.

Отже, атаки даного типу переважають у крупних банках та інших фінансових організаціях. Причинами цих атак є [5]:

- похибки обчислень, які дозволяють по-різному інтерпретувати правила округлення чисел;
- великі обсяги обчислень, які необхідно виконувати при обробці рахунків.

Прикладів атаки на інформаційних джерелах можна знайти досить багато. На жаль, напади салямі розроблені так, що їх важко виявити. Надія полягає в тому, що випадкові перевірки, особливо фінансових даних, виявлять невідповідність та призведуть до виявлення загрози. Навіть крихітну помилку потрібно відстежувати, оскільки це може свідчити про набагато більшу проблему.

Пошук причин розбіжностей серйозно завадить нападу салямі. З точки зору розробки систем, такі шахрайства підсилюють критичну важливість забезпечення якості розробки програмного забезпечення протягом усього життєвого циклу.

Тому запобігти таким атаки можна тільки забезпеченням цілісності і коректності прикладних програм, що обробляють рахунки, розмежуванням доступу користувачів організацій до рахунків, а також постійним контролем рахунків на предмет витоку сум.

Висновки

Напади салямі - це жахливі фінансові шахрайства проти приватного життя шляхом масштабного збору інформації та сум. Їх природа та складність здатні затуманити найуважніших бухгалтерів системи. Підсумуємо що для того щоби визначити винуватця такого нападу, слід розглянути мотиваційні фактори, що беруть участь у нападі салямі. Страйки салямі часто мають певну форму фінансової вигоди, але їх також можна використовувати для збору інформації. Ці атаки часто здійснюють інсайдери, консультанти або будь-хто інший, хто знає систему і хоче вкрасти гроші. Постійний і точний нагляд за нашими фінансами, ретельний контроль за виплатами можуть допомогти запобігти катастрофічним наслідкам.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Michel K. Velocihackers and Tyrannosaurus superior / Kabay Michel., 1993. – 2612 с.
2.Найпоширеніші загрози безпеці комп’ютерних систем [Електронний ресурс] – Режим доступу до ресурсу: https://sites.google.com/site/zagrozu/the-team.
3.Атаки «салями» [Електронний ресурс] // Панова Г.С.. – 1999. – Режим доступу до ресурсу: https://studwood.ru/2363898/bankovskoe_delo/ataki_salyami.
4. Ясенева В. Н. Информационная безопасность / В. Н. Ясенева. – Нижний Новгород, 2017. – 198 с.
5. Бакланов в. В. Введение в информационную безопасность. Направления информационной защиты / В.В. Бакланов. – Екатеринбург: уральский государственный университет, 2007. – 235 с.
6. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом [Електронний ресурс] // Юридический портал Протокол – Режим доступу до ресурсу: https://protocol.ua/ru/kriminalniy_kodeks_ukraini_stattya_361_2/.

Ткачук Людмила Миколаївна – доцент кафедри менеджменту та безпеки інформаційних систем, кандидат економічних наук, заступник декана з навчально-методичної роботи Факультету менеджменту та інформаційної безпеки ВНТУ, e-mail: ludatkachuk2017@gmail.com.

Василенко Кристина Юріївна — студентка групи КІТС-18Б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, tina.vasylenko@gmail.com

Tkachuk Lyudmyla Mykolayivna – associate professor of Department of Management and Security of Information Systems, candidate in economics, deputy dean for educational and methodological work of the Faculty of Management and Information Security of VNTU, e-mail: ludatkachuk2017@gmail.com.

Vasylenko Krystyna Yuriyivna - student of KITS-18B group, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, tina.vasylenko@gmail.com