

during perception process, *Advances in Neural Networks, Fuzzy Systems and Artificial Intelligence, Ser.: Recent Adv. in Computer Engineering*, Ed. J. Balicki (WSEAS Pub.), Vol.21, 143 (2014).

Ключові слова: кібербезпека, інформаційні системи, хаос-геометричний підхід

Ключевые слова: кибербезопасность, информационные системы, хаос-геометрический подход

Keywords: cybersecurity, information systems, chaos-geometric approach

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 необходимость 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.

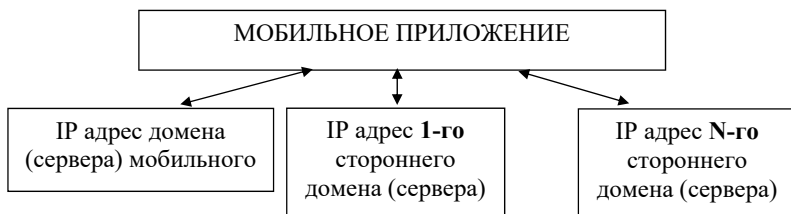


Рис. 1. Обмен данными мобильных приложений с доменным пространством Интернет

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 Firewall¹.

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	<u>*.1e100.net:443</u>	√	+
		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		
		<u>*.1e100.net:443</u>		
		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		
		<u>*.1e100.net:443</u>		
		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		
		<u>*.1e100.net:443</u>		
	Facebook	*.compute-1.amazonaws.com:4244	√	
		*.fbcdn.net:443		
		<u>*.1e100.net:443</u>		
		*.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-серверам *1: 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 контролируруемому 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: витокі даних, збір даних в мобільних додатках, збір даних в месенджерах, збір даних.

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

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