КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (23), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.23.338347
УДК 004.056.5

Крючкова Лариса Петрівна
д.т.н., професор, професор кафедри інформаційної та
кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID 0000-0002-8509-6659
l.kriuchkova@kubg.edu.ua

Стеблина Олександр Станіславович
студент
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID 0009-0002-0132-0885
ossteblyna.fitu20@kubg.edu.ua

ЗАХИСТ СМАРТФОНІВ ВІД ВПЛИВУ ШКІДЛИВИХ ПРОГРАМ В ПРОЦЕСІ ЗАРЯДКИ У ГРОМАДСЬКИХ МІСЦЯХ

Анотація. Оскільки смартфони стають незамінними інструментами для зв'язку, роботи та розваг, ризики, обумовлені їх частим заряджанням у громадських місцях, таких як кафе, коворкінги та станції оренди павербанків, значно зросли. Мета публікації — аналіз зростаючих загроз у сфері кібербезпеки мобільних пристроїв, зокрема, вразливостей, пов'язаних із громадськими зарядними станціями та пристроями для передачі даних через USB. Розглядаються різні кіберзагрози, включно з *Juice Jacking*, атаками *BadUSB*, компрометацією орендованих павербанків та оманливою безпечністю використання громадських USB-портів, які можуть бути налаштовані для розгортання шкідливих програм або проведення несанкціонованого доступу до даних. Детально описано різні вектори атак і запропоновано практичні заходи для зменшення цих ризиків. Серед рекомендацій — використання особистих зарядних пристроїв, використання USB-кабелів або пристроїв, які блокують передачу даних (*USB-condoms*), та важливість регулярних оновлень програмного забезпечення для захисту від відомих вразливостей. Новим рішенням, яке пропонується, є розробка брелока USB-C до USB-C із роз'єднаними контактами передачі даних, який забезпечує заряджання без ризиків передачі даних, і запобіжником, що може надати додатковий захист від перепадів напруги та прямих атак на обладнання, таких як *BadPower*. Брелок-блокувальник розроблено таким чином, щоб його було легко носити з собою, прикріплювати до брелоків або безпосередньо до чохлів смартфонів, що забезпечує його доступність без ризику його забути. Стаття наводить аргументи на користь підвищення обізнаності та превентивних практик як невід'ємних компонентів забезпечення кібербезпеки в епоху, коли мобільні пристрої повсюдно використовуються та постійно піддаються зростаючим загрозам. Результати дослідження підкреслюють неминучість складних кібератак на тлі глобальної напруженості та технологічного прогресу, виступаючи за проактивні заходи для захисту особистих і конфіденційних даних. Постійне оновлення програмного забезпечення та використання апаратних рішень, призначених для забезпечення безпеки мобільних пристроїв, дозволяє ефективно захистити користувачів від більшості кіберзагроз.

Ключові слова: Juice Jacking; кібербезпека; безпека USB; мобільна безпека; кіберзагрози; превентивні заходи.

ВСТУП

Смартфони давно стали незамінними в нашому повсякденному житті, сприяючи зв'язку, організації дня, роботі та розвагам, навіть коли ми перебуваємо у русі. Їх інтенсивне використання постійно призводить до швидкого розрядження батарей, змушуючи користувачів шукати місця для підзарядки поза домівки. У сучасних умовах

війни та перебоїв з електрикою ця проблема набуває нового значення. Часті відключення електроенергії змушують людей заряджати свої пристрої у громадських місцях або Пунктах Незламності, що створює небачені раніше можливості для ворожих агентів та хакерів проводити складні кібератаки.

За будь-якою кіберзлочинною діяльністю завжди є або фінансова, або ідейна складова. У 2010-х роках *NSA* (англ. *National Security Agency*) США заговорило про атаки на смартфони через USB-порти та, так званий, *Juice Jacking* [1], однак жодна хакерська команда в світі ще не мала ні мотивації, ні можливостей правильно проводити такі атаки, тому ці види загроз ігнорувалися до сьогоднішнього дня.

Тепер світ змінився: в кожного з нас на смартфоні є хоча б один банківський чи криптовалютний додаток, ми оточені дешевими «розумними» приладами IoT без належного захисту, що керуються зі смартфону, а за вікном йде найбільша війна з часів Другої світової, в якій майже кожен з нас є потенціальною живою мішенню для атак російських хакерів. Тепер в багатьох хакерських команд є і мотивація, і можливості проводити атаки, від яких наше суспільство ще не навчилось захищатись. Саме на це може вказувати зростання на 52% з 2018 по 2022 роки кількості вірусів, що використовують для поширення USB [2]. На актуаьність цієї загрози також вказує те, що у 2023 році *FFC* (англ. *Federal Communications Commission*) знову застерегла жителів США про загрозу *Juice Jacking* [3].

Мета публікації — аналіз зростаючих загроз у сфері кібербезпеки мобільних пристроїв, зокрема, вразливостей, пов’язаних із громадськими зарядними станціями та пристроями для передачі даних через USB.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Види атак

Атаки через зарядні пристрої. Пентестер під псевдонімом MG продемонстрував, як модифікований зарядний пристрій може використовуватися для встановлення шкідливого програмного забезпечення (ПЗ) в комп’ютери та смартфони [4]. Ця техніка дозволяє хакерам скомпрометувати пристрої через порт USB-C.

Ще одна відома атака **через зарядні пристрої** — *BadPower*, що використовує модифікацію прошивки швидкозарядних пристроїв. Зловмисники змінюють налаштування прошивки, змушуючи зарядний пристрій забезпечувати вищу потужність, ніж дозволено, що призводить до перегріву та знищення пристроїв. В ході дослідження *Tencent* було виявлено, що з понад 200 протестованих зарядних пристроїв, 35 мали вразливості, а 18 були повністю вразливими до *BadPower* [5]. За результатами дослідження, опублікованими в Китайській національній базі даних вразливостей, виявлені проблеми можуть бути вирішені шляхом оновлення прошивки. Це підкреслює необхідність заходів електричного захисту в зарядних пристроях для запобігання майбутнім атакам.

Атаки через *BadUSB* кабелі. В еру цифрових технологій, кіберзагрози стають все більш підступними, зокрема через такі пристрої як *BadUSB* кабелі. Один з яскравих прикладів — *O.MG Cable*, також відомий як «*Offensive MG cable*». Цей кабель на перший погляд не відрізняється від звичайних зарядних кабелів, однак є потужним інструментом для здійснення кібератак [6].

Розроблений вже згаданим вище експертом з кібербезпеки, відомим під псевдонімом *MG, O.MG Cable* був представлений на конференції *Def Con*. Він оснащений мікроконтролером, що дозволяє йому виконувати широкий спектр завдань

від перехоплення клавіатурних введень до встановлення зв'язку з віддаленим сервером для передачі даних, виконання шкідливого програмного забезпечення на цільовому пристрої чи інших задач атак типу *evil maid attack*.

Зловмисник може замінити звичайний зарядний кабель на *O.MG Cable*, і коли жертва використовуватиме цей кабель для зарядки, провести атаку. Це особливо зручно в таких місцях як коворкінги, кафе тощо, де люди часто заряджають свої пристрої під час блекаутів і де можуть бути кабелі загального користування.

Атака через USB-порти на мережевих фільтрах. Мережеві фільтри з USB-портами часто використовуються для одночасного заряджання різних пристроїв, що зробило їх популярним рішенням в Пунктах Незламності та інших громадських місцях. Незважаючи на зручність, вони вносять кілька ризиків, про які користувачі повинні знати.

Перш за все слід зазначити, що не всі мережеві фільтри забезпечують однаковий рівень захисту. Деякі моделі можуть не гарантувати стабільний рівень напруги, що може призвести до перегріву або навіть загоряння смартфона через некоректну роботу мережевого фільтра. Також більшість USB-портів на мережевих фільтрах не підтримують швидку зарядку. Використання цих портів при заряджанні таких смартфонів може викликати, так званий, *undercharging*, що з часом зменшує ємність батареї та скорочує термін служби акумулятора. А ще ці порти можуть бути легко модифіковані для здійснення кібератак, по аналогії з вищезазначеними модифікаціями зарядних пристроїв. Модифіковані мережеві фільтри навряд чи викличуть підозру у звичайної людини, тому можуть бути легко передані в найближчі до критичної інфраструктури Пункти Незламності російськими агентами під виглядом волонтерів.

В контексті поточної військової ситуації, це не може не викликати занепокоєння, оскільки існує потенційна можливість використання таких атак росіянами для вилучення чутливої інформації або завдання шкоди критичним підприємствам.

Атака з допомогою портативних електростанцій. Під час тривалих відключень електроенергії в Україні, спричинених військовими діями, портативні електростанції такі, як *EcoFlow* та *Bluetti* стали не лише незамінними помічниками для громадян та військових, а й потенційними цілями для кібератак.

Оскільки це не просто літієві акумулятори з інверторами, а повноцінні IoT пристрої, вони можуть і мають отримувати оновлення програмного забезпечення через *Internet*, що теоретично дозволяє зловмисникам втручатися у прошивку цих пристроїв, наприклад з допомогою *supply chain attack*. Особливо це стає реальною загрозою з огляду на минулі інциденти атак на IoT, наприклад, такі як атака бот-мережі *Mirai* [7], яка показала можливості масштабних кібератак через уразливості IoT пристроїв.

Враховуючи, що за різними оцінками *EcoFlow* та *Bluetti* займають до 60% відсотків на ринку, а їх висока ціна дозволяє купувати їх тільки відносно забезпеченим людям, зловмисники можуть використовувати вразливості у програмному забезпеченні цих станцій для виконання «*zero-click*» атак, що не потребують активних дій від користувача. Наприклад, вони можуть встановлювати шкідливі оновлення, що містять бекдори для вибіркових атак на пристрої користувачів під час заряджання від USB портів на цих станціях з ціллю вкрасти цінні дані, або гроші, наприклад, з крипто гаманців. До того ж ці станції часто використовуються у Пунктах Незламності, що піддає ризикам і звичайних користувачів.

Атаки через оренду павербанків. Останніми роками оренда павербанків набула популярності як практичне рішення для заряджання мобільного пристроїв в умовах зростаючої залежності від мобільних технологій. Пункти прокату часто розміщені в зручних

місцях, таких як магазини, кафе тощо, забезпечуючи доступність та зручність користування, особливо для тих, хто часто потребує швидкої підзарядки по дорозі на роботу чи навчання.

Однак, популярність цих послуг може стати потенційною мішенню для кібератак, особливо у випадку, коли хакери можуть використовувати компрометовані павербанки для встановлення шкідливого ПЗ або вилучення даних з підключених пристроїв. Це створює особливі ризики для силових структур та працівників критичної інфраструктури, які можуть вимушено користуватися цими послугами під час аварійних відключень електроенергії.

Наприклад, один з простих способів реалізувати таку загрозу — відкрити декілька кав'ярень поряд з силовими структурами або критичною інфраструктурою. Достатньо лише встановити в них скомпрометовані станції з павербанками і зробити каву дешевшою, ніж в інших кав'ярнях поряд. Залишиться тільки чекати, доки співробітники відомств чи інфраструктури скористаються орендою павербанків.

Щодо векторів кібератак, російські хакери, наприклад, можуть використовувати такі сценарії:

- Підроблення павербанків: Російські хакери можуть розмістити модифіковані павербанки в пунктах прокату, які вмістять шкідливе ПЗ або апаратні бекдори. В російських компаній можна офіційно купити ПЗ для злому смартфонів, яке потребує підключення по USB [8]. Тому в росіян точно є технології, щоб зробити *zero-click* взлом смартфонів при наявності з'єднання по USB.
- Скомпрометоване програмне забезпечення: Через мобільні додатки, які використовуються для управління процесом оренди, можуть бути розповсюджені шкідливі програми, спрямовані на компрометацію даних користувача. Вразливості, що працюватимуть таким чином, значно легше знайти або купити, ніж *zero-click* вразливості.
- Зараження через QR-коди: Компрометація QR-кодів, які використовуються для авторизації доступу до павербанків, може дозволити зловмисникам перехоплювати дані користувачів. Деякі приклади атак через QR-коди, що вже відбувались, подано в [9].

Звичайний *Juice Jacking*. Це тип кібератаки, в якому публічні зарядні USB-порти використовуються для компрометації пристроїв користувачів [10]. Цей метод використовує функціонал USB-портів, які можуть передавати не лише електрику, а й дані, для встановлення шкідливого програмного забезпечення чи здійснення крадіжки даних. Такі атаки можуть відбуватися наступним чином:

1. Зловмисники можуть інтегрувати шкідливе обладнання в публічні USB-зарядні порти, які після підключення до пристрою користувача можуть ініціювати встановлення шкідливого ПЗ або крадіжку даних.
2. При підключенні пристрою до скомпрометованого порту, шкідливе обладнання визначає з'єднання і починає атаку, якщо на пристрій користувача можна передавати данні.
3. Шкідливе програмне забезпечення може встановлюватися, залишаючись непомітним на тривалий час, що ускладнюватиме виявлення джерела атаки.
4. В деяких випадках шкідливе ПЗ може надавати зловмисникам віддалений доступ до пристрою, дозволяючи викрадати дані чи використовувати пристрій для інших злочинних дій.

Зазвичай люди не звертають увагу на фахівців, які виконують певні роботи, тому зловмисники можуть непомітно модифікувати публічні USB порти.

Види захисту

Блокування передачі даних як захист від кіберзагроз. Програмне блокування передачі даних через USB є відносно ефективним способом захисту від кіберзагроз, на кшталт *Juice Jacking*. Достатньо просто відкрити налаштування і обрати опцію «тільки заряджання» серед сценаріїв підключення по USB. Проте, як показує практика, таке рішення навряд захистить від *zero-day* експлойтів, які використовують компанії, що спеціалізуються на розблокуванні смартфонів. Тим не менш, це все одно важливо зробити тим, хто регулярно заряджається в коворкінгах, кафе чи інших громадських місцях, де є ризик описаних вище кібератак.

Своєчасне встановлення всіх оновлень. Одним з найважливіших аспектів кібербезпеки є своєчасне встановлення оновлень програмного забезпечення. Це включає оновлення операційних систем, застосунків та прошивок на всіх пристроях, від смартфонів до персональних комп'ютерів та інтелектуальних пристроїв. Виробники часто випускають патчі та оновлення для виправлення вразливостей, які можуть бути використані кіберзлочинцями для проникнення в системи. Ігнорування цих оновлень може коштувати вам конфеденційних данних чи власних збережень.

Використання своїх власних зарядних кабелів. Використання власних зарядних кабелів може бути відносно дієвим способом захисту від описаних вище атак. Треба обирати кабелі саме без можливості передачі даних. Проблема в тому, що зараз такі кабелі знайти значно важче, ніж звичайні *data transfer* кабелі, але такі кабелі знижують ризики, пов'язані з використанням USB портів, які можуть бути скомпрометовані зловмисниками, майже до нуля. Зауважте, що виробники кабелів теж можуть брехати. Коли на кабелі написано, що він не передає дані, це ще не означає, що він справді їх не передає.

Використання власних блоків живлення. Використання особистих блоків живлення та зарядних пристроїв є одним з відносно ефективних способів забезпечення кібербезпеки в умовах зростаючої загрози атак через публічні зарядні станції. Приносячи власні зарядні блоки, користувачі можуть уникнути ризиків, пов'язаних із зарядними USB-портами, що можуть заразити смартфон шкідливим програмним забезпеченням або містити апаратні бекдори, розроблені для крадіжки даних або встановлення вірусів. Особисті якісні зарядні пристрої також дозволяють уникнути нестабільності живлення, яка може виникнути внаслідок використання пошкоджених або несертифікованих публічних зарядних станцій, забезпечуючи більш безпечне та надійне заряджання пристроїв. Однак від атак через скомпрометований кабель вони захистити не здатні.

Використання старих кнопкових телефонів. Старі кнопкові телефони можуть стати бюджетним або навіть безкоштовним способом захиститися від описаних вище кібер-атак. Якщо ви хочете просто підтримувати зв'язок з рідними, то ці телефони прекрасно підійдуть для дзвінків та SMS, а також, за замовчуванням, вони стійкіші до шкідливого програмного забезпечення, оскільки не підтримують складні програмні додатки та високоінтегровані веб-сервіси. До атак по USB вони мають абсолютну стійкість, бо їх порти для заряджання можуть тільки отримувати напругу і апаратно не здатні передавати дані. Але варто уникати покупки сучасних кнопкових телефонів, бо більшість з них вже працюють на *Android OS* і відрізняються від смартфонів тільки форм-фактором. Рекомендується зупинити свій вибір на рішенні з *Symbian OS, Palm OS* чи *BlackBerry OS*, в силу їх непопулярності в сучасному світі.

Невикористання сервісів оренди павербанків. Важливим аспектом кіберзахисту є уникнення використання орендованих павербанків, особливо в місцях загального користування. Хоча це здається зручним рішенням для миттєвої зарядки мобільних пристроїв, існує щонайменше 3 потенційні вектори атаки через ці пристрої, що описані

вище. Замість використання павербанків в оренді, краще використовувати власні зарядні пристрої. Це значно зменшує ризик ненавмисного інсталювання шкідливих програм або доступу зловмисників до особистої інформації.

Використання особистих павербанків для заряджання. Зарядка і використання особистих павербанків забезпечує контроль над безпекою заряджання мобільних пристроїв і мінімізує ризики, пов'язані з публічними зарядними станціями, оскільки павербанки не підлягають злому. Навіть, якщо USB порт скомпрометовано, навряд чи зарядка павербанка від нього здатна хоч якось в подальшому зашкодити користувачу при його використанні. Таким чином, павербанк стає надійним рішенням для безпечного та зручного заряджання в публічних місцях, забезпечуючи спокій і захист даних. До недоліків можна віднести його вагу і довгий час на його заряджання, що потребує додаткового планування розходу заряду своїх пристроїв. Якщо ж недозаряджати павербанк при використанні, з часом це негативно вплине на його якості.

Зарядка автомобільних акумуляторів для використання їх в ролі зарядних станцій. Зарядка автомобільних акумуляторів для використання їх як зарядних станцій стала популярною практикою в умовах блекаутів минулого року. Автомобільні акумулятори, які зазвичай використовуються для запуску двигуна, можуть бути адаптовані для підтримки основних енергетичних потреб у домогосподарствах та заряджання мобільних пристроїв у критичний момент. Це може бути здійснено за допомогою інверторів, які перетворюють постійний струм від акумулятора в змінний, дозволяючи підключення побутових приладів. Цей метод може бути особливо корисним в регіонах, що стикаються з частими відключеннями електроенергії і, головне, він повністю імунний до будь-яких кібер-атак через свою технічну простоту. Але автомобільні акумулятори важкі, довго заряджаються і можуть виділяти токсичні речовини при використанні в закритих приміщеннях.

Використання блокувальників USB to USB. З часом технологія блокувальників USB to USB, відомих також як *USB-condoms*, стала застарілою через впровадження нових стандартів для кабелів смартфонів, а саме переходу виробників на USB-C. Ці пристрої дозволяли лише заряджання пристрою без ризику несанкціонованого доступу або передачі даних. До того ж, у випадку атаки через скомпрометований кабель, вони і раніше ніяк не могли захистити пристрій користувача, тому що основні порти смартфонів тоді були Micro USB та Lightning і блокувальник даних USB to USB фізично ніяк не міг допомогти. Тим не менш, від деяких видів атак вони здатні захистити на сто відсотків.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Останнім часом забезпечення інформаційної безпеки смартфонів широко обговорюється в публікаціях [11], [12]. Зарядні станції та USB-порти загального користування, як і павербанки, що пропонуються через сервіси оренди, становлять значні ризики для крадіжки даних та поширення шкідливого програмного забезпечення. Пристрої, підключені до скомпрометованих станцій чи портів або через скомпрометовані кабелі, можуть мимоволі стати жертвами кібератак, крадіжки даних або встановлення шкідливого програмного забезпечення.

Підкреслено важливість регулярного встановлення оновлень та використання пристроїв, призначених для блокування несанкціонованої передачі даних. Постійне оновлення програмного забезпечення та використання апаратних рішень, призначених

для забезпечення безпеки, дозволяє ефективно захистити користувачів від більшості кіберзагроз, пов'язаних з мобільними пристроями.

Враховуючи динамічний характер розвитку кіберзагроз і постійний розвиток технологій, у звіті прогнозується збільшення кількості складних кібератак, особливо у сценаріях, пов'язаних з мобільними пристроями. Отримані дані свідчать про нагальну потребу в широкому впровадженні обговорюваних захисних заходів для зменшення ризиків, пов'язаних з використанням мобільних пристроїв.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Застосування брелоку-блокувальника **USB-C to USB-C з роз'єднаними контактами передачі даних забезпечує найоптимальніший захист з огляду на** всі сильні сторони і недоліки інших методів захисту. Оскільки головний і чи не єдиний недолік цього виду захисту тільки в тому, що його неможливо встановити між зарядним кабелем та смартфоном, оновлення його до сучасного стандарту USB-C повністю вирішить цю проблему.

Додавання в конструкцію плавкого запобіжника забезпечує захист від атак типу *BadPower*. В такій конфігурації даний виріб може захистити смартфон користувача від всіх відомих на сьогоднішній день загроз в процесі заряджання. Форм-фактор даного вибору зумовлено тим, що звичайний блокувальник USB легко забути і не взяти з собою. Брелок-блокувальник можна підчепити до ключів, без яких користувач навряд чи опиниться на вулиці, чи навіть безпосередньо до чохла смартфону, якщо дозволяє його конструкція. У випадку ж, якщо користувачу все ж таки доведеться скористатися передачею даних по USB, такий виріб не принесе йому зайвого дискомфорту. До того ж в такому форматі його можна без проблем використовувати для заряджання ноутбуків, що заряджаються через USB-C, що збільшить потенційну цільову аудиторію цього виробу.

Перспективи подальших досліджень атак на смартфони під час заряджання і захисту від них важко переоцінити. Хоча на *Juice Jacking* зараз звертають мало уваги, все зміниться з першою гучною атакою. Розквіт цього виду атак ще попереду, і, враховуючи складну та дуже напружену ситуацію в світі, схоже, нам не доведеться довго чекати. Саме тоді ця публікація стане кожному в нагоді.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Security Configuration Recommendations for Apple R iOS 5 Devices 2012.* (n.d.).
2. Honeywell International Inc. Industrial cybersecurity USB threat report 2022. (n.d.). *Software for Digital Transformation|Honeywell Forge.* https://www.honeywellforge.ai/us/en/campaigns/industrial-cybersecurity-threat-report-2022#form
3. Lee, B. D. (2018). *This rigged charger can hijack your new laptop.* BBC Home - Breaking News, World News, US News, Sports, Business, Innovation, Climate, Culture, Travel, Video & Audio. https://www.bbc.com/news/technology-45139397
4. *What is 'Juice Jacking' and Tips to Avoid It.* (2023). Federal Communications Commission. https://www.fcc.gov/juice-jacking-tips-to-avoid-it
5. *Safety Tips: Some Fast Charging Products Have "Bad Power" Risks. (*2020). Tencent Security Xuanwu Lab. https://xlab.tencent.com/cn/2020/07/16/badpower/
6. Faife, C. (2022). *The O.MG Elite cable is a scarily stealthy hacker tool.* The Verge. https://www.theverge.com/23321517/omg-elite-cable-hacker-tool-review-defcon
7. Buxton, O. (2022). *What Is the Mirai Botnet?* What Is the Mirai Botnet? https://www.avast.com/c-mirai

8. *Elcomsoft Phone Breaker | Elcomsoft Co.Ltd.* (n.d.). Digital Forensic, Data Decryption and Password Recovery Solutions for Law Enforcement, Forensic and Corporate Customers | Elcomsoft Co.Ltd. https://www.elcomsoft.com/eppb.html
9. Keepnet Labs. (2024). *5 Examples of Real-World QR Code Attacks*. LinkedIn: Log in or Sign Up. https://www.linkedin.com/pulse/5-examples-real-world-qr-code-attacks-keepnetlabs-a7vee/
10. *FBI Denver.* (2023). X (Twitter). https://twitter.com/FBIDenver/status/1643947117650538498/photo/1
11. Sadykov, Y., et al. (2021). Technology of Location Hiding by Spoofing the Mobile Operator IP Address, *IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics*, 22–25. https://doi.org/10.1109/UkrMiCo52950.2021.9716700
12. Shcheblanin, Y., et al. (2023). Research of Authentication Methods in Mobile Applications. In *Cybersecurity Providing in Information and Telecommunication Systems, Vol. 3421*, 266–271.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (23), 2024
ISSN 2663 - 4023

Larysa Kriuchkova
Doctor of sciences, professor, professor of Volodymyr Buriachok Department of Information and Cybersecurity
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID 0000-0002-8509-6659
l.kriuchkova@kubg.edu.ua

Oleksandr Steblyna
student
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID 0009-0002-0132-0885
ossteblyna.fitu20@kubg.edu.ua

PROTECTION OF SMARTPHONES FROM THE INFLUENCE OF HARMFUL PROGRAMS DURING CHARGING IN PUBLIC PLACES

Abstract. As smartphones become indispensable tools for communication, work, and entertainment, the risks associated with their frequent charging in public places such as cafes, coworking spaces, and power bank rental stations have significantly increased. This publication aims to analyze the growing cybersecurity threats to mobile devices, particularly the vulnerabilities linked to public charging stations and USB data transfer devices. Various cyber threats are examined, including Juice Jacking, BadUSB attacks, rental power bank compromises, and the deceptive safety of public USB ports, which may be configured to deploy malware or conduct unauthorized data access. Detailed descriptions of various attack vectors are provided, along with practical measures to mitigate these risks. Recommendations include using personal chargers, employing USB cables or devices that block data transfer (USB condoms), and the importance of regular software updates to protect against known vulnerabilities. A novel solution proposed is the development of a USB-C to USB-C keychain with disconnected data transfer contacts, ensuring charging without data transfer risks, and a fuse that can provide additional protection against voltage spikes and direct hardware attacks such as BadPower. The keychain blocker is designed for easy portability, attaching to key rings or directly to smartphone cases, ensuring availability when needed without the risk of being forgotten. The article argues for increased awareness and preventive practices as integral components of cybersecurity in an era when mobile devices are widely used and continuously exposed to growing threats. The research results highlight the inevitability of complex cyberattacks amid global tensions and technological advancements, advocating for proactive measures to protect personal and confidential data. Continuous software updates and the use of hardware solutions designed to secure mobile devices effectively protect users from most cyber threats.

Keywords: Juice Jacking; cybersecurity; USB security; mobile security; cyber threats; preventive measures.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. *Security Configuration Recommendations for Apple R iOS 5 Devices 2012.* (n.d.).
2. Honeywell International Inc. Industrial cybersecurity USB threat report 2022. (n.d.). *Software for Digital Transformation|Honeywell Forge*. https://www.honeywellforge.ai/us/en/campaigns/industrial-cybersecurity-threat-report-2022#form
3. Lee, B. D. (2018). *This rigged charger can hijack your new laptop.* BBC Home - Breaking News, World News, US News, Sports, Business, Innovation, Climate, Culture, Travel, Video & Audio. https://www.bbc.com/news/technology-45139397
4. *What is 'Juice Jacking' and Tips to Avoid It.* (2023). Federal Communications Commission. https://www.fcc.gov/juice-jacking-tips-to-avoid-it
5. *Safety Tips: Some Fast Charging Products Have "Bad Power" Risks. (*2020). Tencent Security Xuanwu Lab. https://xlab.tencent.com/cn/2020/07/16/badpower/

6. Faife, C. (2022). *The O.MG Elite cable is a scarily stealthy hacker tool*. The Verge. https://www.theverge.com/23321517/omg-elite-cable-hacker-tool-review-defcon
7. Buxton, O. (2022). *What Is the Mirai Botnet?* What Is the Mirai Botnet? https://www.avast.com/c-mirai
8. *Elcomsoft Phone Breaker | Elcomsoft Co.Ltd.* (n.d.). Digital Forensic, Data Decryption and Password Recovery Solutions for Law Enforcement, Forensic and Corporate Customers | Elcomsoft Co.Ltd. https://www.elcomsoft.com/eppb.html
9. Keepnet Labs. (2024). *5 Examples of Real-World QR Code Attacks*. LinkedIn: Log in or Sign Up. https://www.linkedin.com/pulse/5-examples-real-world-qr-code-attacks-keepnetlabs-a7vee/
10. *FBI Denver.* (2023). X (Twitter). https://twitter.com/FBIDenver/status/1643947117650538498/photo/1
11. Sadykov, Y., et al. (2021). Technology of Location Hiding by Spoofing the Mobile Operator IP Address, *IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics*, 22–25. https://doi.org/10.1109/UkrMiCo52950.2021.9716700
12. Shcheblanin, Y., et al. (2023). Research of Authentication Methods in Mobile Applications. In *Cybersecurity Providing in Information and Telecommunication Systems*, *Vol. 3421*, 266–271.