COLLECTION OF SCIENTIFIC PAPERS
SCIENTIA

20 JANUARY, 2023

AMSTERDAM, THE NETHERLANDS

ADVANCED DISCOVERIES OF MODERN SCIENCE: EXPERIENCE, APPROACHES AND INNOVATIONS

III INTERNATIONAL SCIENTIFIC AND THEORETICAL CONFERENCE

EUROPEAN SCIENTIFIC PLATFORM

DOI 10.36074/scientia-20.01.2023 ISBN 979-8-88862-114-1

UDC 001(08)
A 20

https://doi.org/10.36074/scientia-20.01.2023

Chairman of the Organizing Committee: Holdenblat M.

Responsible for the layout: Bilous T.
Responsible designer: Bondarenko I.

A 20 Advanced discoveries of modern science: experience, approaches and innovations: collection of scientific papers «SCIENTIA» with Proceedings of the III International Scientific and Theoretical Conference, January 20, 2023. Amsterdam, The Netherlands: European Scientific Platform.

ISBN 979-8-88862-114-1
DOI 10.36074/scientia-20.01.2023

Papers of participants of the III International Multidisciplinary Scientific and Theoretical Conference «Advanced discoveries of modern science: experience, approaches and innovations», held on January 20, 2023 in Amsterdam are presented in the collection of scientific papers.

The conference is included in the Academic Research Index ReserchBib International catalog of scientific conferences and registered for holding on the territory of Ukraine in UKRISTEI (Certificate № 02 dated January 9th, 2023).

UDC 001 (08)

ISBN 979-8-88862-114-1

SECTION 10.
CHEMISTRY, CHEMICAL ENGINEERING AND BIOENGINEERING

SULTONES – PERSPECTIVE SUBSTANCES IN ORGANIC SYNTHESIS
Poliudov A., Dobrydnev A.V. 106

THE USE OF COAL MINING UNBURNED ROCKS IN THE CONSTRUCTION INDUSTRY
Khobotova E.B., Datsenko V.V. 108

SECTION 11.
FOOD PRODUCTION AND TECHNOLOGY

НОВІТНІ ТЕХНОЛОГІЇ ХЛІБОБУЛОЧНИХ ВИРОБІВ ПІДВИЩЕННОЇ ХАРЧОВОЇ ЦІННОСТІ
Данилюк І.П., Струтинська Л.Т. 113

SECTION 12.
ECOLOGY AND ENVIRONMENTAL PROTECTION TECHNOLOGIES

ВПЛИВ ТЕХНОЛОГІЙ СПОРУДЖЕННЯ БУДІВЕЛЬ ТА СІТІ-ФЕРМЕРСТВА НА СТАЛИЙ РОЗВИТОК ТЕРИТОРІАЛЬНИХ ГРОМАД
Артьомов Р.М., Бондаренко А.О. 118

SECTION 13.
SYSTEM ANALYSIS, MODELING AND OPTIMIZATION

TRANSFORMATION OF GRAPHS WHEN CALCULATING CHARACTERISTICS IN PERT NETWORKS
Markova A., Turchyna V. 122

SECTION 14.
INFORMATION TECHNOLOGIES AND SYSTEMS

АНАЛІЗ ОСНОВНИХ ПРИЙОМІВ ФІШИНГУ, ЩО ВИКОРИСТОВУВАЛИ КІБЕРЗЛОЧИНЦІ У 2022 РОЦІ
Демидов З.Г., Грінченко Є.М. 124

АСИСТЕНТ ВОДІЯ НА ОСНОВІ ЗГОРТКОВИХ НЕЙРОННИХ МЕРЕЖ
Левкович Р.Ю., Колос Н.М. 129

ВНЕСОК ХАРКІВСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ РАДІОЕЛЕКТРОНІКИ У ДОСЯГНЕННЯ ЦІЛІ СТАЛОГО РОЗВИТКУ 3 - «МІЦНЕ ЗДОРОВ'Я І БЛАГОПОЛУЧЧЯ»
Бєлянінова Г.Г. 132

SECTION 14.
INFORMATION TECHNOLOGIES AND SYSTEMS

Демидов Захар Георгійович
старший науковий співробітник науково-дослідної лабораторії
з проблем інформаційних технологій та протидії злочинності у кіберпросторі
Харківський національний університет внутрішніх справ, Україна

Грінченко Євген Миколайович
канд. техн. наук, доцент, провідний науковий співробітник науково-дослідної лабораторії
з проблем інформаційних технологій та протидії злочинності у кіберпросторі
Харківський національний університет внутрішніх справ, Україна

АНАЛІЗ ОСНОВНИХ ПРИЙОМІВ ФІШИНГУ, ЩО ВИКОРИСТОВУВАЛИ КІБЕРЗЛОЧИНЦІ У 2022 РОЦІ

Існує два основних види онлайн-шахрайства, націленого на крадіжку даних та грошей користувачів – фішинг та скам. Фішинг [1] — це насамперед прийоми зловмисників, націлені на те, щоб жертва видала конфіденційну інформацію, як-от облікові дані або дані банківської картки.

Термін «фішинг» вперше використали в 1996 році, коли кіберзлочинці атакували користувачів найбільшого на той момент інтернет-провайдера America Online (AOL). Шахраї відправляли повідомлення від імені співробітників компанії AOL і вимагали користувачів підтвердити свої облікові записи або повідомити платіжні реквізити. Цей спосіб виуджування особистих даних існує досі і, на жаль, дає результати.

Згодом онлайн-шахрайство ставало все більш витонченим і переконливим. Кіберзлочинці навчилися вдало імітувати офіційні сайти брендів, роблячи їх практично невідмінними від оригіналу, і знаходити нові хитрощі для своїх жертв. З'явилися послуги зі створення шахрайського контенту, фішинг почали використовувати «по-великому», спрямовуючи свої атаки не лише на особисті фінанси та дані звичайних користувачів, а й на політичних діячів та великий бізнес.

Мета фішингу — облікові дані в абсолютно будь-якому інтернет-сервісі: банку, соціальній мережі, державному порталі, онлайн-магазині, поштовому сервісі, службі доставки тощо. Проте найчастіше під загрозу потрапляють користувачі найвідоміших брендів, тому що їм довіряє і користується їх послугами більше людей, відповідно вище та ймовірність успішної атаки.

Щоб вивудити потрібну їм інформацію, зловмисники змушують жертву повірити, що вона вводить дані на офіційному сайті компанії або сервісу, користувачем якого вона є, або повідомляє їх співробітникам компанії. Найчастіше підроблені сайти зовні нічим не відрізняються від оригіналу, і навіть просунутому користувачеві складно помітити каверзу. Фішери вміло копіюють верстку та дизайн офіційних сайтів, додають на свої сторінки додаткові деталі, наприклад чат підтримки (зазвичай, щоправда, непрацюючий), щоб вони викликали більше довіри, і навіть підтягують реальні сайти сервісів як тло.

Останнім часом поряд з онлайн-фішинг активно розвивається вішінг - телефонний фішинг. Шахраї або самі дзвонять жертві, або різними хитрощами змушують її зателефонувати їм і вже по телефону виманюють персональні дані і гроші.

Також актуальним є цільовий фішинг, або спірфішинг (spear phishing), який націлений на певну людину або організацію. Цільові фішингові листи та сторінки більш персоналізовані, ніж масові розсилки, тому їх дуже складно відрізнити від легітимних.

Більшість фішингових починається з розсилки електронних листів із посиланнями на шахрайські сайти, проте на сьогоднішній день можна говорити про зростання популярності альтернативних векторів атаки. Існує безліч різних сервісів для спілкування та обміну інформацією, які зловмисники також використовують для розповсюдження фішингових посилань.

Один із важливих векторів поширення загроз типу фішингу - це месенджери, такі як WhatsApp, Viber та Telegram.

У WhatsApp та Viber повідомлення шахрайського характеру може прийти як від самих кіберзлочинців, так і людей зі списку контактів жертви. Зловмисники розсилають повідомлення від імені відомих брендів чи офіційних органів, проте не гидують залучати і користувачів до поширення шахрайства. Зокрема, для отримання обіцяного у повідомленні подарунка вони нерідко вимагають надіслати його всім чи деяким своїм знайомим.

У Telegram останнім часом з'явилося безліч каналів, що обіцяють розіграші призів чи збагачення за рахунок інвестицій у криптовалюту. У чатах популярних Telegram-каналів теж нерідко можна натрапити на шахраїв, які під виглядом звичайних користувачів публікують «вигідні пропозиції», наприклад, обіцяють допомогти заробити, ботів. Щоб дізнатися про секрет легких грошей, користувачеві пропонують написати повідомлення шахраям або перейти в їхній канал.

Коментарі, що пропонують легкий прибуток, можна зустріти і в соціальних мережах, наприклад під фотографіями в популярних облікових записах, де ймовірність того, що повідомлення прочитають, вище, ніж на сторінці з невеликою кількістю передплатників. Зловмисники пропонують перейти за посиланням у шапці профілю, написати їм особисте повідомлення або вступити до секретного групового чату. У листуванні їм також дадуть посилання на сайт. Крім цього, в соцмережах кіберзлочинці можуть самі писати користувачам особисті повідомлення, проводити промокампанії своїх пропозицій та створювати фейкові акаунти, що обіцяють роздачу цінних подарунків, ігрових монет та подарункових карток. Останні розкручуються за допомогою реклами, хештегів або масових позначок користувачів у постах, коментарях чи на фото.

Маркетплейси виступають у ролі посередника між користувачем і продавцем і певною мірою забезпечують безпеку угоди обох сторін. Проте їхньою функціональністю теж зловживають шахраї. Наприклад, на маркетплейсах досить поширена схема, коли продавець з тієї чи іншої причини не хоче спілкуватися на майданчику і намагається перевести листування до сторонніх месенджерів. Там він може надіслати користувачеві шкідливе посилання без побоювання натрапити на вбудований захист маркетплейсу.

Крім цього, на маркетплейсах шахраї часто коментують відгуки інших користувачів на товари, запевняючи потенційних покупців, що той чи інший товар можна набагато дешевше купити на іншому ресурсі, та прикріплюючи посилання на свій сайт.

Для реалізації своїх атак зловмисники застосовують безліч технічних і психологічних хитрощів, що дозволяють привернути до себе якомога більше користувачів і при цьому звести ризик виявлення до мінімуму.

Нижче наведено основні прийоми, які зустрічалися у фішингу у 2022 році.

Часто шахраї для того, щоб збільшити рівень довіри жертви до підробленого ресурсу, намагаються зробити його максимально схожим на оригінальний. Цей прийом називається спуфінгом [2]. У контексті підробки веб-сайтів можна говорити про два основні види спуфінгу:

- доменний спуфінг - підробка доменного імені сайту;
- контентний спуфінг – імітація зовнішнього вигляду легального сайту.

Нерідко в атаках використовується і те, й інше.

Доменний спуфінг передбачає реєстрацію домену, схожого на домен організації, що цікавить зловмисників. Фішери обирають такі домени, щоб жертва нічого не помітила та не вважала сайт підозрілим. Доменний спуфінг можна поділити на три види.

- Тайпсквоттінг (typosquatting) — використання імені оригінального домену з друкарськими помилками, такими як пропущені літери, зайві символи, заміна одного або двох символів або їх перестановка.

- Комбосквотинг (combosquatting) — використання в імені домену назви бренду, на чиїх користувачів націлена атака, у поєднанні з додатковими словами, часто пов'язаними з авторизацією або безпекою в мережі. Наприклад, це можуть бути такі слова, як login, secure, account, verify тощо.

- Омографи IDN (Internationalized Domain NameHomograph) – написання імен підроблених сайтів з використанням символів з таблиці UTF, які дуже схожі на латиницю. Наприклад, найбільш часто використовують кириличні літери а, с, е, о, р, х, у, які виглядають ідентично латинським a, c, e, o, p, x, y.

Контентний спуфінг використовується для фальшування зовнішнього вигляду легального сайту. Тут можна назвати такі методи.

- Legal IFrame Background – за допомогою iFrame на шахрайський ресурс підвантажується легальний сайт, поверх якого додається фішингова форма.

Іноді шахраям простіше зламати чужі сайти для розміщення шкідливого контенту, ніж створювати власні з нуля. Такі фішингові сторінки існують недовго, оскільки власники ресурсів швидко виявляють і видаляють шахрайський контент, а також регулярно прикривають лазівки та усувають уразливості у своїй інфраструктурі. З іншого боку, якщо зловмисники зламають занедбаний сайт, фішингові сторінки, розміщені на ньому, можуть довго прожити. Фішери можуть використовувати зламані сайти кількома способами.

- Використання iFrame (IFrame Injection) — вставка форми авторизації або іншої частини фішингової сторінки через iFrame [3]. У той час як у методі Legal IFrame Background шахраї використовують iFrame з легальним сайтом, як фон для фішингової форми, в даному випадку легітимною є URL-адреса сторінки, а через iFrame підвантажується фішингова форма, тлом якої служить найчастіше саморобний контент з використанням символіки бренду.

- Злом піддиректорії (Subfolder Hijacking) — частковий злам сайту та отримання доступу до його піддиректорій для розміщення на них шахрайського контенту. У такій атаці шахраї можуть використовувати вже існуючі директорії на легітимному сайті, так і створювати нові. Підміна сайту (Site Swapping) - повна заміна легального сайту на шахрайський. Оригінальний контент при цьому найчастіше видаляється.

Деякі інтернет-шахраї не обтяжують себе створенням або зламуванням сайтів, а застосовують для своїх цілей функції довірених у користувачів сервісів. Так, велика кількість атак відбувається з використанням форм для проведення опитувань та збору даних (Google Forms, MS Forms, HubSpot Form Builder, Typeform, Zoho Forms тощо).

Наприклад, під виглядом техпідтримки популярного криптогаманця виманюють у користувачів через Google-форму їх ідентифікаційні дані, такі як адреса електронної пошти та секретну фразу.

Легітимні сервіси з часом почали попереджати користувачів про те, що передавати паролі через їх форми — небезпечно, а також впровадили автоматичний захист, наприклад, блокування форм, що містять певні ключові слова, такі як «пароль» або password. І все ж завдяки можливості масово створювати фішингові анкети зловмисники продовжують використовувати цей метод. Для обходу вбудованого захисту вони часто застосовують спуфінг тексту – замінюють частину символів у ключових словах візуально схожими, наприклад, пишуть pa$$w0rd замість password, роблячи такі слова нерозпізнаними для автоматичних систем.

Крім форм, зловмисники активно використовують хмарні документи. Зокрема, вони можуть надсилати листи з посиланням на документ у легітимному сервісі, де міститься вже фішингове посилання.

Шахраї можуть використовувати різні способи захисту від виявлення. Серед них є досить ефективні, проте вони зустрічаються не так часто, тому що вимагають від шахраїв глибших технічних знань, ніж ті, які мають багато з них.

Один із методів захисту від виявлення - це обфускація [4], тобто спотворення вихідного коду шахрайської сторінки, який невидимий для користувача, щоб утруднити виявлення атаки автоматичними засобами. Ще один спосіб захистити шахрайський сайт від виявлення - використовувати прийоми, що приховують контент сторінки автоматичного аналізу. Перелічимо деякі з них.

- Використання зображень. Якщо замість тексту на сторінці будуть розміщені зображення з текстом, контентні движки побачити і проаналізувати текст не зможуть, а користувачі - прочитають.

- Повідомлення у браузері. Посилання на шахрайські ресурси можуть поширюватися у браузерних повідомленнях. На відміну від листів та відкритих веб-сторінок, браузерні повідомлення обробляються в кілька етапів, і далеко не всі антифішингові движки їх аналізують. Відповідно, у такий спосіб зловмисники можуть обійти як мінімум частину детектуючих технологій.

- Вспливаючі вікна. Шахрайський контент відкривається у спливаючому вікні сайту. Вспливаючі вікна завантажуються пізніше, ніж основне вікно сайту, тому їх теж бачать не всі антифішингові технології. Крім того, вікна, що спливають, дають зловмисникам додаткові інструменти для копіювання зовнішнього вигляду легітимного сайту. Зокрема, зловмисники можуть використовувати метод «браузер у браузері» (Browser-in-the-Browser), коли спливаюче вікно імітує вікно браузера з адресним рядком, в якому вказана URL-адреса легітимного сайту.

Крім контенту, шахраї намагаються приховати від технологій виявлення та URL-адреси шкідливих сайтів. Для цього вони можуть використати таке.

- Створені URL-адреси — посилання формуються випадковим чином за допомогою хешів. Кожна жертва отримує унікальне посилання, що ускладнює блокування шкідливого сайту.

- Сервіси коротких посилань — зловмисники можуть маскувати адреси шкідливих ресурсів за допомогою легітимних сервісів для скорочення URL, таких як bit.ly.

Хитрощі кіберзлочинців часто націлені не на вразливість систем інформаційної безпеки, а на людину. Шахраї оперують знанням людської психології, щоб обдурити своїх жертв. Вони можуть використовувати як технічні, так і чисто психологічні прийоми.

- Підроблена CAPTCHA — зловмисники імітують на шахрайському ресурсі технологію CAPTCHA, щоб переконати жертву вчинити їхню дію.

- User-Related Dynamic Content — контент сторінки змінюється залежно від даних користувача, наприклад, його поштової адреси: для домену з пошти підвантажуються картинки та вставляються на сторінку фішинга.

- Залякування та погрози — зловмисники загрожують жертві, щоб змусити її втратити самовладання і здійснити дії, що їх цікавлять. Наприклад, вони можуть загрожувати переслідуванням за законом і вимагати «сплатити штраф», щоб жертву дали спокій. Також зловмисники можуть загрожувати блокуванням облікового запису, щоб змусити жертву перейти за фішинговим посиланням.

- Терміновість. Зловмисники залишають одержувачу обмежену кількість часу на те, щоб якось відреагувати на їхнє повідомлення. Це має змусити жертву діяти поспішно та необдумано.

- Тиск на жаль. Зловмисники намагаються викликати у жертви співчуття та, як наслідок, готовність віддати гроші.

- Обіцянка вигоди. Шахраї залучаю жертву неймовірно вигідними пропозиціями, від яких важко відмовитись.

Більшість користувачів зараз тією чи іншою мірою обізнані про актуальні веб-загрози. Багато хто або сам стикався з шахрайством в інтернеті, або дізнався про нього з новин або інших джерел, тому зловмисникам стає все важче викликати довіру у своїх жертв і в хід йдуть нові витончені прийоми та хитрощі. Замість зроблених «на коліні» фішингових сайтів все частіше зустрічаються якісні підробки, такі як імітація вікна браузера з адресою легітимного сайту у вікні, або фішингові сторінки з легітимним сайтом на фоні, завантаженому через iFrame. Також ми спостерігаємо у фішингу елементи цільових атак, такі як завантаження контенту, пов'язаного з поштовим доменом жертви, або використання даних великих витоків для налагодження з нею контакту.

Водночас зростає кількість випадків вишингу, адже телефоном на людину легше натиснути, не залишаючи часу на роздуми. При цьому зловмисники використовують інші доступні канали зв'язку: електронну пошту, популярні месенджери, соцмережі і маркетплейси.

Для реалізації атак застосовується безліч методів, таких як спуфінг, соціальна інженерія, злом сайтів, приховування коду та контенту. При цьому методи уникнення виявлення також ускладнюються та розвиваються. Зловмисники все частіше використовують одноразові згенеровані посилання з хешами, щоб їх не заблокували технології детектування веб-загроз.

Варто зазначити, що як привід для тієї чи іншої шкідливої кампанії шахраї використовували та використовують найактуальніші теми. Якщо десь відбувається великий захід, виникає проблема, яка торкається великої кількості людей, набирає популярності конкретний сервіс чи технологія, то велика ймовірність, що зловмисники спробують використати це у своїх цілях. Тому варто завжди бути пильними в мережі, особливо коли мова заходить про гроші: як би не хотілося вірити в удачу, що звалилася з неба, якщо щось звучить занадто добре, щоб бути правдою, швидше за все, це обман.

Список використаних джерел:

1. Фішинг https://uk.wikipedia.org/wiki/%D0%A4%D1%96%D1%88%D0%B8%D0%BD%D0%B3
2. Що таке спуфінг і як запобігти атаці? ПОРАДИ https://cybercalm.org/novyny/shho-take-spufing-i-yak-zapobigty-atatsi-porady/
3. HTML iframe: приклад та особливості застосування https://presa.com.ua/aktualne/html-iframe-priklad-ta-osoblivosti-zastosuvannya.html
4. ОБФУСКАЦІЯ І ДЕОБФУСКАЦІЯ ПРОГРАМ https://stud.com.ua/128267/informatika/obfuskatsiya_deobfuskatsiya_program