КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№1 (9), 2020
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2020.9.5968
УДК 004.49

Опірський Іван Романович
доктор технічних наук, доцент, професор кафедри захисту інформації
Національний Університет "Львівська Політехніка", Львів, Україна
ORCID: 0000-0002-8461-8996
ivan.r.opirskyi@lpnu.ua

Винар Андрій Сергійович
студент
Національний Університет "Львівська Політехніка", Львів, Україна
ORCID:0000-0003-2044-7590
andrii.vynar.om@gmail.com

АНАЛІЗ ВИКОРИСТАННЯ ХМАРНИХ СЕРВІСІВ ДЛЯ ФІШИНГОВИХ АТАК

Анотація. Фішинг, як різновид інформаційних атак, використовується зловмисниками у корисливих цілях уже доволі тривалий час. Вони користуються широкою популярністю у злочинному світі, оскільки людину набагато легше змусити зробити певні вигідні дії, а ніж програму. З поступовою появою нових технологій, даний тип атак крок за кроком адаптувався до нових умов взаємодії з своєю жертвою. Хмарні сервіси стали чудовим сучасним і широко-розповсюдженим інструментом реалізації фішингових кампаній. Використання таких сервісів надало своїм виконавцям перелік вагомих переваг у порівнянні з використанням власних обчислювальних ресурсів. Відносна дешевизна та простота в експлуатації даних технологій відіграла одну з важливих ролей. Проблема інформаційної безпеки перед використанням хмарних технологій фішингом полягає у тому, що даний вид атак доволі тяжко виявити, тим більше запобігти, значно не вплинувши на комфортність користування кінцевими користувачами інформаційних систем. У статті було проаналізовано актуальність такого типу атак на основі реальних даних. Розглянуто алгоритм їх роботи протягом циклу життя та проведено аналіз використання основних наявних методів захисту, їх доцільність та проблематики використання. Аналіз показав, що не всі сучасні методи захисту здатні виявляти та запобігати фішинговим атакам з використанням хмарних сервісів. Навіть поєднання декількох чи одразу усіх методів не може гарантувати захист користувача від загроз фішингу. Наведено приклади таких фішингових кампаній, які відбулися протягом 2019 року та використали такі популярні хмарні сервіси як Azure Blob storage компаній Microsoft та Google Drive від компанії Google. Також було представлено певний базовий перелік порад, який дозволить підняти рівень захищеності інтернет користувачів, щоб зменшити ризики потенційного компрометування даних чи його наслідків.

Ключові слова: соціальна інженерія; фішинг; хмарні сервіси; хмарні обчислення

1. ВСТУП

Соціально інженерія (англ. Social Engineering) це наука, яка вивчає методи та фактори впливу на людську свідомість та її переконання. Її основною метою є вивчення та аналіз причин тої чи іншої поведінки людини[1-2]. Дані цих досліджень можна використовувати як в благих так і в корисливих цілях. Соціальна інженерія має декілька простих принципів, які використовуються для маніпуляцій жертвами:

- Авторитет
- Залякування, шантаж
- Консенсус / соціальне підтвердження

- Дефіцит, рідкість
- Терміновість
- Знайомство / вподобання
- Довіра

Однією з форм соціальної інженерії, яка використовує сучасні ІТ технології є фішинг (англ. Phishing). Вона використовує цифрове середовище для заволодіння персональною, приватною чи таємною інформацією, шляхом обману своєї жертви і містить хоча б один із принципів соціальної інженерії.

На даний момент фішинг-атака може приймати різні форми. Переважно таким способом зловмисники намагаються викрасти у жертви її логін та пароль, номери кредитних карт або ж певну фінансову інформацію. Ця форма шахрайства отримала широку популярність серед шахраїв, оскільки набагато важче скомпрометувати інтернет мережу чи програмне забезпечення ніж маніпулювати людиною. Зловмиснику потрібно затратити менше зусиль для відправлення звичайного повідомлення з вимогою надати йому пароль. З часом фішинг ставав все складнішим та професіональним. Раніше електронні листи з фішинговим повідомленням можна було легко розпізнати за невідомим або замаскованим відправником, граматичними помилками в словах або з підміненими словами в доменах чи посиланнях які виглядали максимально наближеними до легітимних. Сучасні повідомлення створюються уже професіоналами і не містять попередніх помилок. Дизайн сайтів або скопійований з оригінальних або ж максимально схожий на них. Такі атаки складніше виявити навіть за допомогою сучасних методів та засобів захисту.

Фішинг є досить актуальним на сьогоднішній день. Згідно звіту PhishLabs 2019 “PHISHING TRENDS AND INTELLIGENCE REPORT” [3], протягом 2018 року кількість фішингових атак зросла на 40,9%. Це сигналізує про те, що індустрія фішингу зростає швидкими темпами. Успішність цих атак є досить високою. За даними опитування HippaJournal, 65% організацій в США успішно піддалися фішинговій атаці хоча б раз в 2019 році [4], що підкреслює важливість захисту від них.

Постановка проблеми.

Хмарні сервіси почали широко використовуватися впродовж останнього часу. Аналіз ринку, який оприлюднений в статті Forbs, доказує, що з 2018 по 2019 він зріс на 17.5% [3] і буде продовжувати зростати. Це означає, що послуги будуть продовжувати набувати широкого розголосу та популярності. Ринок кіберзлочинів також розвивається і пристосовується до нових технологій. Хакери уже опанували хмарні сервіси і почали їх використовувати у своїх цілях, а саме у реалізаціях фішингових кампаній. За даними звіту PhishLabs, використання лише безкоштовних хостингових сервісів для зловмисних цілей зросло на 10,8% починаючи з 2015 по 2018 роки. Проблемою використання хмарних сервісів для інформаційної безпеки становить складність їх виявлення та попередження. Причиною цього слугує використання зловмисниками таких принципів соціальної інженерії, як авторитетність та довіра. Усі ми звикли до того, що компанія Microsoft є одним з лідерів у сфері ІТ та дбає про свою безпеку та безпеку своїх продуктів. Тому, коли користувач бачить лист від цієї

компанії, чи посилання на їхні ресурси, йому і на думку б не прийшло, що за цим ховаються кібер-злочинці. В останні роки ці речі стали цілком реальним і несуть справжню загрозу кожному користувачу в мережі інтернет.

Аналіз останніх досліджень і публікацій.

Проблеми кібербезпеки у хмарних середовищах досліджуються багатьма науковцями та спеціалістами цієї галузі. Оскільки технології розвиваються стрімкими темпами, проявляються також нові види атак щодо цих технологій. Використання хмарних технологій у кібератаках та методи їх протидії було описано у статтях J. Singh, "Comprehensive Solution to Mitigate the Cyber-attacks in Cloud Computing" [5] та B. Gupta, N. Arachchilage and K. Psannis, "Defending against phishing attacks: taxonomy of methods, current issues and future directions" [6].

Мета статті.

Метою статті є аналіз наявних загроз інформаційній безпеці з використаннях “cloud computing” для фішингових кампаній, можливість протидії новому виду фішингу сучасними засобами захисту та визначення актуальних методів захисту.

2. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

В останні роки цифровий світ стикнувся з новим видом фішингових атак. Для їх реалізації почали використовувати хмарні SaaS [7] сервіси. Їх модель передбачає надання споживачам доступу до використання певного програмного забезпечення. Водночас модифікація програмної чи хардварної компонент не доступні. Користувач має лише змогу використовувати сервіс через спеціально створений інтерфейс. Основною перевагою фішингу з використанням хмарних технологій є простота в реалізації. Зловмиснику не потрібно прикладати багато зусиль і часу, для налаштування відповідної фішингової платформи. Більшість потрібних речей уже вам надав сам провайдер послуги, а саме забезпечив обчислювальними можливостями і безпечним доступом до них.

Розглянемо типовий сценарій простої фішингової атаки з використанням хмарних сервісів. Графічно зображений на Рисунку 1.

1. Зловмисник підготовлює хмарний сервіс для обману з вимаганням ввести персональні дані. Створює підставний профіль і робить певні надбудови для емуляції форми введення паролю.
2. Далі ці дані надсилаються як пошта нотифікація самого сервісу або ж іншою поштовою скринькою чи через канали швидких повідомлень.
3. Лист проходить перевірку міжмережевими екранами та системами виявлення/запобігання вторгнень, оскільки не містять зловмисних ознак, і потрапляє до отримувача.
1. Жертва реагує на повідомлення і, впевнившись, що у посиланні немає помилок чи підміни, відриває посилання на легітимний сервіс.

ISSN 2663 - 4023

2. Після відкриття сервісу у браузері, канал обміну інформацією стає шифрованим і сертифікат дійсно підтверджує, що сайт належить відповідній організації. Отримавши форму введення паролю, жертва його вводить.

3. Зловмисник отримує скомпрометований пароль.

Рис.1 Модель загрози фішингу з використанням хмарних сервісів

Одним з найяскравіших прикладів стала фішингова кампанія, яка використала сервіс компанії Microsoft “Azure Blob storage” [8]. Він пропонує зберігання великої кількості неструктурованих даних (документи, відео, зображення і тощо) на своїх серверах. Microsoft пропонує три моделі доступу до даних:

- Private (no anonymous access)
- Blob (anonymous read access for blobs only)
- Container (anonymous access for containers and blobs)

Окремим пунктом є можливість хостингу статичних веб сторінок, код яких зберігається у контейнерах “Azure Blob storage” [9]. Усі з’єднання з цими даними відбуваються через HTTP/HTTPS протоколи. Для цього компанією Microsoft було зареєструвала декілька суб-доменів, та придбано для них SSL сертифікати. Прикладом такого є суб-домен *.blob.core.windows.net. Під час публікації сайту, йому генерується, або задається користувачем певний ідентифікатор, який додається до домену і виглядає приблизно так Hfsj12P9fj25djT.blob.core.windows.net. Відповідно і wild-card сертифікат прикріпився під ці сайти. Кінцевий користувач, перейшовши за цим посиланням, помітив, що сайт є безпечним, оскільки використовувався протокол HTTPS та SSL сертифікат, який є дійсним та виданим компанії Microsoft. Таким чином зловмисники публікували фішингові сайти, у який вимагали ввести логін та пароль, щоб автентифікувати особу і отримати подальший доступ до ресурсу. Довіра до сайту була забезпечена трьома основними факторами.

Форма для введення логіну та паролю була скопійована з офіційного сайту, або ж виглядала максимально схожою.

Другим фактором був “Зелений замочок”, до якого звикли користувачі і, що сигналізував, що сайт використовує шифроване з’єднання, та сертифікат не є само підписним, а був виданий офіційно. Приклад такого сайту наведений на Рисунку 2.

ISSN 2663 - 4023

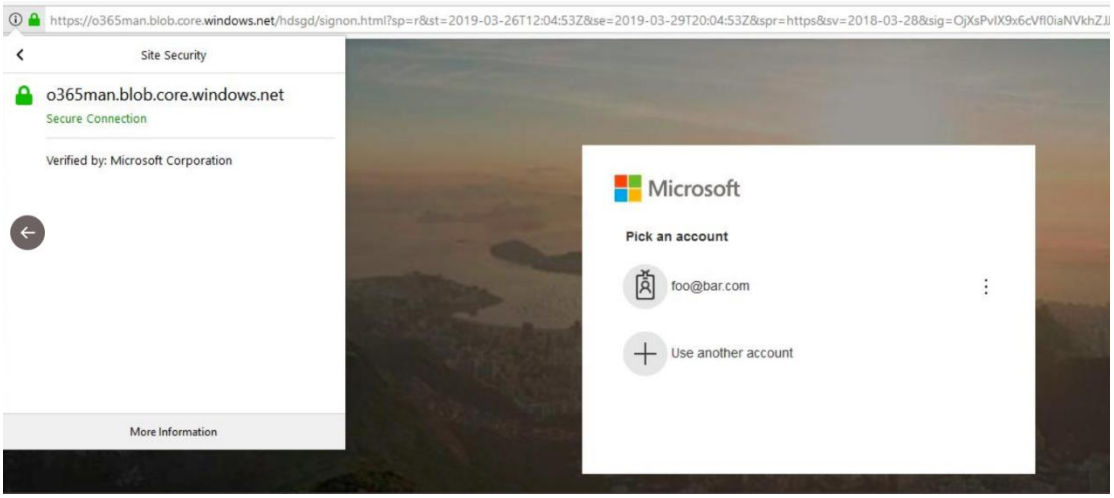

Рис.2 Фішинговий сайт на платформі Azure Blob

По-третє IP адреси, домени та SSL сертифікати дійсно належали компанії Microsoft, що значно вплинуло на рівень довірі користувачів до даного веб ресурсу. Приклад такого сертифікату зображений на Рисунку 3.

Така ж сама ситуація і з сервісами по наданню послуг зберігання і поширення файлів. Пошта не є єдиний способом передачі даних на сьогодні. Ось уже декілька років люди активно використовують хмарні сервіси як основне місце зберігання та поширення даних. Користувач з будь-якого куточка світу може без труднощів отримати доступ до цих технологій. Серед найбільш популярних сервісів можна назвати Google Drive, Microsoft OneDrive і Dropbox. Безумовно, ці великі компанії дбають про безпеку зберігання і передачі інформації яка зберігається на їхніх серверах. Цим і скористалися зловмисники, побудувавши свої фішингові кампанії на безкоштовних платформах. Маючи легітимний канал передачі даних та кінцевий сервер, їм вдалося обійти сучасні засоби захисту. Як і в попередній ситуації, основними чинниками для обману стали “чисті” IP адреси, зареєстровані доменні імена з сертифікатом, яким засвідчував їх валідність і приналежність тій чи іншій організації.

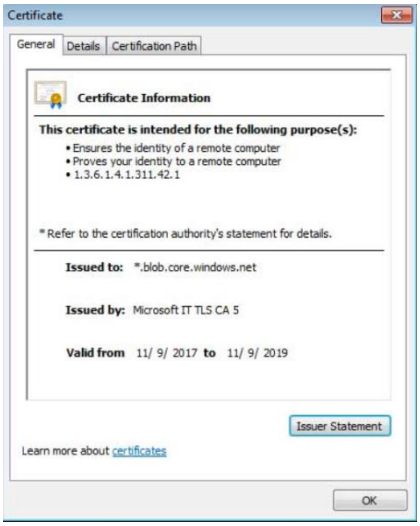

Рис.3 SSL сертифікат

В літку 2019 року, багато авторитетних сайтів новин [8] опублікували статті про використання Google Drive сервісу для поширення шкідливого документу. Користувачі отримували легітимний лист з легітимним посиланням від сервісу про те, що з ними був поширений документ. Перейшовши за посиланням відкривався онлайн документ у якому був певний контекст, метою якого було примусити жертв перейти за посиланням на шкідливий ресурс. Даний метод атаки дозволив обійти захист поштових серверів компанії Майкрософт, що призвело до компрометації кінцевих користувачів.

У статті [6] "Захист від фішинг-атаки: Таксономія методів, поточні проблеми та майбутні напрямки" на основі циклу життя фішингових листів та вебсатів класифіковано багато методів виявлення та захисту від фішингових листів і сайтів. Проаналізувавши атаки на основі хмарних сервісів, які відбулися з засобами захисту, можна пояснити, чому сучасні системи захисту не задетектували загрози.

1. Мережевий рівень захисту

Методи блокування DNS записів та IP адрес не стали ефективним, оскільки хмарних сервісів були легітимним і певна кількість компанії використовує їх у своїх бізнес потребах. Якщо ж впроваджувати такий контроль, то потрібно буди дуже уважним і зважати на всі можливі побічні ефекти.

2. Автентифікація листів відправника [11].

Для захисту від небажаної пошти, багато організацій використовують на поштових серверах фільтрацію листів на основі автентифікації. Ця технологія передбачає перевірку дійсної приналежності електронного листа відправному серверу. Цей метод захисту є досить ефективним проти атак підміни відправника [12]. У одній з згаданих атак, жертви отримували цілком легітимні листи-повідомлення від самих хмарних сервісів, які без сумнівів пройшли автентифікацію.

3. Перевірка посилань і вкладень.

Перевірка посилань і вкладень може здійснюватися на декількох етапам:

- Поштовий сервер/клієнт. До таких механізмів захисту можна віднести такі технології як Microsoft ATP Safe Links [13] Microsoft ATP Safe Attachments [14].
- Антивірусне програмне забезпечення, з модулями сканування пошти та web захисту.
- Перевірка браузерами. Прикладом є вбудовані функції Google Safe Browsing [15] та Safe Browsing [16] у браузерах Google Chrome та Mozilla Firefox. Ці механізми перевіряють сайти, які відкриває користувач на наявність їх в свої базах загроз.

В ідеальній ситуації, коли захист складається з трьох вище згаданих варіантів, ймовірність виявлення шкідливої активності значно зростає, оскільки будуть використані що найменше три джерела індикаторів компрометації трьох різних компаній. Методи перевірки посилань та вкладень не змогли захистили від фішингових атак з використанням хмарних технологій. Причиною слугувала висока довіра засобів захисту до доменів хмарних сервісів. Все ж таки посилання на фішингові ресурси потрапили в джерела індикаторів компрометації після того, як жертви цих атак сповістили відповідні компанії про шкідливі посилання. З цього можна зробити висновок, що завжди буде певний проміжок часу між початком атаки та її виявленням аналітиками безпеки.

Щоб зменшити ризики потенційного компрометування даних чи його наслідків, слід дотримуватися певних простих правил інформаційної безпеки:

1. Оскільки в основному фішингові атаки спрямовані на викрадення логіну та паролю користувача, потрібно використовувати двох факторну автентифікацію у всіх

системах де це передбачено, щоб при зловмисник не зміг отримати доступ до системи. До методів багатофакторної автентифікації відносять такі фактори:

- Те, що ми знаємо (Логін та пароль)
- Те, що ми маємо (Фізичний токен, аплікація на телефоні)
- Те, хто ми є (Біометричні дані)
- Те, що ми робимо (Графічний ключ)
- Те, де ми є (Фізична чи логічна локація)

Двох факторна автентифікація передбачає використання хоча б двох факторі. Використання одного фактора двічі не являє собою двох факторну автентифікацію. Прикладом може слугувати використання двох паролів для входу в систему.

2. Використання різних паролів для різних систем. Це правило доволі старе, проте ще досі актуальне. Проте воно допомагає зменшити ризик компрометація всіх сервісів через викрадення лише одного паролю.

3. Моніторинг новин та рекомендацій від відповідних служб та сервісів, щодо інформаційної безпеки. Для того, щоб вміти швидко реагувати на нові загрози, потрібно вчасно дізнаватися про них. Перегляд останніх новин та рекомендацій від експертів галузі або просте інформування, допоможе кінцевим користувачам краще підготуватися до можливих спроб нападу, тим самим підвищить безпеку організації чи держави.

4. Перегляд на періодичній основі журналу входу. Під час такого аналізу, можна виявити несанкціонованого доступу у систему через ваш профіль. Це буде сигналізувати про те, що вам потрібно звернутися до відповідних служб або ж самому прийняти відповідні заходи для запобіганню поширенню загрози.

5. Не довіряти на 100% сайтам з шифрованим зв'язком та сертифікатами. Правило, що усі web ресурси з протоколом HTTPS безпечні, уже не актуальне. За останні роки кількість сайтів, які використовують шифрований канал зв'язку, значно зросла. Тепер підписний сертифікат також можна отримати безкоштовно. До прикладу сервіс Letsencrypt надає таку послугу.

6. Потрібно завжди ставити під сумнів легітимність листів, які ви не очікували отримати. До прикладу, якщо вам прийшов лист від банку, клієнтом якого ви не є, з вимогою надати персональні данні, це уже може свідчити про фішингову атаку.

7. Перевірка функціоналу сайту. У більшості випадків фішинговий сайт є скопійованим і зловмисник не перевіряє або ж не витрачає часу на налагодження повного функціоналу сайту. Тому потрібно бути дуже обачним.

3. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Отже, хмарні сервіси почали активно використовувати для здійснення фішингових атак на користувачів інтернету, оскільки вони надали хорошу можливість зловмисникам замаскувати свої дії так, що сучасні системи захисту не завжди зможуть виявити їх. Також причиною використання хмарних сервісів є їх дешевизна та простота в експлуатації. Деякі сервіси є навіть безкоштовними, що знижує їх собівартість і тим самим підвищує прибуток. Такі атаки є досить актуальними і завдають певної шкоди. Тому потрібно дотримуватися основних правил інформаційної безпеки, щоб зменшити ризик бути скомпрометованим. Можна сподіватися, що б майбутньому дослідники та виробники захисного програмного забезпечення зможуть використати штучний

інтелект для покращення аналізу інтернет ресурсів та виявлення шкідливого змісту серед легітимного.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Oleksandr Milov, Alexander Voitko, Iryna Husarova, Oleg Domaskin, Yevheniia Ivanchenko, Ihor Ivanchenko, Olha Korol, Hryhorii Kots, Ivan Opirskyy, Oleksii Fraze-Frazenko. Development of methodology for modeling the interaction of antagonistic agents in cybersecurity systems, Eastern-european journal of enterprise technologies. Information and controlling system. – Vol 2, No 9(98), pp.56-66, (2019). DOI: https://doi.org/10.15587/1729-4061.2019.164730.

[2] Дудикевич В. Б. Забезпечення інформаційної безпеки держави: навчальний посібник / В. Б. Дудикевич, І. Р. Опірський, П. І. Гаранюк, В. С. Зачепило, А. І. Партика. – Львів: Видавництво Національного університету «Львівська політехніка», 2017. – 204 с. (IBSN 978-966-941-091-7).

[3] Info.phishlabs.com, 2019. [Електронний ресурс]. Available: https://info.phishlabs.com/hubfs/2019%20PTI%20Report/2019%20Phishing%20Trends%20and%20Intelligence%20Report.pdf.

[4] H. Journal, "65% of U.S. Organizations Experienced a Successful Phishing Attack in 2019", HIPAA Journal, 2019. [Електронний ресурс]. Available: https://www.hipaajournal.com/65-of-u-s-organizations-experienced-a-successful-phishing-attack-in-2019/.

[5] J. Singh, "Comprehensive Solution to Mitigate the Cyber-attacks in Cloud Computing", International Journal of Cyber-Security and Digital Forensics, vol. 3, no. 2, pp. 84-92, 2014. Available: 10.17781/p001294.

[6] B. Gupta, N. Arachchilage and K. Psannis, "Defending against phishing attacks: taxonomy of methods, current issues and future directions", Telecommunication Systems, vol. 67, no. 2, pp. 247-267, 2017. Available: 10.1007/s11235-017-0334-z.

[7] "Software as a service", En.wikipedia.org. [Електронний ресурс]. Available: https://en.wikipedia.org/wiki/Software_as_a_service.

[8] "About Blob (object) storage - Azure Storage", Docs.microsoft.com. [Електронний ресурс]. Available: https://docs.microsoft.com/uk-ua/azure/storage/blobs/storage-blobs-overview.

[9] "Static website hosting in Azure Storage", Docs.microsoft.com. [Електронний ресурс]. Available: https://docs.microsoft.com/uk-ua/azure/storage/blobs/storage-blob-static-website.

[10] S. Gatlan, "Phishing Campaign Uses Google Drive to Bypass Email Gateways", BleepingComputer, 2019. [Електронний ресурс]. Available: https://www.bleepingcomputer.com/news/security/phishing-campaign-uses-google-drive-to-bypass-email-gateways/.

[11] "Email authentication", En.wikipedia.org. [Електронний ресурс]. Available: https://en.wikipedia.org/wiki/Email_authentication.

[12] "Email spoofing", En.wikipedia.org. [Електронний ресурс]. Available: https://en.wikipedia.org/wiki/Email_spoofing.

[13] "How Office 365 ATP Safe Links works - Office 365", Docs.microsoft.com. [Електронний ресурс]. Available: https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/how-atp-safe-links-works?view=o365-worldwide.

[14] "How Office 365 ATP Safe Attachments works - Office 365", Docs.microsoft.com. [Електронний ресурс]. Available: https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/how-atp-safe-attachments-works?view=o365-worldwide.

[15] "Google Safe Browsing", Safebrowsing.google.com. [Електронний ресурс]. Available: https://safebrowsing.google.com/.

[16] "Security/Safe Browsing - MozillaWiki", Wiki.mozilla.org. [Електронний ресурс]. Available: https://wiki.mozilla.org/Security/Safe_Browsing.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (9), 2020
ISSN 2663 - 4023

Ivan R. Opirskyy
Doctor of Science, Professor, Department of Information Security
National University "Lviv Polytechnic", Lviv, Ukraine
ORCID: 0000-0002-8461-8996
ivan.r.opirskyi@lpnu.ua

Andrii S. Vynar
Student
National University "Lviv Polytechnic", Lviv, Ukraine
ORCID:0000-0003-2044-7590
andrii.vynar.om@gmail.com

ANALYSIS OF THE USE OF CLOUD SERVICES FOR FISHING ATTACKS

Abstract. Phishing, as a type of information attack, has been used by intruders for selfish purposes for quite some time. They are very popular in the criminal world because it is much easier for a person to make certain profitable actions than a program. With the advent of new technologies, this type of attack has gradually adapted to the new conditions of engagement with its victim. Cloud services have become a great modern and widespread tool for phishing campaigns. The use of such services has given to malicious actors a number of significant advantages over the use of their own computing resources. The relative cheapness and ease of exploitation of these technologies has played an important role. The problem of information security with using cloud technologies is that this type of attack is difficult to detect, even more to prevent, without significantly affecting the comfort of using end users of information systems. The article analyzes the relevance of this type of attacks based on real data. We considered the algorithm of their work during a life cycle and analyzes the use of the basic available security methods of protection, their feasibility and problems of use. The analysis showed that not all modern security methods are capable of detecting and preventing phishing attacks, which use public cloud services. Even a combination of several or all methods cannot guarantee high protection for users against phishing threats. In the article were mentioned some examples of phishing campaigns that took place during 2019 and used such popular public cloud services as Azure Blob storage created by Microsoft and Google Drive developed by Google. A basic list of tips was also provided that would increase the level of security for internet users in order to reduce the risk of potential data compromise or its consequences.

Keywords: social engineering; phishing; cloud services; cloud computing.

REFERENCES

[1] Oleksandr Milov, Alexander Voitko, Iryna Husarova, Oleg Domaskin, Yevheniia Ivanchenko, Ihor Ivanchenko, Olha Korol, Hryhorii Kots, Ivan Opirskyy, Oleksii Fraze-Frazenko. Development of methodology for modeling the interaction of antagonistic agents in cybersecurity systems, Eastern-european journal of enterprise technologies. Information and controlling system. – Vol 2, No 9(98), pp.56-66, (2019). DOI: https://doi.org/10.15587/1729-4061.2019.164730.

[2] Dudykevych V.B. Provision of information security of the state: a textbook / V.B. Dudykevych, I.R. Opirskyy, P.I. Garanyuk, V.S. Zachepilo, A.I. Partyka. - Lviv: Publisher of Lviv Polytechnic National University, 2017. - 204 p. (IBSN 978-966-941-091-7).

[3] Info.phishlabs.com, 2019. [Online]. Available: https://info.phishlabs.com/hubfs/2019%20PTI%20Report/2019%20Phishing%20Trends%20and%20Intelligence%20Report.pdf.

[4] H. Journal, "65% of U.S. Organizations Experienced a Successful Phishing Attack in 2019", HIPAA Journal, 2019. [Online]. Available: https://www.hipaajournal.com/65-of-u-s-organizations-experienced-a-successful-phishing-attack-in-2019/.

[5] J. Singh, "Comprehensive Solution to Mitigate the Cyber-attacks in Cloud Computing", International Journal of Cyber-Security and Digital Forensics, vol. 3, no. 2, pp. 84-92, 2014. Available: 10.17781/p001294.
[6] B. Gupta, N. Arachchilage and K. Psannis, "Defending against phishing attacks: taxonomy of methods, current issues and future directions", Telecommunication Systems, vol. 67, no. 2, pp. 247-267, 2017. Available: 10.1007/s11235-017-0334-z.
[7] "Software as a service", En.wikipedia.org. [Online]. Available: https://en.wikipedia.org/wiki/Software_as_a_service.
[8] "About Blob (object) storage - Azure Storage", Docs.microsoft.com. [Online]. Available: https://docs.microsoft.com/uk-ua/azure/storage/blobs/storage-blobs-overview.
[9] "Static website hosting in Azure Storage", Docs.microsoft.com. [Online]. Available: https://docs.microsoft.com/uk-ua/azure/storage/blobs/storage-blob-static-website.
[10] S. Gatlan, "Phishing Campaign Uses Google Drive to Bypass Email Gateways", BleepingComputer, 2019. [Online]. Available: https://www.bleepingcomputer.com/news/security/phishing-campaign-uses-google-drive-to-bypass-email-gateways/.
[11] "Email authentication", En.wikipedia.org. [Online]. Available: https://en.wikipedia.org/wiki/Email_authentication.
[12] "Email spoofing", En.wikipedia.org. [Online]. Available: https://en.wikipedia.org/wiki/Email_spoofing.
[13] "How Office 365 ATP Safe Links works - Office 365", Docs.microsoft.com. [Online]. Available: https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/how-atp-safe-links-works?view=o365-worldwide.
[14] "How Office 365 ATP Safe Attachments works - Office 365", Docs.microsoft.com. [Online]. Available: https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/how-atp-safe-attachments-works?view=o365-worldwide.
[15] "Google Safe Browsing", Safebrowsing.google.com. [Online]. Available: https://safebrowsing.google.com/.
[16] "Security/Safe Browsing - MozillaWiki", Wiki.mozilla.org. [Online]. Available: https://wiki.mozilla.org/Security/Safe_Browsing.