МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

МАТЕРІАЛИ
ІІ Всеукраїнської науково-практичної конференції

20 листопада 2020 року

Видавничий дім
«Гельветика»
2020

УДК 004.056(063)
К38

Відповідальний редактор – Дикий Олег Вікторович, декан факультету кібербезпеки та інформаційних технологій, к. ю. н., доцент.

Укладачі:
Логінова Наталія Іванівна – завідувач кафедри інформаційних технологій, к. пед. н, доцент;
Бойко Віктор Дмитрович – доцент кафедри кібербезпеки, к. т. н.;
Флюнт Мар'яна Орестівна – аспірантка кафедри кримінології та кримінально-виконавчого права

К38 **Кібербезпека** в сучасному світі : матеріали ІІ Всеукраїнської науково-практичної конференції (м. Одеса, 20 листопада 2020 р.) / за ред. О. В. Дикого ; уклад.: Н. І. Логінова, В. Д. Бойко, М. О. Флюнт. – Одеса : Видавничий дім «Гельветика», 2020. – 244 с.

ISBN 978-966-992-297-7

У збірнику містяться матеріали доповідей, присвячених актуальним проблемам кібербезпеки в сучасному світі, що змінюється.

Подані матеріали відповідають сучасним тенденціям розвитку кібербезпеки в Україні та можуть бути корисними як у навчальному процесі, так і при проведенні наукових досліджень студентами та молодими вченими, а також для практичних працівників у зазначеній сфері.

УДК 004.056(063)

ISBN 978-966-992-297-7

Задерейко Александр Владиславович
Национальный университет «Одесская юридическая академия»,
доцент кафедры информационных технологий,
кандидат технических наук, доцент

АНАЛИЗ УТЕЧЕК ДАННЫХ ПОЛЬЗОВАТЕЛЕЙ В МОБИЛЬНЫХ ПРИЛОЖЕНИЯХ

Повсеместное использование мобильных приложений для оперативного получения информации и мгновенной коммуникации значительно увеличивает вероятность утечки персональных данных пользователей. Любые мобильные приложения социально-медийной направленности дают разработчикам легальный доступ к приватному спектру данных о пользователе. Перечень собираемой информации определяется лицензионным соглашением к каждому устанавливаемому мобильному приложению, которое большинство пользователей не изучают и «по умолчанию» соглашаются с условиями их использования.

Это обстоятельство определяет небходимость проведения комплекса экспериментальных исследований по изучению интернет-трафика мобильных приложений (см. рис. 1) [1]:

- фиксации всех входящих и исходящих интернет-соединений с удаленными доменами;
- определение доменов, с которыми устанавливаются «сторонние соединения[1]»;

[1] Под сторонними соединениями подразумеваются исходящие и входящие соединения мобильных приложений, которые устанавливаются с доменами, не имеющими прямого отношения к официальным доменам мобильных приложений.

• получение информации о доменах, с которыми устанавливаются «сторонние соединения»;

• блокировку входящих и исходящих «сторонних соединений» мобильных приложений с обязательной проверкой сохранения их работоспособности.

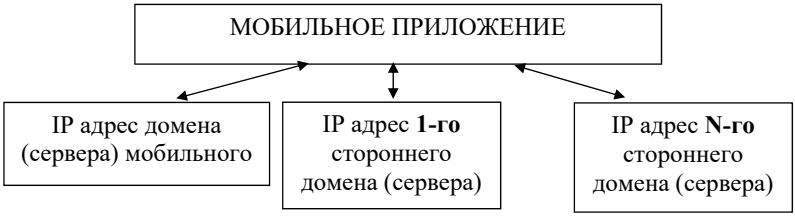

Рис. 1. Обмен данными мобильных приложений с доменным пространством Интернет

Цель исследования – изучить исходящие и входящие соединения мобильных приложений для популярных социальных сетей и мессенджеров с доменным пространством Интернет.

Объект исследования – мобильная операционная система Android 10, мессенджеры Whatsapp, Viber, Telegram, мобильные приложения Facebook, Instagram.

Средства исследования – мобильное программное обеспечение – сетевой экран No Root Firewall[1].

Интернет-провайдер – компания «Интертелеком – Украина».

Результаты исследования

В результате 120-ти дневной фиксации трафика мобильных приложений для коммуникации пользователей был зафиксирован перечень IP-адресов сторонних хостов (доменов), с которыми они выполняют обмен данными (см. табл. 1).

[1] **NoRootFirewall**–https://play.google.com/store/apps/details?hl=ru&id=app.greyshirts.firewall

Таблица 1.

Мобильные приложения		Сторонние IP адреса (домены)	Блокировка IP адресов	Работоспособность мобильного приложения (+ / -)
Мессенджеры	Telegram	*.1e100.net:443	√	+
		dns.google:443		
		149.154.167.*:5222		
		149.154.165.*:5222		
		91.108.56.192:5222		
		104.16.248.249:443		
	Whatsapp	*.static.sl-reverse.com:5222	√	+
		*.static.sl-reverse.com:443		
		*.fbcdn.net:443		
		*.1e100.net:443		
		157.240.14.53:5222		
		169.63.76.65:5222		
	Viber	*.compute-1.amazonaws.com:4244	√	+
		*.deploy.static.akamaitechnologies.com:443		
		*.googleusercontent.com:443		
		*.r.cloudfront.net:443		
		s3-website.eu-central-1.amazonaws.com:80		
		*.1e100.net:443		
		78.154.185.26:443		

Таблица 1. Продолжение

Мобильные приложения		Сторонние IP адреса (домены)	Блокировка IP адресов	Работоспособность мобильного приложения (+ / -)
	Instagram	78.111.180.97:443	√	+
		78.26.240.33:443		
		79.124.240.161:443		
		*.facebook.com		
		*.fbcdn.net		
		*.1e100.net:443		
	Facebook	*.compute-1.amazonaws.com:4244	√	
		*.fbcdn.net:443		
		*.1e100.net:443		
		*.utel.net.ua:443		
		*.vps-default-host.net:443		
		ua*.host.hit.gemius.pl:443		
		es49.mirohost.net:443		
		*.r.cloudfront.net:443		
		*.eu-west-1.compute.amazonaws.com:4244		
		*.clients.your-server.de:443		
		*.ip.kyivstar.net:443		
		*.pl-sh.host4.biz:443		
		*.te.net.net:443		
		*.dialup.umc.net.ua:443		

Примечание*: В таблице 1, * – отмечаются динамически изменяющиеся части доменных имен.*

Анализ входящих и исходящих соединений мобильных приложений позволил выявить домены сторонних интернет-ресурсов, к которым обращаются мобильные приложения и мессенджеры (см. табл. 1). Информация, полученная из

открытых источников об этих доменах позволила установить следующее:

• Домен **sl-reverse.com** – подключен к ns-серверам1: *networklayer.com*, *softlayer.net*. Принадлежит веб-платформе CSC Digital Brand Services, специализирующейся на цифровом управлении брендами и цифровом маркетинге;

• Домен **1e100.net** – подключен к ns-серверам *google.com*. Принадлежит корпорации Google [2];

• Домен **googleusercontent.com** – подключен к ns-серверам *google.com*. Принадлежит корпорации Google [2];

• Домен **akamaitechnologies.com** – подключен к ns-серверам: *akamaistream.net*. Принадлежит компании Akamai Technologies – провайдеру платформы доставки контента и приложений для акселерации доступа к интернет-ресурсам.

• Домен **cloudfront.net** – подключен к ns-серверам: *awsdns-35.org*, *awsdns-07.co.uk*, *awsdns-52.com*, *awsdns-19.net*. Принадлежит корпорации Amazon, специализирующейся на предоставлении услуг в облачных сервисах на основании анализа интернет-трафика.

• Домен **fbcdn.net** – подключен к ns-серверам: *facebook.com*. Принадлежит социальной сети Facebook. Используется для обслуживания доставки статического контента (видео и фото из CDN2).

• Домен **clients.your-server.de** – подключен к ns-серверам: *ns.second-ns.com*, *ns1.your-server.de*, ns3.second-ns.de.

• Домен **pl-sh.host4.biz** – подключен к ns-серверам: *curt.ns.cloudflare.com*, *kiki.ns.cloudflare.com*. *cloudflare.com*. Принадлежит организации «Host4Biz sp. z o.o.», оказывающей услуги хостинга. Находится под управлением, ns-серверов принадлежащим корпорации CloudFlare Inc, предоставляющей услуги CDN и сервера DNS.

---

[1] **NS-сервер** – Name Server (DNS-сервер), преобразующий доменные имена, с которыми работают пользователи, в понятные компьютерам IP-адреса или в обратном направлении.

[2] **CDN (content delivery network)** – сеть доставки контента, – это распределенная сеть серверов, используемых для ускорения доставки запрашиваемого контента с ближайшего к пользователю сервера.

• Домен **es49.mirohost.net** – принадлежит организации Internet Invest, Ltd, регистратору доменных имён и крупнейшему хостинг-провайдеру в Украине.

• Домен **net.net** – принадлежит организации Bodis, LLC. Оказывающей услуги по монетизации и управлению доменным трафиком.

• Домен **kyivstar.net** – принадлежит интернет-провайдеру Киевстар.

• Домен **umc.net.ua** – принадлежит интернет-провайдеру Ukrainian Mobile Communications.

• Домен **utel.net.ua** – принадлежит интернет-провайдеру Укртелеком.

• IP адрес **78.154.185.26** – принадлежит интернет-провайдеру – Eurotranstelecom Ltd (Украина).

• IP адрес **78.111.180.97** – принадлежит интернет-провайдеру LLC Renome-Service (Украина).

• IP адрес **79.124.240.161** – принадлежит интернет-провайдеру Lifecell (Украина).

Выводы

1. Мобильные приложения и мессенджеры устанавливают соединения и ведут интенсивный обмен данными со сторонними доменами (серверами), владельцы которых, представлены компаниями, оказывающими услуги по транзиту, сбору, накоплению, обработке, и монетизации доменного трафика мобильных приложений с использованием облачных технологий. Такой обмен данными с высокой долей вероятности может привести к не контролируемому пользователями сбору их персональных данных.

2. Мобильные приложения Facebook и Instagram устанавливают соединения со сторонними интернет-провайдерами Украины, а также с доменами, принадлежащими компаниям, специализирующимся на монетизации доменного трафика.

3. Все исследуемые мобильные приложения устанавливают соединения с доменами, принадлежащими корпорации Google (домен – 1e100.net). Помимо этого:

• Месенджер Telegram осуществляет попытку перенаправления своего трафика через DNS сервера корпорации Google (домен – dns.google).

• Месенджер Viber устанавливает дополнительное соединение с сервисом анализа контента корпорации Google (домен – googleusercontent.com).

4. Блокировка зарегистрированных соединений мессенджеров Telegram, Whatsapp, Viber и приложений Facebook и Instagram на сторонние сервера, не вызывает потерю их работоспособности и позволяет:

• исключить несанкционированный пользователями сбор персональных данных;

• полностью сохранить функциональность и работоспособность мобильных приложений;

• сократить передачу интернет-трафика пользователя на 50–70%, что позволит сократить расходы пользователей на оплату услуг Интернет-провайдеров мобильного трафика.

Список используемых источников:

1. Задерейко О. В. Аналіз вірогідних витоків конфіденційної інформації користувачів у мобільних застосунках / О. В. Задерейко, Н. І. Логінова, О. Г. Трофименко // Графічні технології моделювання об'єктів, процесів та явищ: зб. тез доп. Міжнар. наук.-практ. конф. (м. Одеса, 23–24 квіт. 2020 р.) / МОН України; Військова академія. – Одеса, 2020.

2. Google: зловещая черта. [Електронний документ]. – URL: https://zadereyko.info/video/google_zloveshaya_cherta.htm.

Ключові слова: витоки даних, збір даних в мобільних додатках, збір даних в месенджерах, збір даних, монетизація даних

Ключевые слова: утечки данных, сбор данных в мобильных приложениях, сбор данных в мессенджерах, сбор данных, монетизация данных

Keywords: data leaks, data collection in mobile apps, data collection in messengers, data collection, data monetization

Наукове видання

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

МАТЕРІАЛИ
ІІ Всеукраїнської науково-практичної конференції

20 листопада 2020 року

Верстка – Т.В. Мартиненко

Підписано до друку 01.12.2020 р. Формат 60х84/16.
Папір офсетний. Гарнітура Cambria. Цифровий друк.
Умовно-друк. арк. 14,18. Тираж 150. Замовлення № 1120-300.
Віддруковано з готового оригінал-макета.

Видавництво і друкарня – Видавничий дім «Гельветика»
65101, Україна, м. Одеса, вул. Інглезі, 6/1
Телефони: +38 (0552) 39 95 80,
+38 (095) 934 48 28, +38 (097) 723 06 08
E-mail: mailbox@helvetica.com.ua
Свідоцтво суб'єкта видавничої справи
ДК № 6424 від 04.10.2018 р.