



Національний університет «Одеська юридична академія»
Факультет кібербезпеки та інформаційних технологій
Наукове товариство молодих вчених, аспірантів і студентів



**ВСЕУКРАЇНСЬКА
НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ**

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

м. Одеса

29 листопада 2019 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
НАУКОВЕ ТОВАРИСТВО МОЛОДИХ ВЧЕНИХ,
АСПІРАНТІВ ТА СТУДЕНТІВ



КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

МАТЕРІАЛИ
Всеукраїнської науково-практичної конференції

29 листопада 2019 року

Одеса
2019

УДК 004.056(063)
К38

*Друкується за наказом ректора
Національного університету «Одеська юридична академія»
В. Є. Загороднього
(наказ №2410-62 від 2 жовтня 2019 року)*

Відповідальний редактор – в.о. декана факультету кібербезпеки та інформаційних технологій, доцент О. В. Дикий.

Укладачі:

Кузьма Яна Іванівна – диспетчер деканату факультету кібербезпеки та інформаційних технологій.

Стоянова Тетяна Федорівна – диспетчер деканату факультету кібербезпеки та інформаційних технологій.

Пастернак Юрій Юрійович – студент 3 курсу факультету кібербезпеки та інформаційних технологій.

Матеріали видано в авторській редакції. Повну відповідальність за достовірність та якість поданого матеріалу несуть учасники конференції, їхні наукові керівники, рецензенти, які рекомендували ці матеріали до друку.

Кібербезпека в сучасному світі: матеріали всеукраїнської науково-практичної конференції (м. Одеса, 29 листопада 2019 р.) / за ред. О.В. Дикого ; уклад.: Я.І. Кузьма, Т.Ф. Стоянова, Ю.Ю. Пастернак. – Одеса: Видавничий дім «Гельветика», 2019. – 332 с.

ISBN 978-966-916-949-5

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

Подані матеріали конференції 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 978-966-916-949-5

© НУ «Одеська юридична академія», 2019
© Факультет кібербезпеки та інформаційних технологій НУ «ОЮА», 2019

Задержко А. В.

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

Троянский А. В.

Одесский национальный политехнический университет, директор института информационной безопасности, радиоэлектроники и телекоммуникаций, кандидат технических наук, доцент

ЗАЩИТА ОТ СКРЫТОГО СБОРА ПЕРСОНАЛЬНЫХ ДАННЫХ ПОЛЬЗОВАТЕЛЕЙ ПРИ ВЕБ-СЕРФИНГЕ В ИНТЕРНЕТ

В настоящее время, такое понятие как приватность пользователя в сети интернет неразрывно связано со структурно организованным сбором персональных данных пользователей, посредством последовательного внедрения современных интернет-технологий [1]. С их стремительным развитием становится все труднее препятствовать сбору данных о пользователях, которые осуществляют веб-серфинг интернет-ресурсов.

Большинство интернет-ресурсов, осуществляют сбор и накопление данных о поведении пользователей. К этим данным можно отнести такую информацию:

- с какого IP-адреса пользователь выполнил посещение интернет-ресурса;
- с какого интернет-ресурса был выполнен переход;
- название и версию веб-браузера;
- название, версию операционной системы устройства пользователя;
- разрешение экрана устройства пользователя;
- какие страницы просматривались пользователем;
- сколько времени пользователь провел на просматриваемой странице интернет-ресурса;
- осуществлялся ли поиск по интернет-ресурсу;
- поиск какой информации выполнялся на интернет-ресурсе.

Сбор этих данных осуществляется с помощью различных сервисов сбора статистики, используемых владельцами интернет-ресурсов.

Сервисы сбора статистики на интернет-ресурсах можно условно разделить на два типа:

- внешние (корпоративные – Google analytics, Easycounter, Яндекс Метрика, Liveinternet, Hotlog, Rambler TOP100, Topmail.ru, и т.д.);
- внутренние (встроенные непосредственно в CMS интернет-ресурса).

Обработка сервисами статистики собираемых данных, позволяет рассчитать такие показатели для каждого интернет-ресурса:

- количество просмотренных страниц;
- количество посетителей в сутки, неделю, месяц;
- усреднённый показатель отказов от страницы / интернет-ресурса;
- показатель отказов для каждой страницы в отдельности;
- средняя длительность просмотра каждой страницы;
- относительная доля выходов с каждой страницы;
- среднее время пребывания пользователя;
- среднее время пребывания на ресурсе;
- доля новых пользователей ;
- доля постоянных пользователей ;
- демографические/гендерные показатели пользовательской аудитории;
- рей тинг посещаемости в тематическом сегменте.

Накапливаемые результаты обработки выше перечисленных данных представляют ценную информацию для правительственных организаций , спецслужб [2], ИТ-корпораций [3], рекламных компаний [4], маркетологов и т. д., так как позволяют осуществлять не только негласный мониторинг, но и манипулятивное управление интернет-аудиторией в различных тематических сегментах, по факту в любом государстве [5].

С другой стороны, нельзя обойти вниманием, ряд свидетельств, ставших известными мировой общественности, показывающих, что массовое использование пользователями бесплатных веб-браузеров от компаний Google, Microsoft, Apple способствует активному участию в программах негласного сбора информации (PRISM, Upstream и т.д.) [6].

Эти обстоятельства диктуют необходимость выработки комплекса мер защиты пользователей от несанкционированного сбора конфиденциальной информации: об их интересах, действиях, возможных предпочтениях, и самое главное – возможностях прогнозирования их поведения в будущем.

Для решения этой задачи на практике применяются веб-браузеры с повышенной степенью защищенности (анонимности) от сбора персональных данных пользователя [7]. К числу наиболее известных из них относится веб-браузер TOR PROJECT, основанный на специальной версии веб-браузера Mozilla Firefox с расширенным сроком поддержки (Extended Support Release (ESR)) [8]. Основным его достоинством является, повышенный уровень безопасности, обусловленный применением специальных мер усиления приватности пользователя:

- не сохраняется история посещений интернет-ресурсов;
- cookies-файлы используются только на время сеанса (в режиме «по-умолчанию»);
- применяются встроенные расширения для безопасного просмотра интернет-ресурсов HTTPS-Everywhere, NoScript, Torbutton;
- применяются транспортные модули для деблокировки IP-адресов сетей Tor с помощью сервисов фильтрации трафика: Obfs3proxy, Obfs4proxy, meek, FTE;
- реализован контроль за перемещением информации, ассоциированной с пользователем, посредством передачи запрашиваемого содержимого интернет-ресурсов через различные цепочки серверов;
- встроена защита от передачи информации о фактическом размере экрана устройства пользователя.

Отличительной особенностью веб-браузера TOR PROJECT, значительно повышающей приватность пользователя является наличие встроенного расширения NoScript Security Suite [9]. Его возможности включают блокирование сценариев JavaScript, Flash, WebGL, медиа-контента, до тех пор, пока пользователь не разрешит их исполнение на посещаемом интернет-ресурсе. Важной особенностью этого расширения является возможность защиты пользователя от XSS атак, с возможностью формирования отдельных списков интернет-ресурсов, для которых необходима функциональность, схожая с ее проявлением.

Фиксация процесса сбора персональных данных при веб-серфинге

Для анализа работы расширения NoScript Security Suite зафиксируем список обнаруженных доменов, которые блокируются им при обращении к авторскому ресурсу <https://zadereyko.info> (см. табл. 1].

Таблица 1

ИССЛЕДУЕМЫЙ ИНТЕРНЕТ-РЕСУРС			
ЗАБЛОКИРОВАННЫЕ ДОМЕНЫ			
УСТАНОВЛЕННЫЕ	СЕРВИСЫ СБОРА СТАТИСТИКИ		
	Корпоративные	Яндекс Метрика	yandex.ru, yastatic.net
		Google Analytics	google-analytics.com, googletagmanager.com
		Sape RTB	acint.net, sape.ru
		Relap	relap.io
		Google Adsense	googlesyndication.com
	Виджеты соц. сетей	Фэйсбук	facebook.com, facebook.net
		Твиттер	twitter.com
		Вконтакте	vk.com
НЕ УСТАНОВЛЕННЫЕ	Сторонние домены	Тизерные, маркетинговые интернет-платформы	dircont3.com
			1dmp.io
			directadvert.ru
		Поисковая система	gstatic.com
			google.com

Следует отметить, что в списке заблокированных доменов присутствуют домены, к которым авторский интернет-ресурс не имеет никакого отношения (см. таблицу 1).

Анализ заблокированных сторонних доменов

В результате выполненного сбора информации о сторонних доменах удалось установить следующее:

Dircont3.com – домен находится под управлением серверов ns-381.awsdns-47.com, ns-807.awsdns-36.net, ns-1239.awsdns-26.org, ns-1842.awsdns-38.co.uk, принадлежащих компании Amazon. Имеет почтовый сервер **mail.dircont3.com**.

Directadvert.ru – домен одной из крупнейших тизерных систем СНГ, которая входит в состав компании «Поисковые технологии», принадлежащая компании «Ашманов и Партнеры» и инвестиционному холдингу «Финам».

Google.com – домен поисковой системы интернета, принадлежащий корпорации Google Inc.

Gstatic.com - домен, принадлежит ИТ-корпорации Google Inc, управляет статическим контентом (проиндексированными изображениями с интернет-ресурсов) для предварительного показа пользователю до его перехода на эти интернет-ресурсы.

1dmp.io – домен выполняет переадресацию на домен *hermann.ai* (data marketing platform), заявляющий себя, как отказоустойчивая, масштабируемая платформа для управления и обработки данных в режиме реального времени для розничной торговли и электронной коммерции.

Выводы и рекомендации по защите персональных данных пользователей при вебсерфинге

Выполненный анализ перечня заблокированных доменов позволяет сделать следующие выводы:

1. Владельцы хостингов участвуют в организации сбора персональных данных пользователей сторонним интернет-сервисам сбора статистики.

2. Владельцы интернет-ресурсов, расположенных на таких хостингах способствуют сбору персональных данных о посетителях своих интернет-ресурсов сторонним интернет-сервисам сбора статистики.

3. Пользователям, необходимо принимать меры для блокировки сбора персональных данных:

- выполнять установку в веб-браузеры дополнительных расширений NoScript Security Suite и/или uMatrix для веб-браузеров.
- выполнять «тонкую» настройку максимального уровня приватности в расширениях NoScript Security Suite[9] и uMatrix [10], позволяющую осуществить блокировку доменов маркетинговых интернет-платформ.

Список использованных источников:

1. Приватность, которую мы почти проиграли. - [Электронный ресурс]. – Режим доступа:
2. Как ЦРУ создавало Google. - [Электронный ресурс]. – Режим доступа: http://zadereyko.info/istoricheskie_faktu/kak_cry_sozdavalo_google.htm.
3. Google: запретная черта. - [Электронный ресурс]. – Режим доступа: <https://zh-cn.facebook.com/Zadereyko.Info/videos/google-запретная-черта/460964081413001/>.
4. Анализ «больших данных» выводит персонализированную рекламу на новый уровень. http://zadereyko.info/sbor_informacii_o_polzovateley/personalizirovannaya_reklama_dla_polzovateley.htm.
5. Как высокотехнологичные корпорации программируют людей. - [Электронный ресурс]. – Режим доступа: http://zadereyko.info/manipulasii_obshestvom/kak_korporacii_programmiruyut_ludey.htm.
6. Самые странные программы АНБ. - [Электронный ресурс]. – Режим доступа: http://muz4in.net/news/samye_strannye_programmy_anb/2019-09-01-50015.
7. Обзор защищенных браузеров. - [Электронный ресурс]. – Режим доступа: https://www.anti-malware.ru/analytics/Market_Analysis/secure-browsers.
8. Реальная анонимность в Tor: как правильно его настроить. - [Электронный ресурс]. – Режим доступа: http://zadereyko.info/anonimnost_v_seti/anonimnost_v_tor.htm.
9. Как использовать NoScript для Firefox. - [Электронный ресурс]. – Режим доступа: <https://www.comss.ru/page.php?id=5283>.
10. Как использовать uMatrix для блокировки рекламы и нежелательного контента. - [Электронный ресурс]. – Режим доступа: <https://www.comss.ru/page.php?id=4652>.

Наукове видання

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

МАТЕРІАЛИ Всеукраїнської науково-практичної конференції

29 листопада 2019 року, м. Одеса

Верстка – О. С. Данильченко

Підписано до друку 7.10.2019. Формат 60х84/16. Папір офсетний . Гарнітура Cambria. Цифровий друк. Умовно-друк. арк. 19,30. Тираж 150. Замовлення № 1119-229. Ціна договірна. Віддруковано з готового оригінал-макета.

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