2012-%D0%BF#Text.

8. Про затвердження Положення про Експертну службу Міністерства внутрішніх справ України. Наказ МВС України № 691 від 09.08.2012 року. Зареєстровано в Міністерстві юстиції України 7 вересня 2012 р. за № 1541/21853. URL: https://zakon.rada.gov.ua/laws/show/z1541-12#Text.

9. Про затвердження Положення про Експертну службу Міністерства внутрішніх справ України. Наказ МВС України № 1343 від 03.11.2015 року. Зареєстровано у Міністерстві юстиції України 06 листопада 2015 р.за № 1390/27835 URL: https://zakon.rada.gov.ua/laws/show/z1390-15#Text.

10. Про державну реєстрацію геномної інформації людини: Закон України від 09.07.2022 року, № 2391-IX URL: https://zakon.rada.gov.ua/laws/show/2391-20#n207.

11. Про затвердження Положення про Електронний реєстр геномної інформації людини: Наказ МВС України № 639 від 04.08.2023 року, зареєстровано в Міністерстві юстиції України 20 вересня 2023 р. за № 1657/40713 URL: https://zakon.rada.gov.ua/laws/show/z1657-23#Text.

12. Горбонос, В. (2021). Класифікація нормативно-правових актів, які регулюють діяльність Експертної служби МВС України. Знання європейського права. 73-78. 10.32837/chern.v0i3.102.

Олександр КОСИЧЕНКО,
доцент кафедри інформаційних технологій
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

СМАРТФОН ЯК ДЖЕРЕЛО РИЗИКІВ КІБЕРБЕЗПЕКИ

Сучасний смартфон – це повноцінний маленький комп’ютер, який, на відміну від настільного комп’ютера або ноутбука, має постійний доступ в Інтернет і тому несе в собі великі ризики: як звичайні комп’ютерні (віруси, не документовані можливості, закладки, стеження), так і інформаційні (вплив на свідомість свого власника, нав’язливий контент, залучення до небезпечних груп у соцмережах). Під впливом на свідомість ми розуміємо насамперед те, що смартфон – платформа для завантаження адиктивного (від англ. addiction – схильність, згубна звичка) контенту, що несе цілий букет ризиків та залежностей: ігри, відеоролики, порнографія, пропаганда тощо.

Основні властивості смартфону, що породжують ці ризики, такі:

– платформа для доставки нав’язливої реклами;

– джерело неконтрольованих повідомлень, пропозицій, приманок, розводок та інших впливів на користувача;

– платформа для встановлення небажаного та непроханого програмного забезпечення: вірусів, троянських програм, шпигунів, рекламних закладок тощо;

– канал витоку персональних даних власника: фотографій, особистих даних, адреси, відомостей про переміщення, номерів кредиток та інше.

Чим інтенсивніше використовується пристрій, тим більше даних про свого власника воно накопичує. Дані бувають прямими – фотографії, контакти, повідомлення, які власник сам повідомив пристрою та Інтернету. Є й опосередковані дані, які обчислюються самим пристроєм з урахуванням дій власника. До них відносяться, наприклад: історія встановлення та використання додатків; історія повідомлень та дій; історія магазину додатків; історія браузера, його кеш (переглянуті нещодавно сторінки); історія переміщень та багато іншого. Дані збирають практично усі виробники пристроїв (наприклад, Apple, Samsung, Xiaomi та інші), платформа операційної системи (iOS або Android), а також легальні та нелегальні (шкідливі) програми. Багато програм при установці вимагають дати їм дозвіл на доступ до вашої телефонної книги, файлів, фотографій і т. д. Безкоштовному додатку вони потрібні для заробітку шляхом отримання та перепродажу ваших персональних даних. У більшості шкідливих програм на смартфоні та ноутбуці – економічні цілі, тобто їм потрібно якось отримати або вкрасти гроші користувача або нажитися на ньому іншими способами. Основні джерела доходу таких додатків такі. Насамперед, це продаж уваги, яка продається найдорожче і яким оплачується доступ практично до будь-яких сервісів. Монетизація уваги може бути різною – показ реклами, створення штучних незручностей, за зняття яких необхідно заплатити, участь у спільному створенні контенту (лайки та перегляди). Кількість контактів з користувачем, щільність утримання його уваги впливають на дохідність будь-якого подібного сервісу. Таким чином, найбільш прибутковим бізнесом є продаж доступу до уваги користувача шляхом показу йому реклами та іншого контенту в браузері та інших додатках.

Далі слідує продаж профілю користувача. Профіль – це сукупність даних про користувача: історія перегляду сайтів, історія використання програм, список контактів, історія геолокацій пристрою, списки бездротових мереж і Bluetooth-пристроїв, записи звукового оточення, параметри середовища (версія ОС, мобільний оператор, характеристики пристрою, що використовується) і т.п. д. Зазвичай ці дані продаються знеособленими: сама собою особистість користувача для рекламодавців не дуже цікава, при тому, що його персональні дані можуть бути чутливими (і стати джерелом юридичних ризиків для продавця). Сукупність таких даних продається через ланцюжок посередників маркетинговим компаніям і дозволяє їм приймати рішення щодо потенційної цінності конкретного користувача рекламодавця. Наприклад, при реєстрації в месенджері (Telegram, Viber та ін.) або іншому схожому сервісі користувачеві відразу доступний список його контактів з пам’яті пристрою. Причому контакти, зазвичай, отримують повідомлення у тому, що він почав користуватися сервісом. На основі списку контактів, бездротових мереж, Bluetooth-пристроїв у зоні видимості користувача можна

робити висновки про його найближче оточення, приблизний рівень доходу, сімейне становище тощо.

Продаж неявного доступу до пристрою. Ще дешевше продається невидимий, неявний доступ до пристрою: накрутка реклами у фоновому режимі, майнінг (видобуток) криптовалюти, розсилка спаму, «проксування трафіку» без відома користувача, тобто використання телефону як маршрутизатора стороннього інтернет-трафіку, що дозволяє зловмисникам маскувати діяльність у Мережі під звичайну активність користувача – наприклад для показів реклами. Все це можуть робити без вашого відома на вашому смартфоні шкідливі програми, якщо ви встановите їх – умисно чи мимоволі.

Дуже небезпечні програми-вимагачі – «локери» (віруси-вимагачі) та шифрувальники, які блокують смартфон і вимагають грошей за розблокування. Попадають на пристрій при завантаженні або встановленні сумнівного контенту, а також під виглядом «добрих» програм. Найвідомішим шифрувальником останніми роками був вірус Petya, який заразив у 2017 році сотні тисяч комп'ютерів. Ще одна категорія шкідливих програм – так звані грошові п'явки, програми з прихованою підпискою або одноразовими платежами, що експлуатують екосистему магазинів додатків і безтурботність користувача.

Таким чином, основні цілі шкідливих програм такі: крадіжка грошей з рахунку мобільного телефону через платні послуги операторів або непрохані підписки; крадіжка грошей із банківських рахунків через фальшиві мобільні додатки банків; використання обчислювальної потужності пристрою для своїх цілей: створення штучного трафіку, розсилання спаму, майнінг криптовалюти тощо без відома користувача; нарощування трафіку передачі, за який власник телефону буде змушений заплатити своєму оператору; збирання особистих даних для перепродажу (геолокація, списки бездротових мереж, контактів, тексти SMS, історія користування додатками тощо); маркетингове «профілювання» користувача: аналіз особистих даних, складання профілів поведінки користувача, перепродаж рекламних систем.

Шкідливі програми можуть встановлюватися добровільно самим користувачем, наприклад для отримання доступу до якогось цікавого або привабливого контенту (свіжий фільм). Існує ряд непрямих ознак шкідливих програм, наявність яких на пристрої має насторожити користувача. Насамперед це "захищені" месенджери. Месенджери із захищеним чатом можуть сигналізувати про бажання підлітка мати секрети від дорослих. Особливо підозрілі месенджери з «зникаючим контентом», які видаляють повідомлення після деякого часу (наприклад, Snapchat, Wickr). У таких додатках виникають ризики втягування підлітків у гру «в секрети» з однолітками, під час якої підлітка можуть зробити об'єктом шантажу, залучити до криміналу, схилити до суїциду тощо.

Підозрілі будь-які додатки, які нібито розширюють функціонал

популярних програм – «доповнення» для WhatsApp, Instagram, Minecraft тощо. Зустрічаються також модифіковані версії додатків «поліпшувачів», в які вбудовано шкідливий код. Як правило, мотивація користувача для встановлення подібних додатків – якась додаткова функціональність, якої немає у вихідному додатку, наприклад, можливість завжди бачити мережевий статус контактів у WhatsApp.

І Як відомо, комп'ютерний вірус – це шкідлива програма, написана спеціально для заподіяння шкоди програм та пристроїв або для кримінальної активності. Троянська програма – це шкідливий агент, що проникає на пристрій у вигляді легітимних програм. Має не тільки заявлену функціональність, але й побічні, небажані для користувача функції: розкрадання даних, приховане використання пристрою для створення трафіку на сайти, розсилки спаму тощо. На зорі цифрової епохи (кінець 1980-х років) перші комп'ютерні віруси створювалися для розваги з хуліганських спонукань. На початку 1990-х років їх було вже багато, але вони не мали комерційних цілей. Творці вірусів – початківці чи досвідчені програмісти – переважно прагнули самоствердження, демонстрації майстерності. При цьому, звичайно, завдаючи реальної шкоди мільйонам користувачів комп'ютерів. З того часу віруси та троянські програми стали комерційними інструментами, дозволивши створити величезну індустрію з оборотом десятки мільярдів доларів на рік. Зараз у цій розвиненій індустрії налагоджено детальний поділ праці: одні пишуть програми-конструктори вірусів, інші генерують ці віруси і запускають у Мережу, треті продають доступ до заражених комп'ютерів, четверті отримують замовлення та поширюють спам та установки непроханих програм тощо. на добу з'являється кілька десятків тисяч нових вірусів, а на рік – до 3-5 мільйонів.

Є кілька способів отримати вірус на комп'ютер або смартфон:

– Відкрити електронний лист із вірусом і тим більше відкрити файл, доданий до листа.

– Зайти на заражений сайт. Досить багато сайтів в Інтернеті, особливо нелегального змісту (порно, піратські відео, музика або софт), можуть встановити віруси на комп'ютер при відкритті веб-сторінок.

– Встановити на свій пристрій невідомий додаток з невідомого сайту. З додатком у процесі установки на пристрій можуть непомітно встановити віруси, рекламні програми та інше електронне сміття.

– Запустити завантаження MMS, надісланого з невідомого номера.

Вище ми вже розглянули ризики встановлення незнайомих програм та програм. Часто такі самі ризики несе і встановлення програм від знайомих брендів. Великі інтернет-сервіси домовляються з розповсюджувачами – файловими хостингами, каталогами програмного забезпечення, а часом і з піратськими сайтами – про поширення свого ПЗ (браузерів, пошукових систем, поштових клієнтів, ігор та агентів новин, месенджерів тощо). Це називається дистрибуцією інтернет-сервісів. Дистрибуцією програм,

покликаних «прив'язати» користувача до сервісу, займаються навіть і великі інтернет-компанії, наприклад, Google та інші. Більше того, їхня частка ринку істотно залежить від активності дистрибуції їхніх браузерів, агентів тощо. Дуже багато з цих розповсюджувачів додають до основного продукту ще 5–10 програм. Одні з них можуть бути нешкідливими або навіть корисними (хоч і отримані без попиту користувача); інші можуть виявитися вірусами і троянами. Відносно чесна програма-установник навіть показує користувачеві список цих додаткових програм із вже проставленими галочками, які дозволяють установку. Але так відбувається далеко не завжди. Легальні господарі основного продукту, з яким «їде» такий неавторизований «причіп», офіційно борються з таким використанням їхнього бренду, але їм не завжди вдається виявити подібне шахрайство та контролювати весь ланцюжок дистрибуції. Прихована або несвідома установка цих додаткових програм у кращому разі заражає комп'ютер або смартфон непроханим рекламним ПЗ, а в гіршому випадку і зовсім перетворює його на частину великого ботнета хакера. Проштовхування шахрайського програмного забезпечення у складі пакета з легальним програмним забезпеченням від відомих брендів – це один із видів так званої соціальної інженерії.

Ми розглянули деякі загрози, уразливості, ризики та проблеми, що виникають при використанні смартфонів, проте існує ще велика кількість проблем [1 - 3], які не завжди виявляються у явному вигляді і подальша робота в цьому напрямку потребує постійних зусиль фахівців з інформаційної безпеки.

1. Stopping Your Smartphone from Being a Cybersecurity Risk. Brian Wallace, November 2, 2021. URL: https://informationsecurity.report/guest-articles/stopping-your-smartphone-from-being-a-cybersecurity-risk/.

2. Are Your Mobile Devices Protected from Cyber Threats? - Cassie McCan September 19, 2023. URL: https://oit.nd.edu/about/news-and-updates/are-your-mobile-devices-protected-from-cyber-threats/.

3. 9 top mobile security threats and how you can avoid them. - Charlie Osborne. Oct. 18, 2023. URL: https://www.zdnet.com/article/9-top-mobile-security-threats-and-how-you-can-avoid-them/.