МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТУСА

ЦВІРА МАКСИМ ФЕДОРОВИЧ

Допускається до захисту:
Завідувач кафедри
інформаційних технологій,
к.т.н., доцент
_____Нескородєва Т. В.
«__»_____20__р.

АТАКИ НА КОРПОРАТИВНІ МЕРЕЖІ ПІД ЧАС ВІДДАЛЕНОЇ РОБОТИ СПІВРОБІТНИКІВ

Спеціальність 125 Кібербезпека

Кваліфікаційна (бакалаврська) робота

Науковий керівник:

Цвіра М. Ф.,
Професор кафедри інформаційних технологій,
д.т.н, професор

_____
(підпис)

Оцінка : _____ / _____ / _____
(бали/за шкалою ЄКТС/за національною шкалою)

Голова ЕК: _____
(підпис)

Вінниця 2021

АНОТАЦІЯ

Цвіра М.Ф. Атаки на корпоративні мережі під час віддаленої роботи співробітників. Спеціальність 125 “Кібербезпека”. Донецький національний університет імені Василя Стуса, Вінниця, 2021.

У кваліфікаційній роботі проаналізовано зміни в атаках на корпоративні мережі під час пандемії COVID-19. Показано роботу фішинг атаки. Запропоновано портативний скрипт для захисту від фішинг-атак.

Ключові слова: Корпоративна мережа, захист корпоративної мережі, соціальна інженерія, фішинг-атаки.

45 сторінок, 13 рисунків, 32 джерела.

Tsvira M.F. Attacks on corporate networks during remote work of employees. Speciality 125 “Cybersecurity”. Vasyl’ Stus Donetsk National University, Vinnytsia, 2021.

The qualification work analyzes changes in attacks on corporate networks during the COVID-19 pandemic. The work of a phishing attack is shown. A portable script for protection against phishing attacks has been proposed.

Key words: corporate network, corporate network protection, social engineering, phishing attack.

46 pages, 13 figures, 32 items.

ЗМІСТ

ВСТУП

Актуальність теми дослідження: Пандемія COVID-19 та накладене блокування призвели до того, що все більше людей залишаються вдома, набагато більше годин проводять в Інтернеті щодня, і все більше покладаються на Інтернет для доступу до послуг, які вони зазвичай отримують в автономному режимі.

Небезпека кіберзлочинності існує вже багато років, але збільшення відсотка населення, підключеного до Інтернету та часу проведеного в Інтернеті, забезпечили більше можливостей для кіберзлочинців скористатися ситуацією та заробити більше грошей, або підірвати репутації компаній.

Обмеження, накладені урядами у відповідь на пандемію коронавірусу, спонукали працівників залишатися та працювати вдома. Як наслідок, технології віддаленої роботи набули ще більшого значення як у нашому робочому, так і в особистому житті. Незважаючи на зростання потреб у даних технологіях помітно, що багато організацій досі не можуть забезпечити безпечного з'єднання віддаленим робочим столом.

Країни по всьому світу повідомляють про збільшення кіберзлочинності під час пандемії. [2] Наприклад, в Італії Polizia Postale, яка є правоохоронним відділенням, відповідальним за кіберзлочини, повідомила про декілька видів шахрайства [3], які надходили у формі оголошень, електронних листів, фальшивих веб-сайтів, а також через телефонні дзвінки та повідомлення. Кіберзлочинці виграють від невміння людей захистити свої пристрої в інтернеті. Використовуючи шкідливі програми, такі як віруси, хробаки, троянські коні, програми-вимагателі та різна шпигунські програми, для вторгнення, пошкодження, викрадення або редагування персональних даних, як на персональних, так і на

кооперативних комп'ютерах. Потім вкрадені дані можна використовувати для різних зловмисних цілей, включаючи доступ до банківських рахунків та шантажу жертв в обмін на викуп.

Також масово почалось з'являтись фальшиве антивірусне програмне забезпечення. Наприклаад “Corona antivirus”, який обіцяє захистити пристрій користувача від коронавірусу, але замість цього він порушує безпеку комп'ютера і бере під свій контроль комп'ютер, ефективно дозволяючи злочинцеві дистанційно керувати ним.

Поширені техніки кіберзлочинності, такі як фішинг, помітно зросли. Фішинг – це шахрайська практика змушувати людей розкривати особисту інформацію, таку як паролі та номери кредитних карток, через підроблені веб-сайти чи електронні листи. Нові дані, зібрані Google та проаналізовані Atlas VPN, постачальником послуг віртуальної приватної мережі (VPN), проливають більше світла на сферу цього. Згідно з повідомленням, у січні Google зареєстрував 149 тис. Активних фішингових веб-сайтів. У лютому ця кількість майже подвоїлася і становила 293 тис. Однак у березні ця кількість зросла до 522 тис. - на 350% більше, ніж у січні. [1]

Там, де традиційно ділові зустрічі проводяться особисто, більшість зараз проводяться фактично.

Мета дослідження: Розглянення варіантів можливих атак на корпоративні мережі, аналіз змін їх внаслідок карантину та розробка рекомендацій комплексу мір по протидії.

Виходячи з поставленої мети дослідження, необхідно вирішити наступні **завдання**:

- Розкрити поняття корпоративної мережі та її функції;
- Розглянути можливі атаки на корпоративні мережі;
- Проаналізувати зміни в атаках під час пандемії “корановірус”;

- Розглянути найпопулярніші атаки на мережі під час карантину та продемонструвати їх на практиці;
- Оцінити рівень розвитку технологій;
- Запропонувати комплекс мір, для безпечної віддаленої роботи під час карантину;
- Сформувати рекомендації та висновки.

Об’єкт дослідження: найпопулярніші атаки на корпоративні мережі під час віддаленої роботи співробітників.

Предмет дослідження: перспективи розвитку безпечних корпоративних мереж та максимального захисту від кібератак.

Методи дослідження. Для реалізації визначеної мети та вирішення поставлених завдань використано комплекс взаємодоповнюючих загальнонаукових та спеціальних методів дослідження та аналізу, зокрема:

- історичний та логічний метод;
- методи синтезу та системного аналізу;
- методи спостереження, порівняння, графічні та статистичні методи обробки інформації.

Структура кваліфікаційної (бакалаврської) роботи

Кваліфікаційна (бакалаврська) робота складається зі вступу, трьох розділів основної частини, висновків, списку використаних посилань із 32 найменувань. Загальний обсяг роботи складає 44 аркуші.

.

Розділ 1. Корпоративні мережі

1.1. Поняття корпоративної мережі

Будь-яка організація – це сукупність взаємодіючих елементів (підрозділів), кожен з яких може мати свою структуру. Елементи пов'язані між собою функціонально, тобто вони виконують окремі види робіт в рамках єдиного бізнес процесу, а також інформаційно, обмінюючись документами, факсами, письмовими та усними розпорядженнями і т.д. Крім того, ці елементи взаємодіють із зовнішніми системами, причому їх взаємодія також може бути як інформаційна, так і функціональна. І ця ситуація справедлива практично для всіх організацій, яким би видом діяльності вони не займалися - для урядової установи, банку, промислового підприємства, комерційної фірми і т.д.

Такий загальний погляд на організацію дозволяє сформулювати деякі загальні принципи побудови корпоративних інформаційних систем, тобто інформаційних систем в масштабі всієї організації [4].

Корпоративна мережа – система, що забезпечує передачу інформації між різними додатками, використовуваними в системі корпорації. Корпоративна мережа являє собою мережу окремої організації, що працює по протоколу TCP / IP і використовує комунікаційні стандарти Інтернету, а також сервісні програми, що забезпечують доставку даних користувачам мережі. Наприклад, підприємство може створити сервер Web для публікації оголошень, виробничих графіків і інших службових документів. Службовці здійснюють доступ до необхідних документів за допомогою засобів перегляду Web [5].

Сервери Web корпоративної мережі можуть забезпечити користувачам послуги, аналогічні послуг Інтернету, наприклад роботу з гіпертекстовими сторінками (що містять текст, гіперпосилання, графічні зображення та інше),

надання необхідних ресурсів по запитах клієнтів Web, а також здійснення доступу до баз даних. У цьому керівництві всі служби публікації називаються "службами Інтернету" незалежно від того, де вони використовуються (в Інтернеті або корпоративної мережі).

Корпоративна мережа, як правило, є територіально розподіленої, тобто об'єднує офіси, підрозділи та інші структури, що знаходяться на значній відстані один від одного. Принципи, за якими будується корпоративна мережа, досить сильно відрізняються від тих, що використовуються при створенні локальної мережі. Це обмеження є принциповим, і при проектуванні корпоративної мережі слід вживати всіх заходів для мінімізації обсягів переданих даних [6]. В іншому ж корпоративна мережа не повинна вносити обмежень на те, які саме програми та яким чином обробляють переносити по ній інформацію.

1.1.1. Функції корпоративної мережі

Сучасні технології передачі даних надають своїм користувачам широкі можливості по організації різних видів послуг і сервісів [7]:

- Організацію електронного документообігу та ведення спільних архівів документів;
- Організацію корпоративної телефонної мережі з єдиним планом нумерації;
- Організацію систем конференц-зв'язку, в тому числі відеоконференц-зв'язку;
- Побудова розподільних систем відеоспостереження з єдиним центром зберігання даних;
- Організацію дистанційного доступу до файлів і серверів з базами даних;
- Підключення до мережі Інтернет з можливістю організація єдиної корпоративної політики інформаційної безпеки;

- Надання доступу до глобальних фінансових, торговим та інформаційним системам.

Крім забезпечення безпеки корпоративна мережа несе в собі і економічну вигоду. Одним із прикладів може служити організація міжміських дзвінків всередині мульти сервісно-корпоративної мережі, з використанням VoIP, що набагато дешевше вартості звичайного міжміського трафік.

1.1.2. Локальна мережа

Корпоративна мережа традиційно базується на стандартах мережі LAN з апаратними комутаторами, маршрутизаторами, Ethernet-кабелями, підключенням Wi-Fi і інтегрованим ПЗ брандмауера, тобто з усіма компонентами, які зазвичай використовуються для створення локальної обчислювальної мережі [8]. Мережеві маршрутизатори і комутатори виконують два завдання: вони підключають мережу LAN до мереж інтернет-провайдерів через оптоволоконну або широкосмуговий інфраструктуру ГВС, а також забезпечують високошвидкісний обмін даними між локальними машинами в офісі, навчальному закладі або на виробництві.

У локальної обчислювальної мережі (LAN) кілька настільних комп'ютерів підключені один до одного для спільного використання принтерів, ПО, файлів, інтернет-з'єднань і інших ресурсів. [9] Для забезпечення безпечного доступу до мережі з настільних комп'ютерів або мобільних телефонів створюються облікові записи користувачів. Користувачам зазвичай потрібно ввійти, ввівши пароль або використовуючи інший засіб перевірки особистості. У корпоративних мережах часто використовується ПО для роботи з віртуальною приватною мережею (VPN), яке зашифровує дані користувачів при підключенні до веб-сайтів або серверів за межами мережі LAN. ПО брандмауера використовується для установки правил, наприклад для того, щоб заборонити доступ до певних веб-

сайтів з офісу або санкціонувати підключення користувачів з певних IP-адрес для доступу до внутрішніх службам. Налаштування брандмауера і прокладка кабелів між настільними комп'ютерами - важливі етапи створення корпоративної мережі, що забезпечують можливість адміністрування корпоративної LAN.

Корпоративна мережа працює за допомогою високошвидкісних комутаторів і маршрутизаторів, які керують передачею даних між настільними комп'ютерами, серверами і іншими пристроями. Мережеві комутатори та маршрутизатори фізично підключаються до оптоволоконних і широкосмуговим з'єднанням, а також часто використовуються для виконання ПО брандмауера в складі мікропрограм на пристроях. Адміністратори і фахівці з обслуговування мережі підключають настільні комп'ютери до маршрутизаторів в офісах, освітніх установах або на виробництві за допомогою Ethernet-кабелів або по мережі Wi-Fi. Кожному кінцевому пристрою присвоюється ідентифікаційний номер в мережі. Крім того, потрібно створити облікові записи користувачів, щоб співробітники могли входити в систему після перевірки облікових даних. Системні адміністратори налаштовують правила брандмауера і обмеження доступу через Інтернет для мережі відповідно до організаційними вимогами до управління.

За допомогою корпоративної мережі LAN можна забезпечити виконання ПО в рамках спеціалізованих ліцензійних угод одночасно для декількох користувачів або спільне використання принтерів. Приватний ЦОД можна розмістити в мережі LAN, яка обслуговує програми бази даних і інше програмне забезпечення для співробітників, в якій веб-сервери звертаються до загальнодоступних ресурсів з використанням стандартів HTTP/HTTPS і TCP/IP для передачі файлів. Доступ до сервера LAN зазвичай надається тільки уповноваженим співробітникам. Протягом останніх 10 років корпорації все частіше звертаються до постачальників і платформ публічних хмар для отримання IT-послуг, які необхідно інтегрувати в корпоративні політики безпеки. Тепер брандмауери необхідно налаштовувати для підтримки додатків

SaaS, які розміщуються у віддалених середовищах з використанням безпечних зашифрованих мережевих підключень через VPN. Усі надіслані електронні листи, викачані матеріали, загальні файли і встановлені локальні додатки повинні перевірятися агентами брандмауера, щоб забезпечити безпеку мережі в корпоративному середовищі.

Швидкість підключення по мережі LAN залежить від маршрутизатора, кабелів і мережевих стандартів, вбудованих в системну архітектуру. Ethernet-кабелі забезпечують максимальну швидкість передачі пакетів даних на рівні 10 Мбіт/с. Швидка мережа Ethernet дозволяє передавати дані зі швидкістю до 100 Мбіт/с, а гігабітна мережа Ethernet забезпечує швидкість до 1000 Мбіт/с. У деяких конфігураціях мережі використовується поєднання комутаторів управління, що підвищує швидкість передачі даних між локальними маршрутизаторами, серверами, концентраторами та мережевими пристроями брандмауера.

1.1.3. Глобальна мережа

Глобальні мережі (Wide Area Networks, WAN), які також називають територіальними комп'ютерними мережами, служать для того, щоб надавати свої сервіси великій кількості кінцевих абонентів, розкиданих по великій території - в межах області, регіону, країни, континенту або всієї земної кулі. Зважаючи на великий протяжності каналів зв'язку, побудова глобальної мережі вимагає дуже великих витрат, в які входить вартість кабелів і робіт по їх прокладці, витрати на комутаційне обладнання та проміжну підсилювальну апаратуру, що забезпечує необхідну смугу пропускання каналу, а також експлуатаційні витрати на постійне підтримання в працездатному стані розкиданої по великій території апаратури мережі.

Типовими абонентами глобальної комп'ютерної мережі є локальні мережі підприємств, розташовані в різних містах і країнах, яким потрібно обмінюватися даними між собою [10]. Послугами глобальних мереж користуються також і окремі комп'ютери. Великі комп'ютери класу майнфреймів зазвичай забезпечують доступ до корпоративних даних, в той час як персональні комп'ютери використовуються для доступу до корпоративних даних і публічним даними Internet.

Глобальні мережі зазвичай створюються великими телекомунікаційними компаніями для надання платних послуг абонентам. Такі мережі називають публічними або громадськими. Існують також такі поняття, як оператор мережі і постачальник послуг мережі. Оператор мережі (network operator) – це та компанія, яка підтримує нормальну роботу мережі. Постачальник послуг, часто званий також провайдером (service provider), - та компанія, яка надає платні послуги абонентам мережі. Власник, оператор і постачальник послуг можуть об'єднуватися в одну компанію, а можуть представляти і різні компанії.

Набагато рідше глобальна мережа повністю створюється якоюсь великої корпорацією (такий, наприклад, як Dow Jones) для своїх внутрішніх потреб. У цьому випадку мережа називається приватною. Дуже часто зустрічається і проміжний варіант – корпоративна мережа користується послугами чи обладнанням громадської глобальної мережі, але доповнює ці послуги або обладнання своїми власними. Найбільш типовим прикладом тут є оренда каналів зв'язку, на основі яких створюються власні територіальні мережі.

1.2 Варіанти можливих атак на корпоративну мережу

Мережева атака – це спроба отримати несанкціонований доступ до мережі організації з метою викрадення даних, або здійснення іншої шкідливої діяльності.

Виділяють такі типи мережевих атак [11]:

- Атаки на кінцеві точки - отримання несанкціонованого доступу до пристроїв користувачів, серверів чи інших кінцевих точок, зазвичай компрометуючи їх, заражаючи шкідливим програмним забезпеченням.
- Атаки шкідливого програмного забезпечення – зараження IT-ресурсів шкідливим програмним забезпеченням, що дозволяє зловмисникам компрометувати системи, красти дані та завдавати шкоди. Сюди також відносяться атаки-вимагачі.
- Уразливості, експлоіти та атаки – використання вразливостей програмного забезпечення, що використовується в організації, для отримання несанкціонованого доступу, компрометації або саботажу систем.
- Розширені постійні загрози – це складні багатошарові загрози, що включають мережеві атаки, а також інші типи атак.

Під час мережевих атак зловмисники орієнтовані на проникнення в периметр корпоративної мережі та отримання доступу до внутрішніх систем [12]. Дуже часто, потрапляючи всередину, зловмисники поєднують декілька тип атак, наприклад, компрометуючи кінцеву точку, поширюючи шкідливе програмне забезпечення та використовуючи вразливість у системі, в мережі.

Також основні типи мережевих атак можна поділити:

1) За характером впливу на активні і пасивні. Активна атака націлена на зміну алгоритмів роботи частин системи і, відповідно, всієї системи в цілому.

Зміна алгоритмів досягається, наприклад, зміною конфігурації системи, логіки роботи мережевих з'єднань і сервісів, виведення з ладу окремих частин системи. Пасивна атака реалізує загрозу розкриття шляхом прослуховування каналів зв'язку і не надає при цьому впливу на функціонування системи;

2) По розташуванню джерела на внутрішні, мережеві і міжмережеві атаки. При внутрішньої атаці джерело розташоване в одному домені колізій з атакованим об'єктом і має можливість прослуховувати абсолютно всі мережеві пакети об'єкта. Під час мережевої атаки джерело знаходиться в одній IP-мережі з атакованим об'єктом, але мережа може бути сегментована комутатором, внаслідок чого атакуючий може прослуховувати тільки широкомовні пакети об'єкта. У разі міжмережевий атаки джерело і об'єкт розташовані в різних IP-мережах, розділених або маршрутизатором, або фаєрволом Firewall;

3) За умовою початку виконання на умовні та безумовні атаки. У разі умовної атаки, атакуючий очікує від об'єкта генерації запиту певного типу (наприклад, генерації DNS-запиту до DNS-сервера) або настання в роботі об'єкта очікуваної події (наприклад, виключення комп'ютера легального користувача без команди LOGOUT). Безумовна атака на увазі активний вплив на об'єкт, незважаючи на стан атакується системи. Прикладом може служити генерація атакуючим великого числа пакетів відкриття сеансів зв'язку для реалізації загрози відмови в обслуговуванні;

4) По наявності зворотного зв'язку на атаки, що вимагають отримання атакуючим відповідних пакетів від об'єкта, і атаки, які не потребують зворотного зв'язку;

5) За рівнем моделі OSI, на якому робиться атака. На фізичному наприклад, безпосереднє підключення до проводів ліній зв'язку для проведення прослуховування лінії або фактичний обрив комунікацій для нейтралізації одного з суб'єктів атаки. На канальному рівні можливе захоплення пакетів з єдиної, яку поділяє середовища. На мережевому рівні об'єктом атаки стає

детаграмна передача IP-пакетів. На транспортному рівні об'єктом впливу стають алгоритми протоколів TCP і UDP, на сеансовому рівні можлива, наприклад, атака з підміною одного із суб'єктів TCP-з'єднання, на представницькому – атаки з підміною портів. Атака на прикладному рівні впливає на алгоритми роботи конкретного додатка.

1.3 Аналіз змін кібератак у наслідок карантину

Обмеження, накладені урядами у відповідь на пандемію коронавірусу, спонукали працівників працювати вдома. Як наслідок, технологія набула ще більшого значення як у нашому робочому, так і в особистому житті. Незважаючи на зростання потреб у технологіях, помітно, що багато організацій все ще не забезпечують віддаленого робочого середовища, що забезпечує безпеку в мережі. Там, де традиційно ділові зустрічі проводяться особисто, більшість зараз проводяться фактично.

У зв'язку з тим, що COVID-19 змінює ситуацію в правоохоронній сфері, Інтерпол (Міжнародна організація кримінальної поліції) опублікував оцінку глобальної загрози злочинності та поліцейської діяльності для своїх 194 країн-членів. Доповідь [13], призначена тільки для правоохоронних органів, спирається на експертні знання і буде регулярно оновлюватися в міру появи нових загроз. У ній описується «життєвий цикл злочинності», а також кращі практики і заходи щодо пом'якшення наслідків злочинів, пов'язаних з COVID-19.

Зокрема, зазначається, що види злочинів постійно еволюціонують, використовуючи особливості онлайн-поведінки і нових потреб громадян в умовах епідемії COVID-19. Оскільки одна третина населення світу в даний час знаходиться в тій чи іншій формі ізоляції, зміни в структурі злочинності вже дали про себе знати.

Одна з причин сплеску кібератак пов'язана з тим, що деякі малі та середні підприємства застосовують підхід "Принеси свій власний пристрій" (BYOD) (на відміну від підходу "Корпоративна власність особиста активність" (COPE)), які означає, що працівники можуть використовувати свої персональні пристрої (телефони, планшети або ноутбуки) для доступу до корпоративної інформації. Робота вдома не гарантує такого рівня кібербезпеки, як офісне середовище. Користуючись персональним комп’ютером або ноутбуком для доступу до

корпоративних файлів та даних (навіть із захистом рішення MDM), користувачі більше піддаються кібератакам. Наприклад, співробітники не можуть регулярно запускати антивірус чи перевіряти ПК на шкідливе програмне забезпечення. Домашнє робоче середовище не передбачає складних заходів запобігання та виявлення загроз на підприємстві. Крім того, ще однією проблемою, яка викликає занепокоєння, є людська помилка. До пандемії людські помилки вже були основною причиною "кібернезахищеності": працівники несвідомо чи необдумано надавали доступ стороннім людям. Однак при роботі вдома проблема стала ще більшою. Коли працівники працюють вдома, вони можуть перериватися в роботі, яку вони роблять на членів сім'ї або відвідувачів соціальних мереж. Ці відволікаючі фактори можуть зробити людей більш необачними. IT-системи повинні адаптуватися до цих змін у робочій практиці та бути готовими збільшення людських помилок. Цього можна досягти багатьма способами, наприклад, включенням тайм-аутів у ключові інформаційні системи, посиленням контролю за застосуванням "принципу чотирьох очей", забезпеченням розподілу обов'язків (СОД) або автоматизованим контролем.

Шкідливі домени. Кіберзлочинці кожен день створюють тисячі сайтів, які містять слова «коронавірус», «COVID-19», різних варіаціях написання цих термінів і використовують їх для проведення спам-кампаній, фішингу, поширення шкідливих програм або злому серверів, управління і їх контролю.

Шкідливе програмне забезпечення (ПО). Кіберзлочинці користуються популярністю повідомлень про коронавіруси для маскування своєї діяльності. Шкідливі, шпигунські та троянські вірусні программи зазвичай представлені під виглядом інтерактивних карт і веб-сайтів про коронавіруси. Спам-повідомлення також змушують користувачів переходити за посиланнями, які завантажують шкідливе ПО на комп'ютери або мобільні пристрої.

Вимагання. Кіберзлочинці піддають сервери лікарень, медичних центрів і державних установ атакам і вимагання. Установи, що знаходяться на передньому краї боротьби з коронавірусів, що зіштовхуються з безпрецедентною

загрозою для здоров'я, тепер також протистоять ще одну загрозу - з боку кіберзлочинців. Їх доступ до життєво важливих файлів і системам виявляється заблокованим до тих пір, поки не буде виплачений викуп. Оскільки в умовах кризи в галузі охорони здоров'я лікарні не можуть дозволити, щоб їх системи були заблоковані, вони змушені платити злочинцям. Блокування роботи лікарень і їх критичних систем не тільки затримує оперативну медичну діяльність, таку необхідну в період пандемії, але і може безпосередньо привести до смертельних випадків.

Програма-вимагач може проникнути в систему через електронні листи, скомпрометовані облікові дані співробітників або за допомогою вразливостей в системі.

1.3.1 Еволюція фішинг-атак

Все більша кількість хакерів в Інтернеті проводить фішингові та шкідливі атаки на робітників, компанії, медичні установи та безробітних. Фактично, останнім часом фішингові електронні листи, пов’язані з COVID-19, зросли на 600%. У першому кварталі 2020 року OpSec Security [14] виявив, що сайти SaaS та веб-пошти є найбільшими об'єктами фішингу, на них припадає більше третини (34%) усіх атак, за ними ідуть потім фінансові установи (19%) та платіжний сектор (13%).

Спосіб фішинг атак також змінюється разом із кількістю випадків. Сюди входить використання занепокоєнь щодо вірусу та бажання йти в ногу з останніми розробками, щоб зробити електронні листи більш законними. Наприклад, деякі кіберзлочинці поширюють шкідливе програмне забезпечення, додаючи текст із новин COVID-19 до фішинг-листів, щоб обійти програмне забезпечення безпеки, яке використовує штучний інтелект (AI) та машинне навчання (ML) для його виявлення. Компанії без захисту, яке існує для

запобігання цим більш складним атакам, підприємства та корпорації ставлять під загрозу своїх клієнтів та своїх працівників.

В результаті цих посилених атак ряд гучних технологічних підприємств, таких як Microsoft, вживають більш жорстких заходів проти кіберзлочинців. У 2020 році відділ цифрових злочинів (DCU) Microsoft [15] здійснив широкомасштабну ділову процедуру щодо електронної пошти, в ході якої хакери використовували фішинг-листи, пов’язані з COVID-19, для проникнення в облікові записи електронної пошти клієнтів, списки контактів та конфіденційні документи, щоб надсилати електронні листи, схожі на те, що вони надійшли з надійного джерела. Незважаючи на те, що це не такий підхід, який можуть застосовувати всі підприємства, робота з відповідними партнерами та органами, та наявність інструментів для запобігання фішинговим атакам, що проскакують через мережу, пом'якшують ризик, пов’язаний із цим видом діяльності.

Розділ 2. Найпопулярніші атаки на практиці під час карантину

2.1 Соціальна інженерія

Під час карантину атаки за допомогою соціальної інженерії виросли майже в два рази і стали одні із самих популярних по всьому світу.

Соціальна інженерія – це метод управління діями людини без використання технічних засобів. Метод заснований на використанні слабкостей людського фактора і вважається дуже руйнівним. Найчастіше соціальну інженерію розглядають як незаконний метод отримання інформації, проте це не зовсім так. Соціальну інженерію можна також використовувати і в законних цілях, і не тільки для отримання інформації, а й для здійснення дій конкретною людиною. Сьогодні соціальну інженерію часто використовують в інтернеті, для отримання закритої інформації, або інформації, яка є великою цінністю.

Соціальна інженерія – це сукупність підходів в прикладних соціальних науках, орієнтованих:

- на зміну поведінки і установок людей;
- на вирішення соціальних проблем;
- на адаптацію соціальних інститутів до умов, що змінюються;
- на збереження соціальної активності.

Зловмисник отримує інформацію, наприклад, шляхом збору інформації про службовців об'єкта атаки, за допомогою звичайного телефонного дзвінка або шляхом проникнення в організацію під виглядом її службовця. Наприклад він може подзвонити працівникові компанії (під виглядом технічної служби) і вивідати пароль, пославшись на необхідність вирішення невеликої проблеми в комп'ютерній системі. Дуже часто цей трюк проходить, адже більшість

працівників в компаніях не є освідченими в безпеці користування ПК. Також імена службовців вдається дізнатися після дзвінків і вивчення імен керівників, які є на сайті компанії і інших джерел відкритої інформації (звітів, реклами і т. п.).

Використовуючи реальні імена в розмові зі службою технічної підтримки, зловмисник розповідає вигадану історію. Наприклад, що не може потрапити на важливу нараду на сайті зі своїм обліковим записом віддаленого доступу [16].

Соціальна інженерія – це відносно молода наука, яка є складовою частиною соціології, і претендує на сукупність тих специфічних знань, які направляють, упорядковують і оптимізують процес створення, модернізації та відтворення нових («штучних») соціальних реальностей. Певним чином вона «добудовує» соціологічну науку, завершує її на фазі перетворення наукових знань в моделі, проекти та конструкції соціальних інститутів, цінностей, норм, алгоритмів діяльності, відносин, поведінки і т. П. Заняття зорієнтовані на озброєння слухачів насамперед методологією аналітико синтетичного мислення і знаннями формалізованих процедур (технологій) конструкторсько-винахідницької діяльності. У характеристиці формалізованих операцій, з яких складається ця остання, особлива увага звертається на операції складної комбінаторики. Ігнорування принципу системності в операціях комбінаторики завдали і продовжують завдавати великої шкоди на всіх рівнях трансформаційних процесів, які відбуваються в нашому суспільстві. Послідовні знання принципових вимог до зазначених операцій дають підстави до запобігання помилкових збочень в реформаційної практиці на її макро-, мезо- і мікрорівнях.

2.1.1. Типи соціальної інженерії

Всі техніки соціальної інженерії засновані на особливостях прийняття рішень людьми, які називаються когнітивним базисом [17]. Вони також можуть бути названі особливістю прийняття рішення людської і соціальної психологій, заснованої на тому, що людина повинна комусь довіряти в соціальному середовищі виховання.

1) Претекстінг

Претекстінг – це дія, відпрацьований за заздалегідь складеним сценарієм (претексту). В результаті мета повинна видати певну інформацію або вчинити певну дію. Цей вид атак застосовується зазвичай по телефону. Найчастіше ця техніка включає в себе більше, ніж просто брехня, і вимагає будь-яких попередніх досліджень (наприклад, персоналізації: дата народження, сума останнього рахунку і ін.), З тим, щоб забезпечити довіру у цілі. До цього ж виду належать атаки і по онлайн-мессенджерам.

2) Фішинг

Фішинг – техніка, спрямована на шахрайське отримання конфіденційної інформації. Зазвичай зловмисник посилає цілі e-mail, підроблений під офіційний лист - від банку, або платіжної системи. Вимагає перевірки певної інформації або здійснення певних дій. Цей лист зазвичай містить посилання на фальшиву веб-сторінку, яка імітує офіційну, з корпоративним логотипом і контентом, і містить форму, що вимагає ввести конфіденційну інформацію, таку як: логіни, паролі, пін-коди, домашню адресу та інше.

3) Троянський кінь

Троянський кінь – це техніка грунтується на цікавості, страху або інших емоціях користувачів. Зловмисник відправляє лист жертві за допомогою електронної пошти чи мессенджерів, як додаток до якого знаходиться «оновлення» антивіруса, ключ до грошового виграшу або компромат на співробітника. Насправді ж у вкладенні знаходиться шкідлива програма, яка

після того, як користувач запустить її на своєму комп'ютері, буде використовуватися для збору або зміни інформації зловмисником.

4) Кви про кво (послуга за послугу)

Кви про кво (послуга за послугу) – дана техніка передбачає звернення зловмисника до користувача по електронній пошті або корпоративному телефону. Зловмисник може представитися, наприклад, співробітником технічної підтримки та інформувати про виникнення технічних проблем на робочому місці. Далі він повідомляє про необхідність їх усунення. У процесі «рішення» такої проблеми, зловмисник підштовхує жертву на вчинення дій, що дозволяють атакуючому виконати певні команди або встановити необхідне програмне забезпечення на комп'ютері жертви.

5) Дорожнє яблуко

Дорожнє яблуко – цей метод є адаптацію троянського коня і полягає у використанні фізичних носіїв (CD, флеш-накопичувачів). Зловмисник зазвичай підкидає такий носій в загальнодоступних місцях на території компанії (парковки, столові, робочі місця співробітників, туалети). Для того, щоб у співробітника виник інтерес до даного носія і він вставив носій у робочий ПК. Щоб більше зацікавити працівників зловмисник може нанести на носій логотип компанії або якісь підписи. Наприклад, «дані про продажі», «зарплата співробітників», «звіт в податкову» та інше.

6) Зворотня соціальна інженерія

Зворотній соціальна інженерія – даний вид атаки спрямований на створення такої ситуації, при якій жертва змушена буде сама звернеться до зловмисника за «допомогою». Наприклад, зловмисник може вислати лист з телефонами і контактами «служби підтримки» і через деякий час створити оборотні неполадки в комп'ютері жертви. Користувач в такому випадку подзвонить або зв'яжеться по електронній пошті з зловмисником сам, і в процесі «виправлення» проблеми зловмисник зможе отримати необхідні йому дані.

2.1.2 Атака за допомогою соціальної інженерії

Атаки соціальної інженерії є найбільш успішними проти тих, хто ще не стикався з нею [18] та не знає про потенційні загрози, можливі шахрайські чи зловмисні наміри. Виділяють 4 основні кроки в атаках соціальної інженерії:

a) Збір інформації. Більшість атак соціальної інженерії спрямовані на дуже велику аудиторію. Інформація, яку збирають зловмисники, буває двох типів. Одним із них є загальна контактна інформація якомога більшої кількості цілей. Це використовується для початкового підходу до даних цілей. Лише після певного аналізу цілі та її оточуючих зловмисники йдуть далі. Також злочинці перешкоджають цілі, для того щоб зібрати інформацію іншого типу [19]. Сюди входять жаргон та інші терміни, з якими ціль може асоціюватись. Ця інформація часто допомагає зловмиснику на наступних кроках атаки соціальної інженерії. На цьому етапі атаки соціальної інженерії населення, яке не знає про наслідки розкриття інформації для безпеки. Основними помилками людей є те, що вони не розуміють важливості даних для соціального інженера, що призводить до розкриття інформації. Вони можуть включати розкриття інформації, яка з точки зору безпеки, мабуть нешкідлива для очей даної людини, але може бути корисною для зловмисника.

b) Розвиток стосунків з ціллю. Готовність цілі ділитися інформацією та відповідати взаємністю відіграє дуже важливу роль в атаці. Лише та частина населення, яка знає про соціальну інженерію додатково орієнтована. На основі інформації, зібраної зловмисником на попередньому кроці атаки, вони намагаються ввійти в стосунки з жертвою. Для цього вони часто використовують зібрану інформацію та намагаються ввійти в образ, який зміг би зацікавити ціль. При

формуванні стосунків зловмисник використовує властиву манеру спілкування, якій слід довіряти. Зловмисник виведе жертву в позицію впевненості при встановленні партнерства, яким він потім може маніпулювати. Люди мають бажання довіряти іншим і піклуватися про них. Для того, щоб використовувати та впливати на людей для створення автентичності та набуття впевненості, соціальні інженери часто використовують дані властивості. Цифровий контакт – це взаємодія із засобами масової інформації, такими як телефон, електронна пошта чи навіть соціальні медіа. Такі маніпуляції, як перевантаження, зворотно-поступальний рух та поширення прозорості, є універсальними психологічними поняттями.

c) Експлуатація цілі на основі стратегії цілеспрямованої атаки. Тепер зловмисники соціальної інженерії мають доступ до інформації цілі, її місцезнаходження або іншої важливої інформації. Використовуючи стосунки та впевненість, створені людиною шляхом примусу на попередньому етапі, або реалізуючи інші подібні тактики зловмисник використовує ціль, щоб отримати паролі або виконати дії, які не відбудуться за звичайних обставин. У цей момент зловмисник може закінчити або перенести його на наступний рівень.

d) Виконання атаки. На цьому етапі зловмисники використовують всю доступну інформацію, щоб зробити остаточний хід і отримати гроші, інформацію чи конфеденційну інформацію від цілі. Якщо всі попередні етапи були успішними, зловмисники майже завжди добиваються успіху.

2.2 Фішинг атаки під час карантину

Кіберзлочинність можна сприймати як бізнес, який має погані наміри. Але, як і будь-який інший суб'єкт господарювання, кінцевою метою будь-якого кіберзлочинця є отримання прибутку за роботу, яку вони виконують. Коли кіберзлочинність розглядається з такої точки зору, пандемія COVID-19 може розглядатися як нова можливість для бізнесу. Ця унікальна можливість є цікавою для кіберзлочинців, оскільки пандемія штовхає більше людей в Інтернет, збільшуючи кількість користувачів, на яких можна заробити.

Відповідно до звітів від Google, більшість атак зараз виконуються як фішинг-атаки через електронні листи чи веб-сайти [20]. Ці атаки застосовують багато різних тактик. Використовуючи ідентичність бренду відомих організацій та їх торгові марки, такі як назви компаній та логотипи, для розробки фішингових веб-сайтів або надсилання електронних листів, які виглядають як справжні. Це спокушає користувачів вводити конфіденційну інформацію, таку як імена користувачів, паролі, банківські реквізити та інші деталі, які можуть допомогти їх ідентифікувати. Google повідомляє, що вони щодня блокують понад 100 мільйонів фішинг-повідомлень із заявленою точністю 99,9 відсотка [21].

Microsoft повідомив про збільшення кількості фішингових заходів електронної пошти, заявивши, що фішинг-атаки становлять майже 70 відсотків усіх атак. У вересні 2020 року опубліковано звіт про цифрову оборону [22], де повідомляється, що зловмисники виділяють значний час, гроші та зусилля для розробки шахрайства та стратегій атак, щоб обманути навіть тих, хто насторожено ставиться до таких атак. Цей розвиток подій можна пояснити збільшенням доступної для користувачів інформації про такі атаки, підвищенням обізнаності користувачів та технологічним прогресом у виявленні атак. Корпорація Майкрософт, заснована на телеметрії з пропонованого ними

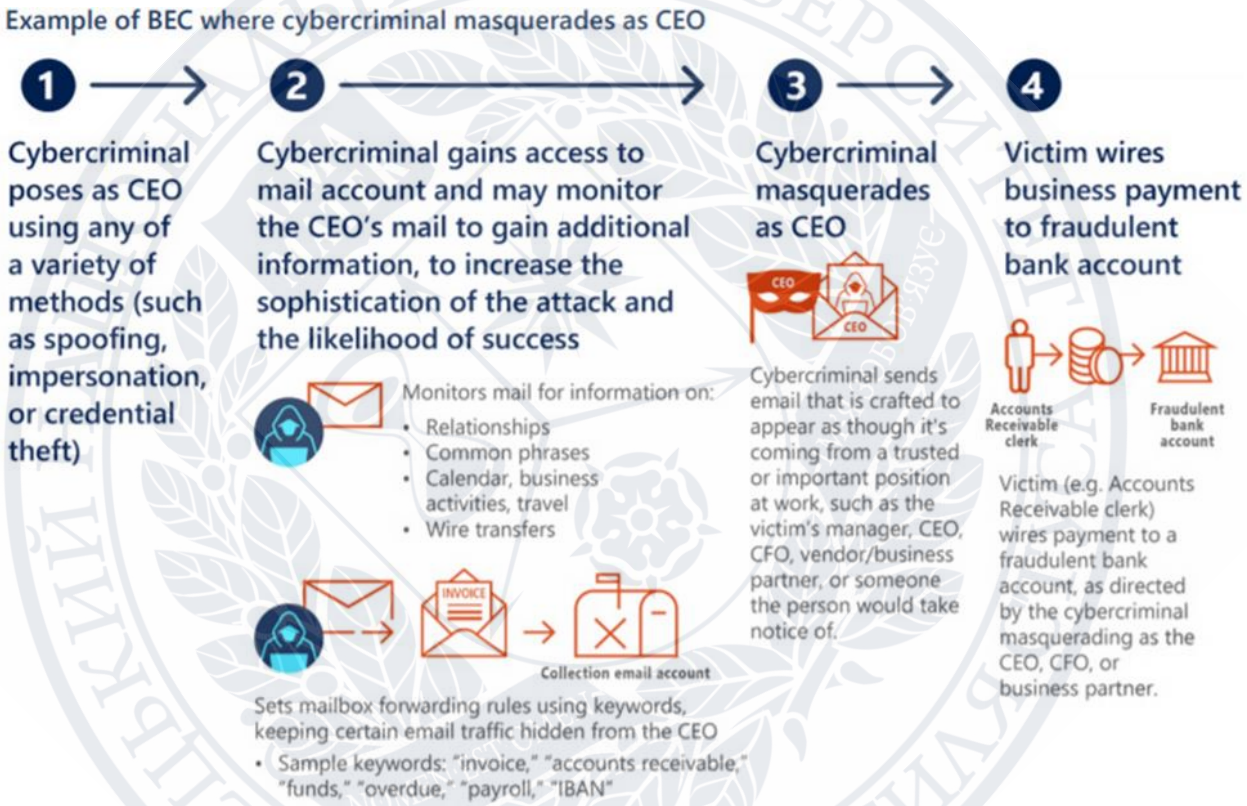
програмного забезпечення для бізнесу “Office365”, повідомляє [22], що користувачі стикаються з трьома основними типами фішингових атак:

- фішинг облікових даних;
- компрометація ділової електронної пошти;
- Поєднання фішингу та компрометації.

Фішинг здійснюється кіберзлочинцем, який видає себе добре відомим сервісом у шаблоні електронної пошти та намагається заманити користувачів на перехід за посиланням, яке переводить їх на фейкову сторінку входу. Коли користувачі вводять свої облікові дані на сторінці, ці облікові дані можна використовувати для подальшого запуску більш глибоких і складних атак, для створення присутності всередині організації за допомогою лише хмарних API та систем. Потім ця присутність використовується для бічного переміщення, щоб викрасти дані, гроші або іншим чином нашкодити організації. Ілюстрація процесу показана на рис.2.2.1.

(Рисунок 2.2.1) Схема фішинг атаки з отриманям конфеденційних даних;

Компрометуючі фішингові атаки на ділову електронну пошту спеціально націлені на бізнес і знаходяться в центрі уваги віддаленої роботи. Цей тип атак характеризується прийомами, які маскуються під когось, хто займає високу посаду в компанії. Наприклад, генерального директора компанії, фінансового директора чи вищого персоналу. Атака може також включати транзакцію між бізнесом. Наприклад, зловмисник може обманним шляхом отримати доступ до системи компанії, а потім діяти як ця компанія, щоб кримінально вимагати оплати в іншої компанії. Ілюстрація нападу наведена Рисунку 2.



(Рисунок 2.2.2) Схема фішинг атаки з вимаганням коштів;

Також поширеним є використання фішингових атак, як засобу доставки шкідливого програмного забезпечення чи програм-вимагачів. Як повідомляється, під час пандемічного періоду атаки з вимогами стали набагато частішими, ніж шкідливі програми. Оскільки програми вимагачі можуть виконувати одну і ту ж роботу, зі збору інформації та грошовими виплатами з цільової групи. Яка платить для дешифрування файлів, які шифрує програмне забезпечення для викупників.

Пандемія та наслідки зміни роботи, а також навчання в Інтернеті можуть розглядатися як каталізатор для збільшення як фішингових атак, так і компромісних атак бізнес-електронної пошти. Вимагальні програми також спричинили атаки зловмисного програмного забезпечення в результаті посиленої активності в мережі під час пандемії. Незважаючи на те, що ці зміни були зафіксовані під час пандемії, основним моментом є зміна стратегій атаки від загальних суб'єктів до тем, пов'язаних з пандемією.

2.2.1 Атаки, які використовують тематику COVID-19

Надзвичайна ситуація в галузі охорони здоров’я, спричинена пандемією COVID-19, а також страх, тривога, невизначеність серед населення, та бажання отримати інформацію про пандемію - ідеальна можливість для кіберзлочинців. Коли новини про пандемію були в заголовках в перші місяці 2020 року, фішинг сайти з темою про пандемію почастішали [23]. Ця тенденція проілюстрована на Рисунку 2. В іншому звіті, підготовленому консалтинговою фірмою Deloitte, відзначається 254-відсоткове збільшення кількості нових тематичних веб-сайтів та субдоменів COVID-19, що реєструвалися щодня на ранніх стадіях пандемії [24]. Це призвело до того, що багато урядових організацій, таких як Федеральне Бюро Розслідувань та Агентство з питань кібербезпеки та інфраструктури у США, випустили попередження про дані події.

Фішингові-електронні листи, які використовували пандемію як приманку, мали такі теми, як «Оновлення коронавірусу 2020», «Коронавірус нові новини», «Нові підтверджені випадки у вашому місті» та «Спалах коронавірусу у нашому місті (Надзвичайна ситуація) ”. Вищезазначені типи електронних листів були спрямовані на людську природу допитливості, інстинкт збору інформації та страх. Вміст таких електронних листів містив вкладення, які розгортали шкідливе програмне забезпечення та програми-вимагачі приводили

до фальшивих сайтів для збору облікових даних користувачів. Вміст був сформульований таким чином, що вони заохочували користувачів відвідувати веб-сайти, які зловмисники використовували для збору цінних даних, таких як імена користувачів та паролі, інформацію про кредитні картки та іншу особисту інформацію[23].

2.3 Evilginx2 та фішинг атака за допомогою даної утиліти

Evilginx2 – це платформа для атаки людина-посередині (man-in-the-middle), яка використовується для крадіжки облікових даних (логіна і пароля) шляхом фішингу. Також вміє перехоплювати куки сеансу, які в свою чергу, дозволяють обійти захист двухфакторної аутентифікації [26].

Цей інструмент є наступником Evilginx, випущеного в 2017, який використовує спеціально налаштовану версію HTTP сервера nginx для забезпечення функціональності людина-посередині, щоб діяти як проксі між браузером і фішингових сайтом. Справжня версія повністю написана на GO і є самостійним додатком, який реалізують свій власний HTTP і DNS сервер, роблячи процес установки і користання простим та зручним.

2.3.1 Історія Evilginx2

Автор Evilginx2 – польський етичний хакер Куба Грецькі. Перша згадка про Evilginx (на той момент ще першої версії) в його блозі датована 6 квітня 2017 року.

Спочатку за основу він узяв два модуля популярного веб-сервера Nginx: sub_filter і proxy_pass. У Evilginx перший модуль блокує доступ жертви до реального ресурсу, а другий передає перехоплені запити на необхідний сервер і назад. Уже на той момент програма представлялася як інструмент, який здатний пробити захист 2FA(двофакторна авторизація) [27].

Розробника запросили для виступу на конференцію WarCon 2018, де його помітив Кевін Митник. Він написав про Evilginx, що послужило відмінною рекламою. Після чого дана утиліта почала швидко набирати популярність. До червня того ж року було випущено два релізу Evilginx - 1.0 і 1.1.

На все тому ж WarCon 2018 Куба Грецькі познайомився з провідним фахівцем з інформаційної безпеки італійської фірми Zimperium – «білим хакером» Сімоном Маргарітеллі, який публікує свої дослідження під псевдонімом evilsocket. Маргарітеллі показав йому всю красу мови Go і

надихнув переписати Evilginx. Рік по тому вийшов повністю перероблений Evilginx 2 [28]. Проект еволюціонував від від ідеї MITM через Nginx до «Evilginx 2 w/o Nginx. Pure Go, and pure evil ». Це був перший переломний момент.

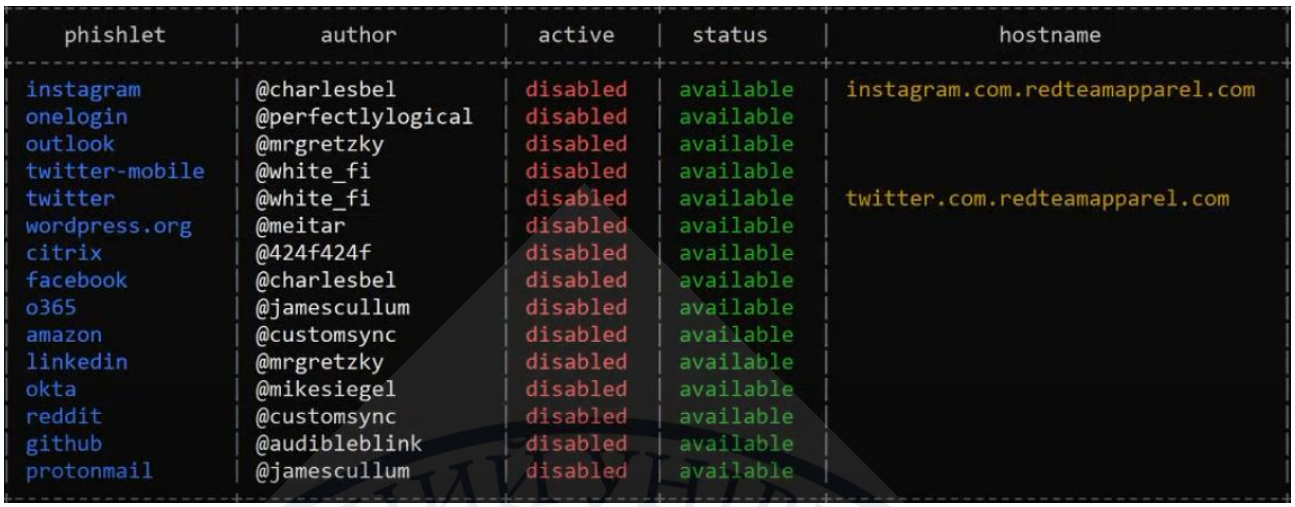
Другий настав, коли світ побачив опенсорсний проект Modlishka. На той момент складність використання Evilginx 2 полягала в проксінг трафіку. Необхідно було писати безліч фільтрів, які б динамічно замінювали посилання на фішингові. Робилося це шляхом проб і помилок, що сильно ускладнювало код.

Потім Куба Грецькі побачив, як реалізована підміна URL в Modlishka. Виявилося, що не обов'язково писати тонни фільтрів - досить один раз додати домен сайту і прописати загальні правила підміни трафіку [29]. Це було народження компонентів phishlets - готових скриптів для імітації структури популярних сайтів.

2.3.2 Атака за допомогою Evilginx2

У даній атаці було підмінено сайт LinkedIn. Для початку був запущений Evilnginx2 на сервері рис 2.3.2.1. На данному етапі можна спостерігати список популярних сайтів, які можемо скопіювати, їх авторів, статус та хостинг рис.2.3.2.2.

(Рисунок 2.3.2.1) Запуск Evilnginx2.

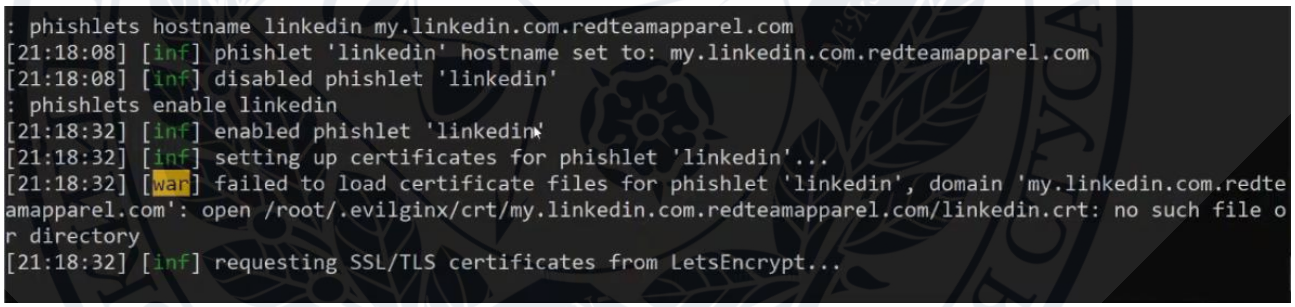


phishlet	author	active	status	hostname
instagram	@charlesbel	disabled	available	instagram.com.redteamapparel.com
onelogin	@perfectlylogical	disabled	available	
outlook	@mrgretzky	disabled	available	
twitter-mobile	@white_fi	disabled	available	
twitter	@white_fi	disabled	available	twitter.com.redteamapparel.com
wordpress.org	@meitar	disabled	available	
citrix	@424f424f	disabled	available	
facebook	@charlesbel	disabled	available	
o365	@jamescullum	disabled	available	
amazon	@customsync	disabled	available	
linkedin	@mrgretzky	disabled	available	
okta	@mikesiegel	disabled	available	
reddit	@customsync	disabled	available	
github	@audibleblink	disabled	available	
protonmail	@jamescullum	disabled	available	

(Рисунок 2.3.2.2) Список популярних сайтів для фішингу.

В першу чергу потрібно було налаштувати фішлет, який використовувався у даній атаці. У даному випадку використовувався фішлет LinkedIn. Тому було прописано команди рис 2.3.2.3:

1) phishlets hostname linkedin my.linkedin.com.redteampparel.com;
2) phishlets enable linkedin.



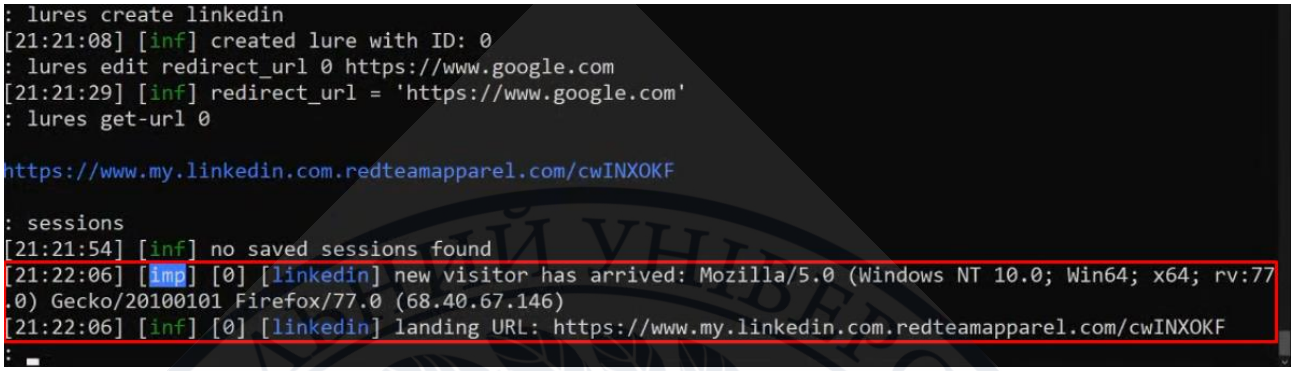
(Рисунок 2.3.2.3) Налаштування фішлета.

Далі коли фішинг-сайт запрацював. Потрібно було вказати, який сайт скопіювати із списку вище. Далі куди жертва буде перенапралена після вводу логіна і пароля на нашому фішинг сайту рис.2.3.2.4.

1) lures create linkedin
2) lures edit 0 redirect_url https://www.google.com
3) lures get-url 0

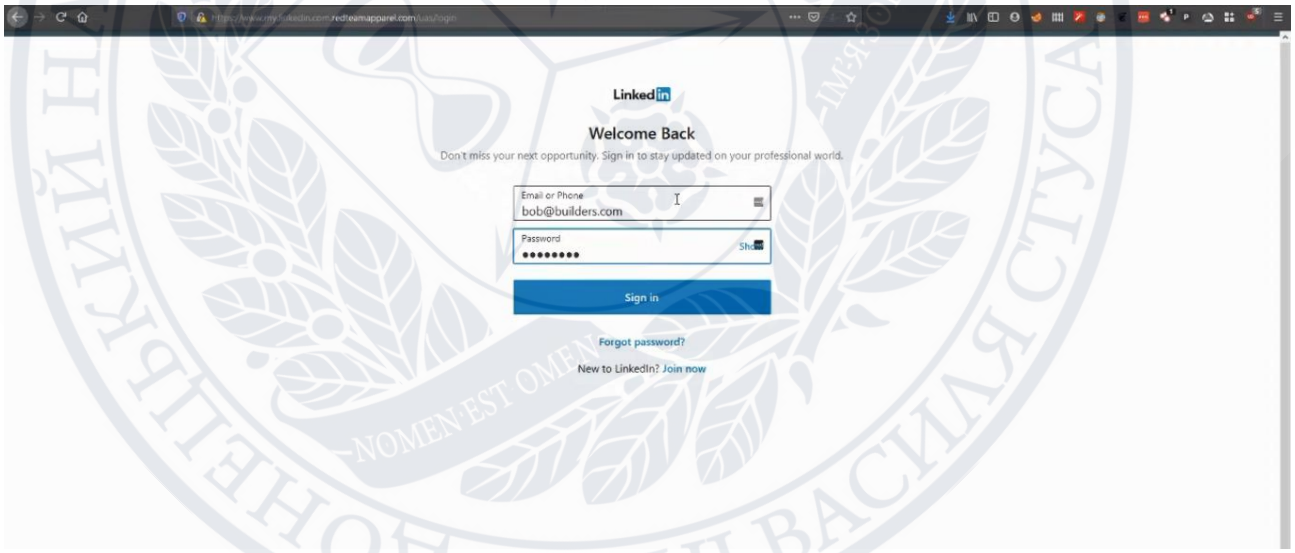
(Рисунок 2.3.2.4) Налаштування фішинг сайта.

Коли налаштування було заершено і фішинг сайт був запущений та працюючим, оставалось тільки дочекатись жертву. Як тільки жертва переходила на сайт, одразу зав’язувалась сесія із її даними. рис.2.3.2.5:



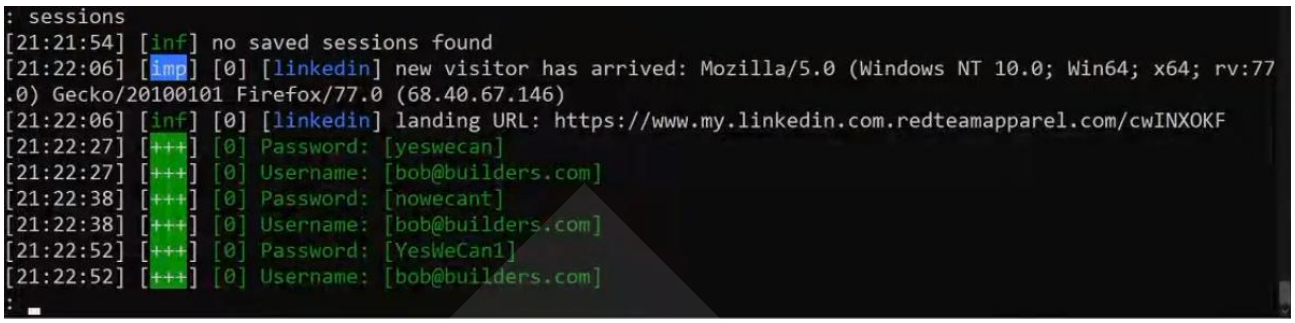
(Рисунок 2.3.2.5) Моніторинг сеансу.

Жертва тим часом намагалась ввести логін та пароль, щоб зайти в свій обліковий запис. У більшості людей декілька паролів і вони не завжди пам’ятають, де який використовували, тому будуть намагатись вводити їх усі рис2.3.2.6.



(Рисунок 2.3.2.6) Фішинговий сайт.

Тим часом було перехоплено усі логіни та паролі, які жертва ввела, що показано на рис 2.3.2.7.



(Рисунок 2.3.2.7) Логіни та паролі жертви.

На даному етапі тестова атака була завершена. Було отримали логіни та паролі жертви, яка перейшла за посиланням та не подивилась на URL-адресу даного сайту. Звісно дану атаку можна було б продовжити і розвинути щодо цілей зловмисника, використовуючи різні типи кібератак. Але головною задачою було показати, як створити та як працюють фішингові сайти. Також як було продемонстровано, це досить просто, а це означає що це може зробити людина з мінімальними навичками володіння комп'ютером. Тому при вводі будь якої персональної інформації потрібно завжди переконуватись, що це дійсно офіційний сайт.

Розділ 3. Комплекс мір по протидії мережевим атакам

3.1 Комплекс мір по протидії соціальній інженерії

Основним способом захисту від методів соціальної інженерії є навчання співробітників. Всі працівники компанії мають бути попереджені про небезпеку розкриття персональної інформації та конфіденційної інформації компанії, а також про способи запобігання витоку даних. Крім того, у кожного співробітника компанії, в залежності від підрозділу і посади, повинні бути інструкції про те, як і на які теми можна спілкуватися зі співрозмовником, яку інформацію можна надавати для служби технічної підтримки, як і що повинен повідомити співробітник компанії для отримання тієї або іншої інформації від іншого співробітника.

Можна виділити наступні правила:

1) Призначені для користувача облікові дані є власністю компанії [30].

Всім співробітникам в день прийому на роботу має бути роз'яснено те, що ті логіни і паролі, які їм видали, не можна використовувати в інших цілях (на web-сайтах, для особистої пошти, тощо), передавати третім особам або іншим співробітникам компанії, які не мають на це право. Наприклад, дуже часто, йдучи у відпустку, співробітник може передати свої авторизовані дані своєму колезі для того, щоб той зміг виконати деяку роботу або подивитися певну інформацію в момент його відсутності.

2) Необхідно проводити вступні та регулярні навчання співробітників компанії, спрямовані на підвищення знань з інформаційної безпеки.

Проведення таких інструктажів дозволить співробітникам компанії мати актуальні дані про існуючі методи соціальної інженерії, а також не забувати основні правила по інформаційної безпеки.

3) Обов'язковою є наявність регламентів з безпеки, а також інструкцій, до яких користувач повинен завжди мати доступ. В інструкціях повинні бути описані дії співробітників при виникненні тієї чи іншої ситуації.

Наприклад, в регламенті можна прописати, що необхідно робити і куди звертатися при спробі третьої особи запросити конфіденційну інформацію або облікові дані співробітників. Такі дії дозволять виявити зловмисника і не допустити витоку інформації.

4) На комп'ютерах співробітників завжди має бути актуальне антивірусне програмне забезпечення. Також необхідно встановити та налаштувати брандмауер під компанію та працівників.
5) У корпоративної мережі компанії необхідно використовувати системи виявлення та запобігання атак.

Також необхідно використовувати системи запобігання витоку конфіденційної інформації, такі як антивірусне ПЗ.

6) Всі співробітники повинні бути проінструктовані, як вести себе з відвідувачами.

Необхідні чіткі правила для встановлення особи відвідувача і його супроводу. Відвідувачів завжди повинен супроводжувати хтось із співробітників компанії. Якщо співробітник зустрічає невідому йому людину, він повинен в коректній формі поцікавитися, з якою метою він чи вона знаходиться в даному приміщенні і де його супровід. При необхідності працівник повинен повідомити про невідому особу в службу безпеки.

7) Необхідно максимально обмежити права користувача в системі.

Наприклад, можна обмежити доступ до web-сайтів і заборонити використання знімних носіїв. Адже, якщо співробітник не зможе потрапити на фішингові сайти або використовувати на комп'ютері флеш-накопичувач з «троянської програмою», то і втратити особисті дані він також не зможе.

Виходячи з усього перерахованого, можна зробити висновок: основний спосіб захисту від соціальної інженерії – це навчання співробітників. Необхідно знати і пам'ятати, що незнання не звільняє від відповідальності. Кожен користувач системи повинен знати про небезпеку розкриття конфіденційної інформації і знати способи, які допоможуть запобігти витоку. Попереджений значить озброєний!

Для пом'якшення цих атак можна дотримуватися наступних вказівок:

- Там, де це можливо, дозволяти багатофакторну автентифікацію, додаючи ще один рівень захисту до будь-яких програм, якими користуються працівники. Крім того, менеджер паролів може допомогти стримати ризиковану поведінку, наприклад, зберігання та обмін паролями.
- Спробуйте скористатися рішенням зашифрованого мережевого підключення VPN (віртуальна приватна мережа). Доступ до IT-ресурсів в організації та в будь-якому місці Інтернету безпечний для працівника.
- Структуру кібербезпеки компаній слід переглянути та включити роботу вдома та віддалено. Коли компанія налаштовується на виведення більшої кількості людей за межі робочого місця, переконайтеся, що стратегія є відповідною. Для доступу працівників до документів та іншої інформації вони повинні забезпечити віддалене управління доступом, використання персональних пристроїв та переглянуті міркування щодо конфіденційності даних.
- Працівники можуть спілкуватися з колегами, використовуючи надане роботодавцем IT-обладнання для офіційних питань. В контексті IT для бізнесу також встановлено різноманітне програмне забезпечення, яке забезпечує безпеку людей. Компанія та працівник не можуть бути повністю захищені, якщо на персональному комп'ютері працівника відбулась атака.

- Персональні пристрої, що використовуються для доступу до робочих мереж, залишать організації вразливими до злому без належного захисту. Якщо інформація просочиться з персонального комп’ютера або зламається, компанія буде нести відповідальність.

У статті представлено декілька необхідних вказівок, яких слід дотримуватись демографічним показникам для подолання атак соціальної інженерії під час COVID-19, як у часи:

- Для фішинг-атак: Сильна автентифікація може захистити користувачів від великої кількості атак особистості, зменшуючи ймовірність порушень безпеки при сильній автентифікації. Для найкращого захисту та зручності користування рекомендуються варіанти автентифікації без пароля. Кращим вибором над SMS [25].
- Для шахрайських дзвінків, пов’язаних із охороною здоров’я: Перевірте всі вхідні дзвінки органу. Не діліться жодною інформацією до тих пір, поки не підтвердите іншу особу. Це по суті, щоб уникнути взаємності. Більшість зловмисників продовжують нападати лише на тих, хто йде їм на зустріч.
- Уникайте попадання цілеспрямованих атак: Як обговорювалося в попередніх розділах, зловмисники збирають інформацію про цілі. Сюди входять як особиста інформація, так і інформація їх близьких членів сім’ї. Це фактично будь-яка інформація. Якщо зроблена підозріла спроба дізнатись інформацією про вашу минулу історію здоров'я або про когось із членів сім'ї, можливо це зловмисники і вони націлились або на вас, або на когось із членів вашої сім;ї
- Атаки на основі історії здоров’я. Якщо будь-яка зловмисна спроба робиться шляхом цитування історії здоров’я та медичних записів цілі або їхньої сім’ї, спроба перевірити ці дані допоможе уникнути даної атаки.

3.2 Скрипт та комлпекс дій для захисту від фішингу

3.2.1 Розпізнавання фішингових електронних листів

Мір для протидії фішингу не так і багато. Звісно існують різні скрипти в електронних скриньках, які блокують спам повідомлення з підозрою на фішинг, але досить часто в ці заблоковані письма попадають і важливі повідомлення. Тому ідеальними такі міри захисту назвати не можна. Самим важливим аспектом для боротьби з фішингом є знання про нього та вміння його розпізнати.

Способи розпізнавання фішингових електронних листів:

1) Негайний призив до дій або загрози – Співробітникам слід ставитись з підозрою до електронних повідомлень, які вимагають негайно перейти по посиланню, зателефонувати або відкрити вкладення. Часто злочинці вимагають негайних дій, спираючись на психологію людини, щоб отримати винагороду або уникнути штрафу. Створення помилкового почуття терміновості – поширений трюк фішингових атак і шахраїв. Вони так роблять, щоб не дати потенційній жертві часу подумати або проконсультуватися з довіреною особою, яка може його застерегти. Тому якщо працівник побачить повідомлення, що закликає до негайних дій, потрібно не поспішати, подумати і уважно прочитати його. Тільки коли людина переконається, що повідомлення справжнє їй можна буде перейти за посиланням. [30]

2) Перші або нечасті відправники. Хоча отримання першого листа від кого-небудь, особливо із-за організації, не буває чимось незвичайним, це також може бути ознакою фішингу. Коли хтось отримує повідомлення від якогось невідомого відправника, слід уважно проглянути дане повідомлення і не поспішати з діями.

3) Граматичні та орфографічні помилки. У професійних компаніях або організаціях, як правило, є редактори, які відповідають за високу якість і професійний характер матеріалів для клієнтів. Якщо повідомлення електронної пошти містить явні орфографічні або граматичні помилки, мова може йти про шахрайство. Іноді ці помилки є результатом невмілого перекладу з іноземної мови, а іноді їх навмисно допускають, щоб обійти фільтри, що блокують такі атаки.

4) Універсальне звернення. Організація, що надає послуги, в повідомленнях електронної пошти звертається до компанії або її представників по імені. Якщо повідомлення починається з універсального звернення, такого як "Добрий день!, Вітаю", і все. Це тривожний знак того, що насправді це можуть бути шахраї.

5) Підозрілі посилання або несподівані вкладення. Якщо працівник вважає, що повідомлення електронної пошти є шахрайським, йому потрібно не відривати посилання чи вкладення, що містяться в ньому. [31] Замість цього навести курсор миші на посилання, але не переходити по ньому, щоб порівняти виплившу адресу з адресою на посиланні, зазначеної в повідомленні. У наступному прикладі при наведенні покажчика миші на посилання справжній веб-адрес відображається в полі з жовтим фоном. Слід звернути увагу якщо рядок з IP-адресою зовсім не схожий на веб-адрес компанії, як на рис 3.1.2.1.

(Рисунок 3.1.2.1) Підозрілий домен.

6) Різні домени електронної пошти. Якщо електронне повідомлення нібито відправлено від імені відомої компанії, такої як Microsoft, тоді як воно відправлено з іншого поштового домену, наприклад Yahoo.com, або microsoftsupport.ru, це може бути шахрай. Також слід звернути увагу на непомітні помилки в правильному доменному імені. Наприклад, micros0ft.com,

де друга буква "o" замінена нулем, або rnicrosoft.com, де "m" замінено на "r" та "n". Це поширені методи шахраїв.

7) Також завжди слід пам’ятати, що у фішингових листах і на фальшивих сайтах зазвичай запитують [32]:

- ім'я користувача та пароль (або пропонують оновити пароль);
- номера особистих документів;
- номер банківського рахунку;
- PIN-код;
- номер кредитної картки;
- дівоче прізвище вашої матері;
- дату вашого народження.

3.2.2 Скрипт для вияву фішингових сайтів

У даному скрипту можна перевірити чи є справжньою URL-адреса, відносно програмі Evilnginx2. Список даних сайтів показано на рис 2.3.2.2. Даннний скрипт має список справжніх URL-адрес сторінок входу та реєстрації популярних сайтів, як на українській (для сайтів, які не мають українського перекладу використовується російська) так і на англійській мові. Цей список порівнюється із введеною користувачем URL-адресою. Якщо введена адреса є у списку, то результатом буде повідомлення “Сайт є оригінальним!”, якщо ж данної адреси у списку немає то результатом буде“ Обережно, підозра на фішинговий сайт!”

Продемонстровано данний скрипт на практиці, який зображено на рис. 3.2.2.1.

```
domen = input("Вставте повну URL-адресу для перевірки на фішинг: ")
domenList = ['https://www.instagram.com/?hl=us', 'https://www.instagram.com/?hl=uk', 'https://www.instagram.com/accounts/emailsignup/?hl=uk',
             'https://www.instagram.com/accounts/emailsignup/?hl=us','https://app.onelogin.com/login',
             'https://office.live.com/start/Outlook.aspx?ui=en%2DUS&rs=US', 'https://office.live.com/start/Outlook.aspx?ui=ru%2DRU&rs=US',
             'https://twitter.com/login', 'https://twitter.com/i/flow/signup', 'https://login.wordpress.org/?locale=en_US', 'https://login.wordpress.org/?locale=uk_uk'
             'https://login.wordpress.org/register', 'https://identity.citrix.com/Utility/STS/Sign-In?ReturnUrl=%2fUtility%2fSTS%2fsaml20%2fpost-binding-response',
             'https://www.citrix.com/welcome/create-account/create-account-form.html', 'https://www.facebook.com/', 'https://www.amazon.com/ap/signin?openid.pape.max_a
             'https://www.amazon.com/ap/signin?openid.pape.max_auth_age=0&openid.return_to=https%3A%2F%2Fwww.amazon.com%2Fyour-account%3F%26ref_%3Dnav_signin&openid.id
             'https://www.linkedin.com/login/us', 'https://www.linkedin.com/login/ru', 'https://www.linkedin.com/signup/cold-join', 'https://www.okta.com/login/',
             'https://www.okta.com/free-trial/', 'https://www.reddit.com/login/', 'https://www.reddit.com', 'https://www.reddit.com/account/register/',
             'https://github.com/login', 'https://github.com/join?source=login', 'https://mail.protonmail.com/login', 'https://protonmail.com/signup',
             'https://protonmail.com/ru/signup']


if domen in domenList:
    print("Сайт є оригінальним!")
else: print ("Обережно, підозра на фішинговий сайт!")
```

(Рисунок 3.2.2.1) Скрипт на перевірку фішингового сайту

При запуску скрипта було введено справжню URL-адресу входу в GitHub (https://github.com/login) при виході було отримано повідомлення, що сайт є оригінальним рис.3.2.2.2.

```
Python 3.8.6 (tags/v3.8.6:db45529, Sep 23 2020, 15:52:53) [MSC v.1927 64 bit (AM
D64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
============== RESTART: D:\univer\Бакалавровська робота\script.py ==============
Вставте повну URL-адресу для перевірки на фішинг: https://github.com/login
Сайт є оригінальним!
>>>
```

Рисунок 3.2.2.2 - Спрацьовування скрипта з позитивним результатом.

Якщо ж ввести невірну URL-адресу входу в GitHub, наприклад (https://githubb.com/login) із подвійною буквою [b] в кінці, то результатом буде попередження, що сайт можливо фішинговий, як на рис 3.2.2.3.

```
============== RESTART: D:\univer\Бакалавровська робота\script.py ==============
Вставте повну URL-адресу для перевірки на фішинг: https://githubb.com/login
Обережно, підозра на фішинговий сайт!
>>>
```

Рисунок 3.2.2.3. - Спрацьовування скрипта з негативним результатом.

ВИСНОВОК

У роботі було проаналізовано зміни в атаках на корпоративні мережі під час пандемії COVID-19. Розглянуте поняття фішинг-атаки та проведено її за допомогою інструменту Evilginx2. Запропоновано портативний скрипт для захисту від фішинг-атак, з урахуванням можливостей Evilginx2.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1.https://support.google.com/websearch/answer/106318?hl=ru

2.https://www.interpol.int/en/News-and-Events/News/2020/Preventing-crime-and-protecting-police-INTERPOL-s-COVID-19-global-threat-assessment

3.https://www.commissariatodips.it/da-sapere/per-i-cittadini-ei-ragazzi/internet-rischi-e-minacce/index.html

4. https://www.sviaz-expo.ru/ru/ui/17166/

5.https://itbox.pro/services/telekommunikatsionnye-resheniya/korporativnye-seti-peredachi-dannykh-wan/

6. https://www.vmware.com/ru/topics/glossary/content/enterprise-networking.html

7.https://studbooks.net/2339183/tehnika/funktsii_harakteristiki_tipovaya_struktura_korporativnyh_kompyuternyh_setey

8. https://searchnetworking.techtarget.com/definition/local-area-network-LAN

9.https://www.cisco.com/c/en/us/products/switches/what-is-a-lan-local-area-network.html

10.https://www.sviaz-expo.ru/ru/articles/globalnye-seti/=

11.http://infocell.ru/solutions/networking/corporate_networks/

12.https://www.vmware.com/ru/topics/glossary/content/enterprisenetworking.html

13.https://www.interpol.int/en/News-and-Events/News/2020/Preventing-crime-and-protecting-police-INTERPOL-s-COVID-19-global-threat-assessment

14.https://www.opsecsecurity.com/resource/whitepaper/consumer-barometer-report-2020

15.https://www.itpro.co.uk/security/phishing/356379/microsoft-secretly-taking-control-of-covid-19-phishing-domains

16.https://www.imperva.com/learn/application-security/social-engineering-attack/#:~:text=Social%20engineering%20is%20the%20term,in%20one%20or%20more%20steps.

17.https://www.webroot.com/us/en/resources/tips-articles/what-is-social-engineering

18.https://doi.org/10.1504/IJEBR.2018.095343

19. Хасан Чизарі, Ахмад Зулкурнайн, Ахмад Хаміді, Аффанді Хусайн. Пом'якшення нападів соціальної інженерії. 2015; 188–198ст.

20.https://blog.google/threat-analysis-group/findings-covid-19-and-online-security-threats/

21.https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond

22.https://www.microsoft.com/uk-ua/security/business/security-intelligence-report

23.https://oacta.memberclicks.net/assets/docs/COVID-19%20Privacy%20Alert%20-%20FBI%20Alert%20Social%20Engineering%20Cyber%20Attacks.pdf

24.https://z3x0k1mf9pv4dfy4d3m15mq1-wpengine.netdna-ssl.com/wp-content/uploads/2020/05/Social-engineering-attacks-and-COVID-19.pdf

25. https://us-cert.cisa.gov/ncas/alerts/aa20-099a

26.https://kali.tools/?p=4761#:~:text=%D0%9E%D0%BF%D0%B8%D1%81%D0%B0%D0%BD%D0%B8%D0%B5%20evilginx2,%D0%BF%D0%BE%D0%B7%D0%B2%D0%BE%D0%BB%D1%8F%D1%8E%D1%82%20%D0%BE%D0%B1%D0%BE%D0%B9%D1%82%D0%B8%20%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D1%83%20%D0%B4%D0%B2%D1%83%D1%85%D1%84%D0%B0%D0%BA%D1%82%D0%BE%D1%80%D0%BD%D0%BE%D0%B9%20%D0%B0%D1%83%D1%82%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D0%B5%D0%B9

27.https://xakep.ru/2019/10/28/evilginx-phishing/

28.https://github.com/kgretzky/evilginx2

29.https://kali.tools/?p=4761

30.https://efsol.ru/articles/social-engineering.html

31.https://support.google.com/mail/answer/8253?hl=ru#zippy=%2C%D0%BA%D0%B0%D0%BA-%D1%81%D0%BE%D0%BE%D0%B1%D1%89%D0%B8%D1%82%D1%8C-%D0%BE-%D1%84%D0%B8%D1%88%D0%B8%D0%BD%D0%B3%D0%B5

32.https://www.smart-soft.ru/blog/sozdanie_korporativnoj_seti/