WORLD DEVELOPMENT OF SCIENCE AND TECHNOLOGY

Abstracts of XLV International Scientific and Practical Conference
Canada, Ottawa

16 – 17, January 2023

Canada, Ottawa
16 – 17, January 2023

UDC 001.1
BBK 29

The 45th International scientific and practical conference "World Development of Science and Technology" (16 – 17 January, 2023) Pegas Publishing, Canada, Ottawa. 2023. 128 p.

ISBN 978-1-74174-612-9

The recommended citation for this publication is:
Petrov P. Learning Styles and Strategies // World Development of Science and Technology. Abstracts of the 45th International scientific and practical conference. Pegas Publishing, Canada. 2023. Pp. 39-43. URL: http://el-conf.com.ua/

Science editor:
Solodka N.V.
Ph.D. in Economics, Associate Professor
Reviewers:
Monique Carnaghan
Associate Professor in Economics in the Department of Economics, University of Lethbridge, Canada
Ostin Koonin
Professor of Information, Operations & Management Sciences, NYU Stern

Collection of scientific articles published is the scientific and practical publication, which contains scientific articles of students, graduate students, Candidates and Doctors of Sciences, research workers and practitioners from Europe, Ukraine, Russia and from neighbouring coutries and beyond. The articles contain the study, reflecting the processes and changes in the structure of modern science. The collection of scientific articles is for students, postgraduate students, doctoral candidates, teachers, researchers, practitioners and people interested in the trends of modern science development.

e-mail: el-conf@ukr.net
homepage: *http://el-conf.com.ua*

CONTENT

№2074–IX. URL: https://zakon.rada.gov.ua/go/2074-20 (дата звернення: 15.04.2022).

5. Проект №7150 Закону Про внесення змін до Податкового кодексу України щодо оподаткування операцій з віртуальними активами від 13.03.2022. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/39211 (дата звернення: 15.04.2022).2022.

6. FATF. Отчет ФАТФ. Виртуальные валюты. Ключевые определения и потенциальные риски в сфере ПОД/ФТ. (Франция. Париж, 2014). Франция. Париж : FATF, 2014. URL: https://eurasian-group.org/files/FATF_docs/Virtualnye_valyuty_FATF_2014.pdf (дата звернення: 12.04.2022).2014.

УДК 004.49 Інформаційні технології

ОСНОВНІ ПРИЙОМИ, ЯКІ ВИКОРИСТОВУВАЛИ СКАМЕРИ У 2022 РОЦІ, ТА ЇХ АНАЛІЗ

Демидов З.Г., Хлестков О.В.
старший науковий співробітник
науково-дослідної лабораторії
з проблем інформаційних технологій
та протидії злочинності у кіберпросторі
Харківського національного
університету внутрішніх справ
м. Харків, Україна

Існує два основних види онлайн-шахрайства, націленого на крадіжку даних та грошей користувачів – фішинг та скам. Скам [1] — це шахрайство, за якого користувача за допомогою соціальної інженерії переконують самостійно перерахувати зловмисникам гроші. Він з'явився приблизно у 90-ті, коли банки почали активно впроваджувати системи інтернет-банкінгу, шахраї надсилали користувачам SMS нібито від родичів із проханням терміново переказати гроші за вказаними у повідомленні реквізитами.

На початку 2000-х у скамі стала популярною тема благодійності: наприклад, після масштабного землетрусу в Індійському

океані у 2004 році користувачі почали отримувати листи від підроблених благодійних організацій із проханням пожертвувати гроші постраждалим. У той же час фішери переключилися на платіжні системи та інтернет-банки. Оскільки аккаунти були захищені лише паролем, зловмисникам було достатньо вивудити його, щоб отримати доступ до чужих грошей. Для цього злочинці надсилали електронні листи від імені PayPal та інших компаній, де просили користувачів перейти на підроблений сайт із логотипом сервісу та ввести свої облікові дані. Щоб сайти виглядали правдоподібно, зловмисники реєстрували безліч доменів, дуже схожих на оригінальний, із різницею у дві-три літери. Неуважний користувач міг прийняти такий сайт за ресурс банку або платіжної системи. Також найчастіше шахраї використовували особисту інформацію із соціальних мереж жертв, щоб зробити свої атаки більш таргетованими, а отже, успішнішими.

Якщо фішинг націлений навіть на бізнес, то скам в більшості випадків становить загрозу для звичайних користувачів інтернету. Найчастіше в скам-схемах жертві обіцяють багато грошей, цінний приз або щось безкоштовне або з величезною знижкою. Основна мета шахраїв у цьому випадку — збагачення, однак вони можуть збирати й персональні дані жертви, які згодом можуть продати чи використати в інших схемах.

Наприклад, зловмисники стверджують, що жертва виграла смартфон і просять її сплатити невелику комісію за відправку призу, а також вказати адресу електронної пошти, дату народження, стать, номер телефону та домашню адресу.

У більшості випадків шахраї намагаються переконати жертву в тому, що вони справді збираються надіслати їй приз, і при цьому самі дані не зберігають. Однак деякі скам-сайти можуть «запам'ятовувати» всю введену на них інформацію. Це робиться для того, щоб у майбутньому, наприклад, надсилати шкідливі листи від імені жертви, використовуючи її ім'я та електронну адресу.

Окрім обіцянок легкого заробітку та виграшу цінних призів, скамери активно заманюють користувачів на неіснуючі сайти знайомств. Наприклад, надсилають запрошення поспілкуватися з

посиланням на шахрайський ресурс та прикладають до нього привабливі фотографії. Потрапивши на підроблений сайт, користувач бачить, що саме цього дня він може отримати преміум-доступ до платформи для онлайн-знайомств практично задарма. Потрібно лише оформити передплату і заплатити невеликий внесок.

Існують і інші способи залучення жертв на скам-сайти: «продаж» затребуваних або навіть дефіцитних товарів, поїздки з попутниками і т.п. Загалом, якщо щось популярне у користувачів, шахраї можуть використовувати це як приманку.

Більшість скам-атак 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 посилань.

Один із важливих векторів поширення загроз типу скама – 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 скам-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 скам-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 скамі 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. Скамери 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 підробна форма.

Іноді шахраям простіше зламати чужі сайти для розміщення шкідливого контенту, ніж створювати власні з нуля. Такі сторінки існують недовго, оскільки власники ресурсів швидко виявляють і видаляють шахрайський контент, а також регулярно прикривають лазівки та усувають уразливості у своїй інфраструктурі. Скамери можуть використовувати зламані сайти кількома способами.

• Використання iFrame (IFrame Injection) [3] — вставка форми

авторизації або іншої частини сторінки через iFrame. У той час як у методі Legal IFrame Background шахраї використовують iFrame з легальним сайтом як фон для підробної 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, шахраї 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 підробні 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.

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. Спливають 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.

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» скам-сайтів все частіше зустрічаються якісні підробки, такі як імітація вікна браузера з адресою легітимного сайту у вікні, або підроблені сторінки з легітимним сайтом на фоні, завантаженому через iFrame. Також спостерігається у скамі елементи цільових атак, такі як завантаження контенту, пов'язаного з поштовим доменом жертви, або використання даних великих витоків для налагодження з нею контакту.

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. Так, під час пандемії коронавірусу виникали масові скам-кампанії з «виплати матеріальної допомоги», а зі зростанням цін на криптовалюти минулого року з'явилося багато шахрайських схем, пов'язаних із криптовалютою. 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.

Література:

1. Що таке скам? https://itechua.com/other/185186
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

---

УДК 358:343.37 Економічні науки

ЗМІСТ ПОНЯТТЯ “ЕКОНОМІЧНА ЗЛОЧИННІСТЬ”: ОГЛЯД НАУКОВОЇ ЛІТЕРАТУРИ

Дикий А.П., Барановська Т.В.,
докторант кафедри національної безпеки,
публічного управління та адміністрування,
кандидат економічних наук, доцент
Державний університет
“Житомирська політехніка”
м. Житомир, Україна

Анотація: *Економічна злочинність має безумовний вплив на систему економічної безпеки держави, адже є деструктивним фактором, що руйнує систему економічних відносин різних рівнів як з середини, так і ззовні. Аналіз наукових джерел дав можливість згрупувати усі підходи відповідно до того як їх тлумачать автори, зокрема: кримінально-карані корисливі діяння; вид злочинів; протиправна діяльність; соціально-економічне явище; умисні корисливі злочини; діяння у сфері економічних відносин; порушення інтересів; джерела тіньової економіки; корисливі зазіхання; навмисні*