КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (23), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.23.199212
УДК 004.738.2

Задерейко Олександр Владиславович
кандидат технічних наук, доцент, доцент кафедри інформаційних технологій
Національний університет «Одеська юридична академія», Одеса, Україна,
ORCID 0000-0003-0497-9861
zadereyko@onua.edu.ua

Трофименко Олена Григорівна
кандидат технічних наук, доцент, доцент кафедри інформаційних технологій
Національний університет «Одеська юридична академія», Одеса, Україна,
ORCID 0000-0001-7626-0886
trofymenko@onua.edu.ua

Лобода Юлія Геннадіївна
кандидат технічних наук, доцент, доцент кафедри інформаційних технологій
Національний університет «Одеська юридична академія», Одеса, Україна,
ORCID 0000-0001-7083-552X
jul.loboda@gmail.com

Логінова Наталія Іванівна
кандидат педагогічних наук, доцент, завідувачка кафедри інформаційних технологій
Національний університет «Одеська юридична академія», Одеса, Україна,
ORCID 0000-0002-9475-6188
loginova@onua.edu.ua

Прокоп Юлія Віталіївна
кандидат історичних наук, доцент, доцент кафедри інженерії програмного забезпечення
Національний університет «Одеська політехніка», Одеса, Україна,
ORCID 0000-0002-6608-3668
prokop.y.v@op.edu.ua

АНАЛІЗ ПОТЕНЦІЙНИХ ВИТОКІВ ПЕРСОНАЛЬНИХ ДАНИХ У ВЕББРАУЗЕРАХ

Анотація. Розповсюдження переважної кількості веббраузерів активно стимулюється за рахунок їх безоплатного використання. Це є звичайною практикою розробників веббраузерів, тому що вона надає їм великі можливості стосовно їх розповсюдження. Зворотною стороною цього процесу є не контрольований користувачем збір персональних даних розробниками веббраузерів. Зібрані дані автоматично передаються провідним IT-компаніям таким як Google, Microsoft, Cloudflare, які здійснюють збір, накопичення, обробку та монетизацію персональних даних користувачів в автоматизованому режимі. Фактично це призводить до того, що будь-який користувач веббраузера профілюється у сервісах провідних IT-компаній, які отримують повну інформацію про дії користувача в мережі Інтернет. Такий стан речей суперечить положенням статті 32 Конституції України, яка гарантує право людини на невтручання в її особисте життя, а також базовим положенням Закону України «Про захист персональних даних». У рамках дослідження виконано довготривалу фіксацію і подальший аналіз мережевого трафіка популярних в Україні веббраузерів Google Chrome, Microsoft Edge, Mozilla Firefox, Opera. Особливість виконаного дослідження полягала у тому, щоб отримати мережевий трафік який ініціюють саме веббраузери в активному стані впродовж тривалого часу. З метою підвищення достовірності дані про мережеві з'єднання веббраузерів були отримані за допомогою двох незалежних програмних інструментів для моніторингу трафіка на мережевому інтерфейсі пристрою комунікації. Виконаний аналіз мережевих з'єднань веббраузерів дозволив встановити наявність тісного зв'язку компаній-розробників безкоштовно розповсюджуваних веббраузерів і провідних IT-компаній, які монопольно контролюють дії користувачів в інтернет-просторі. Такий стан справ суперечить правовим

нормам щодо забезпечення приватності користувачів веббраузерів у контексті використання їх персональних даних без їх відома та згоди. Запобігти цьому може використання мережевих екранів, які працюють на 3, 4 та 7 рівні моделі OSI стека TCP/IP.

Ключові слова: аналіз мережевого трафіка; мережевий трафік веббраузера; збір персональних даних; веббраузер; витоки персональних даних у веббраузерах.

ВСТУП

Сучасні технології комунікації користувачів з інтернет-простором здійснюються за допомогою веббраузерів. Більшість їх поширюється розробниками на безоплатній основі. Такий підхід викликає закономірне питання: чому вибрано саме таку політику розповсюдження веббраузерів і чим насправді розплачуються за їх використання користувачі?

Постановка проблеми. Чи може користувач інтернет-послуг уникнути збору даних про нього? Адже статтею 32 Конституції України проголошено право людини на невтручання в особисте життя, а в Законі України «Про захист персональних даних» визначено механізми його реалізації. Крім того, не допускається збирання, зберігання, використання поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

Дослідження, проведене WhoTracks.Me, свідчить, що 82% вебтрафіка містять сторонні скрипти Google і половина з них збирають персональні дані користувачів. Google відстежує 74% вебтрафіка, Amazon — 17%, Meta — 14%, Microsoft — 12% (https://whotracks.me/). Трекери використовують інструменти ідентифікації, щоб зв'язати інформацію про людину з різних сайтів і створити профіль користувача на основі історії вебперегляду. Профілювання трекера розміщує користувачів у групи і продає дані третім сторонам. Здебільшого при використанні безкоштовних веббраузерів розробники вбудовують приховані механізми, які постійно функціонують та здійснюють збір особистих даних користувачів, незалежно від конфігурації та кінцевих налаштувань веббраузерів [1]. При використанні веббраузерів розробники повідомляють користувача про збирання анонімної статистики, яка збирається з метою покращення якості продукту та надають перелік нечітко сформульованих умов використання, що розв'язує руки юристам компанії-розробника [2].

Аналіз останніх досліджень та публікацій. Відмінною рисою функціонування сучасних веббраузерів є те, що вони зберігають дані, пов'язані з діями користувача у мережі [3]. Дані накопичуються в локальному сховищі веббраузера, при цьому їхнє подальше збереження може становити загрозу конфіденційності користувача. Для вирішення проблеми конфіденційності розробники ввели режим приватного перегляду, який не передбачає локального збереження конфіденційних даних користувача [4]. Однак насправді не існує гарантії, що режим приватного перегляду в сучасних веббраузерах реалізований з урахуванням перевірки можливості вилучення особистих даних користувача з локального сховища даних веббраузера [5].

Іншим, не менш важливим аспектом є те, що веббраузери не працюють автономно від серверної інфраструктури їх розробників. Більшість веббраузерів зв'язуються зі своїми серверами для перевірки оновлень [6], полегшення проведення тестових випробувань (наприклад, перевірки нових функцій перед повним розгортанням), телеметрії тощо [7] – [9].

Розробники веббраузерів надають різні онлайн-послуги своїх сервісів, доступ до яких здійснюється безпосередньо через веббраузери або через інтегровану підтримку сервісів. Тобто, коли користувачі запускають веббраузери та/або відкривають вебсторінки, веббраузери обмінюються даними із серверами розробників [10].

Важливо, що передача веббраузерами персональних даних користувача на сервери розробників є порушенням конфіденційності. Наприклад, передача докладної інформації про модель/версію комунікаційного пристрою користувача, його мовний стандарт, пов'язана з ризиком для конфіденційності, оскільки дані можна легко зв'язати з користувачем [11], [12]. Це відбувається, коли веббраузер пов'язує довгий рандомізований рядок з одним екземпляром веббраузера, який потім діє як ідентифікатор екземпляра веббраузера (оскільки інші екземпляри браузера не мають однакового рядкового значення). Це дозволяє при відправленні разом з іншими даними пов'язувати дані з тим самим екземпляром веббраузера.

Коли один і той самий ідентифікатор використовується в кількох з'єднаннях, це дозволяє зв'язувати дані з'єднання у часі. Суттєво, що дані, які передаються, завжди містять IP-адресу комунікаційного пристрою користувача, що використовується для визначення розташування користувача через служби geoIP. Попри те, що прив'язка даних до веббраузера не розкриває реальну особу користувача, проаналізовані дослідження показали, що дані про місцезнаходження, пов'язані з часом, можуть використовуватися для деанонімізації [13], [14]. Наприклад, на основі даних про місцезнаходження можна зробити висновок про місце роботи та будинок користувача, а в поєднанні з іншими даними ця інформація є вельми наочною [14]. Важливим фактором є частота з'єднань веббраузера з його серверами. Наприклад, передача IP-адреси пристрою комунікації користувача один раз на день має набагато менший потенціал витоків персональних даних, ніж передача IP-адреси з інтервалом в 1 годину. Іншим аспектом порушення конфіденційності користувача є передача історії переглядів користувачів на сервери розробників веббраузерів. Як показують дослідження [15], [16], деанонімізувати історію відвідувань нескладно, особливо у поєднанні з іншими даними (нагадаємо, що передача даних завжди передбачає спільне використання IP-адреси пристрою комунікації (місце розташування), тому їх можна легко поєднати з історією переглядів). Все це зумовлює потребу детального вивчення мережевого трафіка, ініційованого веббраузерами. Це дозволить встановити кінцевих бенефіціарів, які отримують персональні дані користувачів та визначити способи захисту від потенційних витоків.

Метою статті є аналіз мережевого трафіка веббраузерів, що надасть змогу визначити способи захисту персональних даних користувачів від потенційних витоків.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Для виконання поставленої мети необхідно здійснити фіксацію з'єднань TCP на рівні Операційної Системи (ОС). Це може бути виконано з використанням Програмного Забезпечення (ПЗ) засобів розробника ОС [17] та спеціалізованого ПЗ, що здійснює перехоплення мережевого трафіка на мережевому інтерфейсі пристрою комунікації [18].

Для отримання достовірніших результатів варто виконати фіксацію мережевого трафіка веббраузерів протягом тривалого проміжку часу. Оптимальним є часовий інтервал, що відповідає середньостатистичній тривалості робочого дня користувача. У

досліджені час фіксації мережевого трафіка веббраузерів було збільшено до 12 годин для забезпечення запасу достовірності отриманих даних.

Фіксація мережевого трафіка веббраузерів виконувалася за суворого дотримання таких умов:

– виконання підготовки «чистої» ОС, в якій відсутнє якесь встановлене Прикладне Програмне Забезпечення (ППЗ);
– встановлення останніх версій дистрибутивів досліджуваних веббраузерів з офіційних сайтів їх розробників;
– виконання запуску веббраузерів з усталеними налаштуваннями від розробника.

Наразі найпопулярнішими веббраузерами в Україні є: Google Chrome, Microsoft Edge, Mozilla Firefox, Opera [19].

Загальний процес проведення дослідження подано у вигляді узагальненого алгоритму визначення потенційних витоків персональних даних користувача веббраузера (рис. 1).

Рис. 1. Алгоритм аналізу з'єднань веббраузера

Для виконання поставленої мети було підготовлено робоче місце користувача, яке містить:

– стаціонарний персональний комп'ютер;
– ОС Windows 11 з офіційного сайту розробника;
– веббраузери: Google Chrome, Microsoft Edge, Mozilla Firefox, Opera [19];
– ПЗ TCPview [17];
– ПЗ Wireshark [18].

Отримані результати фіксації мережевого трафіка веббраузерів [19] подані у табл. 1–2.

ISSN 2663 - 4023

Таблиця 1

Зафіксовані TCP з'єднання веббраузерів на рівні ОС з використанням ПЗ TCPview

Веббраузер	IP адреса	Порт	Назва підмережі	Власник
Mozilla FireFox	34.235.58.193	443		Amazon Technologies Inc.
	35.244.181.201	443	Google-Cloud	Google LLC
	34.107.221.82	80	Googl-2	Google LLC
	34.117.237.239	443	Googl-2	Google LLC
	34.160.144.191	443	Googl-2	Google LLC
	185.225.250.17	80	Akamai	e-Poludnie Contact Role
	185.225.250.42		Akamai	
	34.149.100.209	443	Googl-2	Google LLC
	34.117.35.28	443	Googl-2	Google LLC
	34.107.243.93	443	Googl-2	Google LLC
	198.187.28.133	443	Ncnet-2	Namecheap, Inc.
	142.250.203.195	80	Google	Google LLC
Chrome	142.250.186.193	443	Google	Google LLC
	64.233.164.84	443	Google	Google LLC
	216.58.208.196	443	Google	Google LLC
	142.250.203.195	443	Google	Google LLC
Opera	77.111.244.47	443	Hernlabs	Hern Labs Netops
	185.26.182.122	443	No-Opera-Ams-Public	Opera Software AS
	95.101.23.73	443	Akamai-Pa	Akamai Technologies
	77.111.247.15	443	Hernlabs	Hern Labs Netops
	77.111.247.47	443	Hernlabs	Hern Labs Netops
	40.114.177.156	443	MSFT	Microsoft Corporation
	142.250.203.132	443	Google	Google LLC
	185.26.182.106	443	No-Opera-Ams-Public	Opera Software AS
	82.145.216.19	443	No-Opera-Ams-Public	Opera Software AS
Edge	204.79.197.203	443	Ecn-network	Microsoft Corporation
	204.79.197.203	443		
	204.79.197.200	443		
	13.107.21.239	443	MSFT	
	13.107.42.14	443		
	20.223.35.26	443		
	13.107.6.158	443		
	13.107.6.200	443		
	20.52.64.201	443		
	20.127.253.7	443		
	77.75.149.203	443	ua-dataline-ua-20070511	Dataline LLC
	77.75.149.211	443		
	77.75.149.226	443		
	77.75.149.235	443		
	68.219.88.97	443	bls-68-219-0-0-1003020945	Asm Adsl Eeua
	95.100.111.41	443	Akamai-pa	Akamai Technologies
	95.100.111.56	443		
	104.91.48.24	443		
	2.23.109.30	443		
	2.18.29.176	443		
	2.18.29.161	443		
	18.172.242.100	443	Amazon-cf	Amazon Technologies Inc.
	13.248.245.213	443		
	18.172.242.21	443		
	146.75.1.44	443	Fastly	Fastly

	70.42.32.95	443	inap-nym-outbrain-70-42-32-0	Private Customer
	52.49.83.158	443	Amazon-Dub	Amazon Data Services Ireland Limited
	185.255.84.152	443	AdYouLike	Iguane Solutions SAS
	35.208.249.213	443	Google Cloud	Google LLC
	35.213.89.133	443	Google Cloud	Google LLC
	162.19.138.83	443	Sd-Lim	OVH Gmbn

Таблиця 2

Зафіксовані з'єднання веббраузерів на мережевому інтерфейсі з використанням ПЗ Wireshark

Веббраузер	Домен	IP-адреса	Протокол	Порт	Власник
Mozilla FireFox	detectportal.firefox.com	34.127.255.255	DNS	53	Google LLC
	prod.detectportal.prod.cloudops.mozgcp.net	34.127.255.255	DNS	53	
		34.107.221.82	TCP	80	
	contile.services.mozilla.com	34.127.255.255	DNS	53	
		34.117.237.239	TCP	443	
		34.107.221.82	HTTP	80	
		34.117.237.239	TLSv1.3	443	
	content-signature-2.cdn.mozilla.net	34.191.255.255	DNS	53	
	prod.content-signature-chains.prod.webservices.mozgcp.net	34.191.255.255	DNS	53	
		34.160.144.191	TCP	443	
	firefox.settings.services.mozilla.com	34.191.255.255	DNS	53	
	push.services.mozilla.com	34.127.255.255	DNS	53	
		34.149.100.209	TCP	443	
		34.149.100.209	TLSv1.3	443	
	autopush.prod.mozaws.net	34.127.255.255	DNS	53	
	safebrowsing.googleapis.com	142.251.255.255	DNS	53	
		142.250.186.202	TCP	443	
		142.250.186.202	TLSv1.3	443	
		34.107.243.93	TCP	443	
		216.58.208.195	TCP	443	
		216.58.208.195	OCSP	443	
	pki-goog.l.google.com	142.251.255.255	DNS	53	
		35.244.181.201	TCP	443	
	prod.balrog.prod.cloudops.mozgcp.net	35.247.255.255	DNS	53	
		185.225.250.17	TCP	443	Akamai Technolo-gies
	ocsp.digicert.com	192.229.255.255	DNS	53	Edgecast Inc
	fp2e7a.wpc.phicdn.net	192.229.255.255	DNS	53	
		192.229.221.95	OCSP	80	
Chrome	clientservices.googleapis.com	142.250.203.195	DNS	53	Google LLC
	lh5.googleusercontent.com	142.250.186.193	DNS	53	
	www.gstatic.com	216.58.215.99 142.250.75.3	DNS	53	
	apis.google.com	142.250.186.206	DNS	53	
	plus.l.google.com	142.250.203.206 216.58.208.206	DNS	53	
	clients2.googleusercontent.com	172.217.16.33	DNS	53	
	googlehosted.l.googleusercontent.com	216.58.208.193	DNS	53	
	update.googleapis.com	142.250.203.131 142.250.186.195	DNS	53	

	optimizationguide-pa.googleapis.com	172.217.16.10 172.217.16.42 216.58.215.106 216.58.209.10 142.250.203.202 216.58.208.202 142.250.75.10 142.250.186.202 142.250.203.138	DNS	53	
	clients2.google.com	142.250.75.14 216.58.208.206	DNS	53	
	edgedl.me.gvt1.com	34.104.35.123	DNS	53	
		172.217.16.3	TCP	53	
		142.250.186.196	TCP	53	
		142.250.186.193	TCP	53	
		173.194.222.84	TCP	53	
		142.250.203.206	TCP	53	
		216.58.215.99	TCP	53	
		142.250.203.131	TCP	53	
		172.217.16.33	TCP	53	
		172.217.16.10	TCP	53	
		142.250.75.14	TCP	53	
		142.250.75.3	TCP	53	
		172.217.16.42	TCP	53	
		172.217.16.42	TLSv1.3	53	
		142.250.186.196	UDP	53	
		142.250.186.193	UDP	53	
		173.194.222.84	UDP	53	
		216.58.215.99	UDP	53	
		142.250.203.206	UDP	53	
		142.250.203.131	UDP	53	
		172.217.16.33	UDP	53	
		172.217.16.10	UDP	53	
		142.250.75.14	UDP	53	
		216.58.215.99	UDP	53	
		172.217.21.163	UDP	53	
Opera	opera.cloudflare-dns.com	162.159.255.255	DNS	53	Cloudf-lare Inc.
		172.64.41.5	TCP	443	
		172.64.41.5	TLSv1.3	443	
		185.26.182.123	TCP	443	Opera Software AS
		185.26.182.111	TCP	443	
		185.26.182.112	TCP	443	
		185.26.182.118	TCP	443	
		82.145.216.24	TCP	433	
		82.145.216.24	TLSv1.3	433	
		82.145.217.121	TCP	433	
		77.111.247.15	TCP	443	HERN labs AB
		77.111.244.10	TCP	443	
		77.111.244.10	TLSv1.3	443	
		142.250.203.132	TCP	433	Google LLC
		216.58.208.195	TCP	433	
		95.101.23.73	TCP	433	Akamai Technolo-gies
Edge	www-msn-com.a-0003.a-msedge.net	204.79.197.255	DNS	53	
	ntp.msn.com	204.79.197.255	DNS	53	

	srtb.msn.com	204.79.197.255	DNS	53	Microsoft Corporation
	arc.msn.com	20.128.255.255	DNS	53	
	edge.microsoft.com	204.79.197.255	DNS	53	
		204.79.197.203	TCP	443	
		204.79.197.203	TLSv1.2	443	
		204.79.197.239	TCP	443	
		204.79.197.239	TLSv1.2	443	
		204.79.197.219	TCP	443	
		204.79.197.219	TLSv1.2	443	
		20.231.121.79	TCP	443	
		52.108.8.254	TCP	443	
		52.108.8.254	TLSv1.2	443	
		13.107.6.158	TCP	443	
		13.107.6.158	TLSv1.2	443	
		13.107.21.200	TCP	443	
		13.107.21.200	TLSv1.2	443	
		20.189.173.15	TCP	443	
		20.189.173.15	TCP	443	
		20.223.35.26	TCP	443	
		20.223.35.26	TLSv1.2	443	
		20.13.241.89	TCP	443	
		20.13.241.89	TLSv1.2	443	
		20.189.173.15	TCP	443	
		13.107.213.45	TCP	443	
		13.107.213.45	TLSv1.2	443	
		40.119.249.228	TCP	443	
		40.119.249.228	TLSv1.2	443	
		13.107.6.158	TCP	443	
		68.219.88.97	TCP	443	
		68.219.88.97	TLSv1.2	443	
		2.18.29.178	TCP	443	Akamai Technologies
		2.18.29.178	TLSv1.2	443	
		95.100.111.10	TCP	443	
		95.100.111.10	TLSv1.2	443	
		23.48.2.57	TCP	443	
		23.48.2.57	HTTP	80	
		2.18.29.186	TCP	443	
		2.18.29.186	TLSv1.2	443	
		2.18.29.193	TCP	443	
		2.18.29.193	TLSv1.2	443	
		2.18.29.186	UDP	443	
		18.244.102.57	TCP	443	Amazon, Inc
		18.244.102.57	TLSv1.2	443	
		77.75.149.217	TCP	443	Data Line LLC
		77.75.149.217	TLSv1.2	443	
		77.75.149.232	TCP	443	
		77.75.149.232	TLSv1.2	443	
		77.75.149.203	TCP	443	
		77.75.149.203	TLSv1.2	443	
		77.75.149.217	TCP	443	

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Аналіз отриманих експериментальним шляхом доменів та IP-адрес, з якими веббраузери (в режимі налаштувань «default») здійснюють з'єднання виявив:

1. під час активізації веббраузер Google Chrome встановлює з'єднання з IP-адресами за протоколами TCP, DNS, TLS, UDP виключно із серверами компанії розробника Google LLC;

2. під час активізації веббраузер Mozilla Firefox встановлює з'єднання з IP-адресами за протоколами TCP, DNS, HTTP, TLS із серверами компанії розробника Google LLC та з IP-адресами сторонніх інтернет-сервісів:

- IP-адреса 192.229.221.95 належить компанії Edgecast Inc, яка надає послуги CDN;
- IP-адреса 185.225.250.17 належить компанії Akamai Technologies, яка надає повний контроль за ним компанії Stowarzyszenie e-Poludnie — асоціації E-South, що займається інтеграцією малих та середніх операторів зв'язку Misot;
- IP-адреса 198.187.28.133 належить компанії Namecheap, Inc — акредитованому ICANN реєстратору доменних імен та вебхостингової компанії;
- IP-адреса 34.235.58.193 належить компанії Amazon Technologies Inc, яка надає послуги хостингу, хмарних обчислень та зберігання інформації [20].

3. при активізації веббраузер Opera встановлює з'єднання з IP-адресами за протоколами TCP і TLS із серверами компанії розробника Opera Software AS та з IP-адресами сторонніх інтернет-сервісів:

- домен opera.cloudflare-dns.com та IP-адреса 172.64.41.5 належить компанії Cloudflare Inc, яка надає послуги CDN, захист від DDoS-атак, захист від витоків DNS;
- IP-адреси 142.250.203.132 та 216.58.208.195 належать компанії Google LLC;
- IP-адреса 95.101.23.73 належить компанії Akamai Technologies, яка надає послуги для акселерації інтернет-ресурсів та платформ для доставки контенту та застосунків.

4. під час активізації веббраузер Edge встановлює з'єднання з IP-адресами за протоколами TCP, UDP та TLS із серверами компанії розробника Microsoft Corporation та з IP-адресами сторонніх інтернет-сервісів:

- IP-адреси 2.18.29.178, 95.100.111.10, 23.48.2.57, 2.18.29.* належать компанії Akamai Technologies, яка надає послуги для акселерації інтернет-ресурсів та платформ для доставки контенту та застосунків;
- IP-адреса 18.244.102.57 належить компанії Amazon Technologies Inc, яка надає послуги хостингу, хмарних обчислень та зберігання інформації;
- IP-адреси 77.75.149.* належать інтернет-провайдеру Dataline, який надає послуги магістрального оптоволоконного зв'язку на території України.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У роботі виконано фіксацію з'єднань популярних веббраузерів з інтернет-простором у режимі налаштувань, встановлених розробником. Аналіз з'єднань веббраузерів з інтернет-простором дозволив встановити:

- веббраузер браузер Google Chrome встановлює з'єднання лише з IP-адресами, що належать компанії розробника Google LLC. Це свідчить про монопольний контроль з боку компанії розробника та недопущення будь-яких потенційних витоків персональних даних користувачів на сторонні інтернет-сервіса [21]. Виявлено з'єднання веббраузера Google Chrome за протоколом DNS із піддоменами кореневого домену *.googleusercontent.com. Відомо [22], що цей домен (сервіс) використовується компанією Google для зберігання статичних даних користувачів, наприклад, для хостингу різних файлів і зображень з подальшою організацією загального доступу до них. У дослідженні з'єднання з цим сервісом відбувалося веббраузером в перші хвилини його активізації. Цей факт підтверджує, що при активізації веббраузера відбувається його ініціалізація в сервісі googleusercontent.com (виконується прив'язка персональних даних користувача: IP-адреси, геолокації, версії веббраузера, набору плагінів, мовних налаштувань, кешу веббраузера тощо) [23]. Це дозволяє розробнику виконувати прив'язку веббраузера користувача до його інтернет-контенту. У разі наявності у користувача єдиного облікового запису в сервісах Google і подальшої авторизації у веббраузері Chrome додається пряма прив'язка облікового запису користувача до всіх його дій, здійснюваних у веббраузері та інтернет-просторі;
- веббраузер Mozilla Firefox встановлює з'єднання з IP-адресами, що належать компанії розробника Google LLC та з IP-адресами, що належать компаніям, які надають послуги CDN та доступ до інтернет-простору. Це дозволяє їм зібрати конфіденційну інформацію про IP-адресу користувача (його геолокацію) та інтернет-контент, який він запитує [23]. Отримані результати дозволяють зробити висновок про те, що компанія Google LLC здійснює фактично монопольний контроль за всіма діями користувача в інтернет-просторі з використанням веббраузера Mozilla Firefox;
- веббраузер Opera встановлює з'єднання з IP-адресами, що належать компанії розробника Google LLC та з IP-адресами, що належать компаніям, які надають послуги CDN та захисту від витоків DNS. Вони контролюють понад 50% загальносвітового інтернет-трафіка;
- веббраузер Edge встановлює з'єднання з IP-адресами, що належать компанії Microsoft Corporation, та з IP-адресами, що належать компаніям, які надають послуги CDN.

Проведений аналіз з'єднань популярних веббраузерів свідчить про високу ймовірність наявних домовленостей між розробниками веббраузерів та провідними IT-компаніями, що займають за фактом монопольне становище на інтернет-ринку, щодо використання їхніх сервісів для збору, оброблення та подальшої монетизації персональних даних користувачів [21].

Візуальну інтерпретацію зв'язку веббраузерів і провідних IT-компаній наведено на рис. 2.

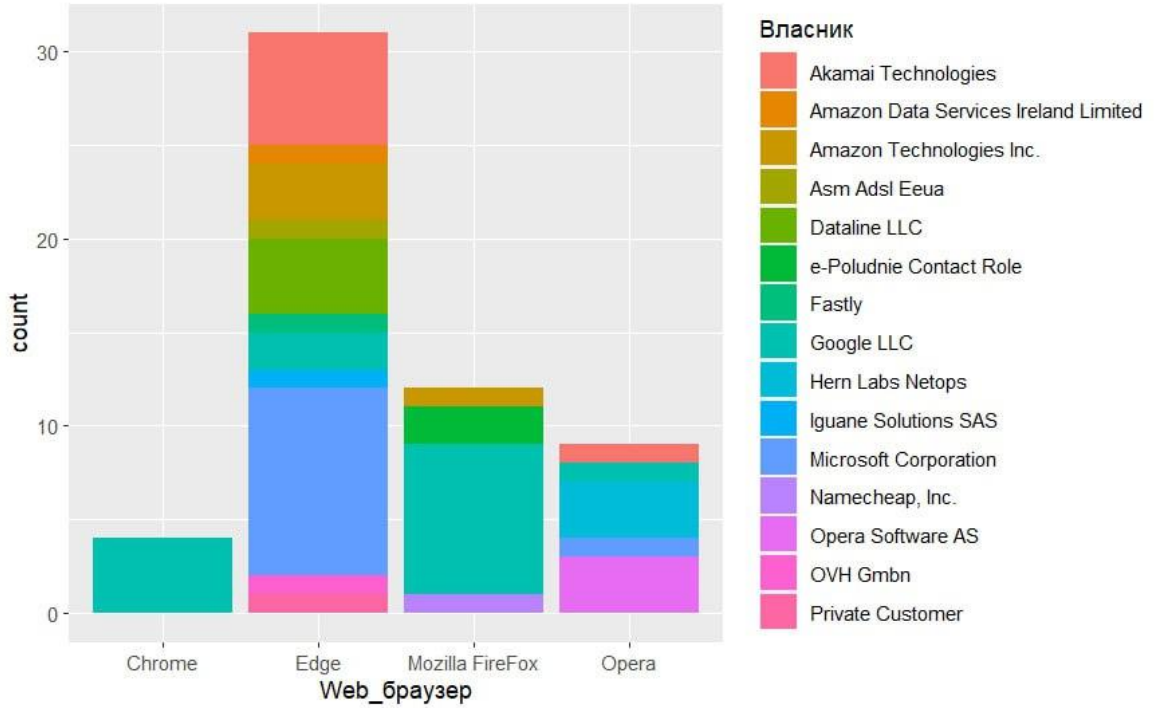

Рис. 2. Зв'язок веббраузерів і провідних IT-компаній

Такий стан справ суперечить правовим нормам щодо забезпечення конфіденційності даних користувачів. Вирішення цієї проблеми може бути реалізовано за рахунок фільтрації трафіка з використанням мережевих екранів, що працюють на 3, 4 і 7 рівнях моделі OSI стека TCP/IP [24]. Практична реалізація такого походу довела його високу ефективність забезпечення конфіденційності користувачів за рахунок блокування встановлених з'єднань (див. табл. 1–2). Це дозволить значно підвищити конфіденційність користувачів при використанні безкоштовних веббраузерів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Halle, M., Demeusy, V., & Kikinis, R. (2017). The open anatomy browser: a collaborative web-based viewer for interoperable anatomy atlases. *Frontiers in neuroinformatics*, *11*. https://doi.org/10.3389/fninf.2017.00022
2. Nomoto, K., et al. (2023). Understanding the Inconsistencies in the Permissions Mechanism of Web Browsers. *Journal of Information Processing, 31,* 620–642. https://doi.org/10.2197/ipsjjip.31.620
3. Pau, K., et al. (2023). The Development of a Data Collection and Browser Fingerprinting System. *Sensors, 23, 3087.* https://doi.org/10.3390/s23063087
4. *Overview. Safe Browsing APIs (v4).* (n.d.). Google for Developers. https://developers.google.com/safe-browsing/v4
5. Cai, H., et al. (2023). Toward Correlated Data Trading for Private Web Browsing History. *IEEE Internet of Things Journal, 10(7),* 5859–5872. https://doi.org/10.1109/JIOT.2023.3237707
6. *Autoupdating. Apps. Chrome for Developers*. (n.d.). Chrome for Developers. https://developer.chrome.com/apps/autoupdate
7. *Google Chrome Privacy Whitepaper*. (n.d.). Google. https://www.google.com/chrome/privacy/whitepaper.html
8. Firefox Telemetry API. (n.d.). https://firefox-source-docs.mozilla.org/toolkit/components/telemetry/
9. *Normandy — Normandy 0.1.0 documentation*. (n.d.). https://mozilla.github.io/normandy/
10. Leith, D. (2021). Web Browser Privacy: What Do Browsers Say When They Phone Home? *IEEE Access, 9,* 41615–41627. https://doi.org/10.1109/access.2021.3065243

11. Bareh, C. (2022). Privacy Evaluation of Popular Web Browsers from Information Seekers' Point of View.
12. Majeti, G., et al. (2023). Digital Forensic Advanced Evidence Collection and Analysis of Web Browser Activity. *ICST Transactions on Scalable Information Systems*, *10(5)*, 1–8. https://doi.org/10.4108/eetsis.3357
13. Golle, P., & Partridge, K. (2019). On the anonymity of home/work location pairs. *Pervasive Computing: 7th International Conference*, 390–397. https://doi.org/10.1007/978-3-642-01516-8_26
14. Caragiannis, I., & Tsitsoka, E. (2019). Deanonymizing Social Networks Using Structural Information. *Twenty-Eighth International Joint Conference on Artificial Intelligence, IJCAI-19*, 1213–1219. https://doi.org/10.24963/ijcai.2019/169
15. Shivangi, M., Lataben, G., & Harshil, J. (2023). Anomaly Detection to Prevent Sensitive Data Exposure Using GMM Clustering Model. *Proceedings of World Conference on Artificial Intelligence: Advances and Applications*. https://doi.org/10.1007/978-981-99-5881-8_35
16. Rautenstrauch, J., Pellegrino, G., & Stock, B. (2023). The Leaky Web: Automated Discovery of Cross-Site Information Leaks in Browsers and the Web. *IEEE Symposium on Security and Privacy (SP)*, 2744–2760. https://doi.org/10.1109/SP46215.2023.10179311
17. *TCPView for Windows - Sysinternals*. (n.d.). Microsoft Learn: Build skills that open doors in your career. https://learn.microsoft.com/en-us/sysinternals/downloads/tcpview
18. *Wireshark Download*. (n.d.). Wireshark. https://www.wireshark.org/download.html
19. Пономаренко, Д. (2023). *Стали відомі найпопулярніші браузери у світі та Україні у 2023 році*. Новини України - останні новини України сьогодні - УНІАН. https://www.unian.ua/techno/nazvano-naypopulyarnishi-brauzeri-u-sviti-ta-ukrajini-v-2023-roci-12201777.html
20. Задерейко, О., Логінова, Н., & Троянський, О. (2023) Аналіз потенційних витоків данних в пристроях комунікації. *Кіберпростір в умовах війни та глобальних викликів XXI століття: теорія та практика*, 105–108.
21. Zadereyko, O., et al. (2022). Research of potential data leaks in information and communication systems. *Radioelectronic and Computer Systems*, *(4)*, 64–84. https://doi.org/10.32620/reks.2022.4.05
22. *What is Googleusercontent Com.* (2023). Tips and Advices For technology. https://tips.msry.org/technology/what-is-googleusercontent-com/
23. *Googleusercontent.com can trip you up, if you disable third-party cookies.* (2012). Get more done, with Kerika. https://blog.kerika.com/googleusercontent-com-can-trip-you-up-if-you-disable-third-party-cookies/
24. Задерейко, О., Трофименко, О., Прокоп, Ю., Логінова, Н., Кухаренко, С., & Дика, А. (2022). Захист даних користувачів в інформаційних системах. *Сучасна спеціальна техніка, 1(68)*, 23–33. https://doi.org/10.36486/mst2411–3816.2022.1(68).

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

Zadereyko Olexander
PhD, Associate Professor, Associate Professor at the Department of Information Technologies
of the National University "Odessa Law Academy", Odesa, Ukraine,
ORCID 0000-0003-0497-9861
zadereyko@onua.edu.ua

Trofymenko Olena
PhD, Associate Professor, Associate Professor at the Department of Information Technologies
of the National University "Odessa Law Academy", Odesa, Ukraine,
ORCID 0000-0001-7626-0886
trofymenko@onua.edu.ua

Loginova Nataliia
PhD, Associate Professor, Head of the Department of Information Technologies
of the National University "Odessa Law Academy", Odesa, Ukraine,
ORCID 0000-0002-9475-6188
loginova@onua.edu.ua

Loboda Yuliia
PhD, Associate Professor, Associate Professor at the Department of Information Technologies
of the National University "Odessa Law Academy", Odesa, Ukraine,
ORCID 0000-0001-7083-552X
jul.loboda@gmail.com

Prokop Yuliia
PhD, Associate Professor, Associate Professor at the Department of Software engineering
of the Odessa Polytechnic National University, Odesa, Ukraine,
ORCID 0000-0002-6608-3668
prokop.y.v@op.edu.ua

ANALYSIS OF POTENTIAL PERSONAL DATA LEAKS IN WEB BROWSERS

Abstract. The distribution of the vast majority of web browsers is actively encouraged by their free use. This is a common practice of web browser developers, as it provides them with great opportunities for their distribution. The flip side of this process is the collection of personal data by web browser developers that the user does not control. The collected data is automatically transferred to leading IT companies such as Google, Microsoft, and Cloudflare, which collect, accumulate, process, and monetize the users' data in an automated manner. This leads to the fact that any web browser user is profiled in the services of leading IT companies, which receive complete information about the user's actions on the Internet. This state of affairs contradicts Article 32 of the Constitution of Ukraine, which guarantees the right to privacy and the basic provisions of the Law of Ukraine "On Personal Data Protection". The study involved long-term recording and subsequent analysis of the network traffic of Ukraine's most popular web browsers: Google Chrome, Microsoft Edge, Mozilla Firefox, and Opera. The peculiarity of the study was to obtain network traffic initiated by web browsers that have been active for a long time. To increase the reliability, the data on network connections of web browsers were obtained using two independent software tools for monitoring traffic on the network interface of a communication device. The analysis of network connections of web browsers made it possible to establish close ties between companies developing free web browsers and leading IT companies that monopolistically control the actions of users in the Internet space. This state of affairs contradicts the legal norms on ensuring the privacy of web browser users in the context of using their data without their knowledge and consent. This can be prevented using network screens operating at Layers 3, 4, and 7 of the TCP/IP stack OSI model.

Keywords: network traffic analysis; web browser network traffic; personal data collection; web browser; personal data leaks in web browsers.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Halle, M., Demeusy, V., & Kikinis, R. (2017). The open anatomy browser: a collaborative web-based viewer for interoperable anatomy atlases. *Frontiers in neuroinformatics, 11*. https://doi.org/10.3389/fninf.2017.00022
2. Nomoto, K., et al. (2023). Understanding the Inconsistencies in the Permissions Mechanism of Web Browsers. *Journal of Information Processing, 31,* 620–642. https://doi.org/10.2197/ipsjjip.31.620
3. Pau, K., et al. (2023). The Development of a Data Collection and Browser Fingerprinting System. *Sensors, 23, 3087.* https://doi.org/10.3390/s23063087
4. *Overview. Safe Browsing APIs (v4).* (n.d.). Google for Developers. https://developers.google.com/safe-browsing/v4
5. Cai, H., et al. (2023). Toward Correlated Data Trading for Private Web Browsing History. *IEEE Internet of Things Journal, 10(7),* 5859–5872. https://doi.org/10.1109/JIOT.2023.3237707
6. *Autoupdating. Apps. Chrome for Developers*. (n.d.). Chrome for Developers. https://developer.chrome.com/apps/autoupdate
7. *Google Chrome Privacy Whitepaper*. (n.d.). Google. https://www.google.com/chrome/privacy/whitepaper.html
8. Firefox Telemetry API. (n.d.). https://firefox-source-docs.mozilla.org/toolkit/components/telemetry/
9. *Normandy — Normandy 0.1.0 documentation*. (n.d.). https://mozilla.github.io/normandy/
10. Leith, D. (2021). Web Browser Privacy: What Do Browsers Say When They Phone Home? *IEEE Access, 9,* 41615–41627. https://doi.org/10.1109/access.2021.3065243
11. Bareh, C. (2022). Privacy Evaluation of Popular Web Browsers from Information Seekers' Point of View.
12. Majeti, G., et al. (2023). Digital Forensic Advanced Evidence Collection and Analysis of Web Browser Activity. *ICST Transactions on Scalable Information Systems, 10(5),* 1–8. https://doi.org/10.4108/eetsis.3357
13. Golle, P., & Partridge, K. (2019). On the anonymity of home/work location pairs. *Pervasive Computing: 7th International Conference,* 390–397. https://doi.org/10.1007/978-3-642-01516-8_26
14. Caragiannis, I., & Tsitsoka, E. (2019). Deanonymizing Social Networks Using Structural Information. *Twenty-Eighth Int. Joint Conf. on Artificial Intell. 19,* 1213–1219. https://doi.org/10.24963/ijcai.2019/169
15. Shivangi, M., Lataben, G., & Harshil, J. (2023). Anomaly Detection to Prevent Sensitive Data Exposure Using GMM Clustering Model. *Proceedings of World Conference on Artificial Intelligence: Advances and Applications*. https://doi.org/10.1007/978-981-99-5881-8_35
16. Rautenstrauch, J., Pellegrino, G., & Stock, B. (2023). The Leaky Web: Automated Discovery of Cross-Site Information Leaks in Browsers and the Web. *IEEE Symposium on Security and Privacy (SP),* 2744–2760. https://doi.org/10.1109/SP46215.2023.10179311
17. *TCPView for Windows - Sysinternals*. (n.d.). Microsoft Learn: Build skills that open doors in your career. https://learn.microsoft.com/en-us/sysinternals/downloads/tcpview
18. *Wireshark Download*. (n.d.). Wireshark. https://www.wireshark.org/download.html
19. Ponomarenko, D. (2023). *Staly vidomi naipopuliarnishi brauzery u sviti ta Ukraini u 2023 rotsi.* Novyny Ukrainy - ostanni novyny Ukrainy sohodni - UNIAN. https://www.unian.ua/techno/nazvano-naypopulyarnishi-brauzeri-u-sviti-ta-ukrajini-v-2023-roci-12201777.html
20. Zadereiko, O., Lohinova, N., & Troianskyi, O. (2023) Analiz potentsiinykh vytokiv dannykh v prystroiakh komunikatsii. *Kiberprostir v umovakh viiny ta hlobalnykh vyklykiv KhKhI stolittia: teoriia ta praktyka,* 105–108.
21. Zadereyko, O., et al. (2022). Research of potential data leaks in information and communication systems. *Radioelectronic and Computer Systems, (4),* 64–84. https://doi.org/10.32620/reks.2022.4.05
22. *What is Googleusercontent Com.* (2023). Tips and Advices For technology. https://tips.msry.org/technology/what-is-googleusercontent-com/
23. *Googleusercontent.com can trip you up, if you disable third-party cookies.* (2012). Get more done, with Kerika. https://blog.kerika.com/googleusercontent-com-can-trip-you-up-if-you-disable-third-party-cookies/
24. Zadereiko, O., et al. (2022). Zakhyst danykh korystuvachiv v informatsiinykh systemakh. *Suchasna spetsialna tekhnika, 1(68),* 23–33. https://doi.org/10.36486/mst2411–3816.2022.1(68).