DOI https: //doi.org/10.26486/mst2411-2816
DOI (Issue): https: //doi.org/10.26486/mst2411-2816.2021.2(66)

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ДЕРЖАВНИЙ НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ

СУЧАСНА СПЕЦІАЛЬНА ТЕХНІКА

НАУКОВО-ПРАКТИЧНИЙ ЖУРНАЛ

№ 3(66), 2021

ВИДАЄТЬСЯ ЩОКВАРТАЛЬНО

ЗАСНОВНИК

Державний науково-дослідний інститут МВС України; Національний авіаційний університет; Національна академія внутрішніх справ

НАКАЗОМ

МОН України від 17.03.2020 № 409 науково-практичний журнал "Сучасна спеціальна техніка" включено до Переліку наукових фахових видань України відповідно до списку згідно з додатком 1 (категорія "Б")

ЗАРЕЄСТРОВАНО

Міністерством юстиції України 13 лютого 2015 року

Свідоцтво – серія КВ № 21221-11021Р

Науково-практичний журнал "Сучасна спеціальна техніка" внесено до переліку міжнародної науковометричної бази

Index Copernicus International Journal Master List

Рекомендовано до друку рішенням Вченої ради ДНДІ МВС України
(протокол від 27.10.2021 № 7)

Науково-практичний журнал посів ІІІ місце в конкурсі на краще наукове періодичне видання в системі МВС України у 2017 році та І місце у 2020 році

Київ 2021

DOI https: //doi.org/10.?6486/mst2411-?816
DOI (Issue): https: //doi.org/10.?6486/mst2411-?816.2021.?(66)

MINISTRY OF INTERNAL AFFAIRS OF UKRAINE
STATE RESEARCH INSTITUTE

MODERN SPECIAL TECHNICS

SCIENTIFIC AND PRACTICAL JOURNAL
№ 3(66), 2021
ISSUED FOUR TIMES A YEAR

FOUNDER
State Research Institute MIA Ukraine; National Aviation University; National Academy of Internal Affairs
BY ORDER
No 409, dated 17.03.2020 scientific and practical journal "Modern Special Technics" was included into the List of Professional Academic Journals of Ukraine according to the List on Supplement 1 (Category "B")
REGISTERED
by Ministry of Justice of Ukraine 13.02.2015
Certificate-series KB No 21221-11021 P
Scientific and Practical Journal "Modern Special Technics" has been included into International Scientometric Base **Index Copernicus International Journal Master List**

Recommended by State Research Institute's Scientific Council
(Record No 7 dated 27.10.2021)

The scientific and practical journal won the third place in the competition for the best scientific periodical in the system of the Ministry of Internal Affairs of Ukraine in 2017 and the first prize in 2020

For the accuracy of the posted material, it is necessary to bring an author reviewer.

When reprinting the materials, the reference to the scientific and practical journal "Modern Special Technics" is obligatory

Kyiv 2021

ISSN 2411-3816 (Print)

СУЧАСНА СПЕЦІАЛЬНА ТЕХНІКА
MODERN SPECIAL TECHNICS

DOI (Issue): https: //doi.org/10.36486/mst2411–3816.2021.3(66)

Issue 3(66) 2021

З М І С Т

СИСТЕМИ ТА МЕТОДИ ОБРОБКИ ІНФОРМАЦІЇ

ІНФОРМАЦІЙНЕ ТА НОРМАТИВНЕ ЗАБЕЗПЕЧЕННЯ НАУКОВОЇ ДІЯЛЬНОСТІ

ТЕХНІКА, ЗБРОЯ, ТРАНСПОРТ ТА ОБМУНДИРУВАННЯ

СПЕЦІАЛЬНІ РОЗРОБКИ

ISSN 2411-3816 (Print)

СУЧАСНА СПЕЦІАЛЬНА ТЕХНІКА
MODERN SPECIAL TECHNICS

DOI (Issue): https: //doi.org/10.36486/mst2411–3816.2021.3(66)

Issue 3(66) 2021

CONTENTS

SYSTEMS AND METHODS OF INFORMATION PROCESSING

INFORMATIONAL AND REGULATORY SUPPORT OF SCIENTIFIC ACTIVITIES

EQUIPMENT, ARMS, TRANSPORT AND UNIFORMS

SPECIAL PRODUCTS

УДК 004.738.2

Задерейко Олександр Владиславович, кандидат технічних наук, доцент, доцент кафедри інформаційних технологій, Національний університет "Одеська юридична академія", м. Одеса, Україна, ORCID ID 0000-0003-0497-9861
Трофименко Олена Григорівна, кандидат технічних наук, доцент, доцент кафедри інформаційних технологій, Національний університет "Одеська юридична академія", м. Одеса, Україна, ORCID ID 0000-0001-7626-0886
Прокоп Юлія Віталіївна, кандидат історичних наук, старший викладач кафедри інформаційних технологій, Державний університет інтелектуальних технологій та зв'язку, м. Одеса, Україна, ORCID ID 0000-0002-6608-3668
Логінова Наталія Іванівна, кандидат педагогічних наук, доцент, завідувачка кафедри інформаційних технологій, Національний університет "Одеська юридична академія", м. Одеса, Україна, ORCID ID 0000-0002-9475-6188
Кухаренко Сергій Вікторович, кандидат технічних наук, доцент кафедри кібербезпеки, Національний університет "Одеська юридична академія", м. Одеса, Україна, ORCID ID 0000-0001-7100-6408

АНАЛІЗ ВИТОКІВ ДАНИХ У ІНФОРМАЦІЙНИХ СИСТЕМАХ

У статті розглянуто питання забезпечення приватності користувачів інформаційних систем, представлених стаціонарними та мобільними пристроями комунікації. Показано, що наявна організація комунікації DNS трафіку інформаційної системи несе загрозу приватності користувача. Виконано фіксацію і аудит DNS трафіку пристроїв комунікації з цифровим простором. Установлено, що при виконанні блокування сторонніх з'єднань системного і прикладного програмного забезпечення пристроїв комунікації працездатність інформаційної системи не порушується. Визначено, що ідентифікація пристрою комунікації пов'язана із процесом збору інформації про апаратне та програмне забезпечення пристрою комунікації.

***Ключові слова**: DNS запит, DNS сервер, витоки даних, DNS трафік, аналіз витоків даних, пристрій комунікації, ідентифікація пристроїв комунікації.*

В статье рассмотрены вопросы обеспечения приватности пользователей информационных систем, представленных стационарными и мобильными устройствами коммуникации. Показано, что существующая организация коммуникации DNS траффика информационной системы несет угрозу приватности пользователя. Выполнены фиксация и аудит DNS траффика устройств коммуникации с цифровым пространством. Установлено, что при выполнении блокировки сторонних соединений системного и прикладного программного обеспечения устройств коммуникации работоспособность информационной системы не нарушается. Определено, что идентификация устройства коммуникации связана с процессом сбора информации об аппаратном и программном обеспечении устройства коммуникации.

Ключевые слова: *DNS запрос, DNS сервер, утечки данных, DNS траффик, анализ утечек данных, устройство коммуникации, идентификация устройств коммуникации.*

Вступ

Сучасні тенденції несанкціонованого збору, накопичення та обробки даних з комп'ютерів користувачів, долучених до інтернет-простору, дедалі частіше викликають занепокоєння не лише у громадських правозахисник організацій, а й у дедалі більшої кількості користувачів. Енергійні зусилля високотехнологічних ІТ-компаній неухильно призводять до негласної монополізації цифрового ринку цих користувачів. При цьому регуляторна роль різних державних інституцій у питаннях дотримання прав на приватність життя користувачів, як-от: таємниця листування, інформація про відвідувані адреси, імена користувачів і паролі, пошукові запити, неухильно знижується.

Такий стан справ природним чином зумовлює нагальну потребу у проведенні поглибленого аналізу принципів обміну даними користувачів у цифровому просторі. Результати такого аналізу дозволять значно підвищити приватність і анонімність користувачів і, як наслідок, знизити вплив монополістів цифрового ринку на їхні рішення та поведінкові переваги.

Метою роботи є аудит трафіка класичної інформаційної системи користувача та аналіз принципів ідентифікації пристроїв комунікації в цифровому просторі.

Для досягнення поставленої мети необхідно вирішити низку завдань:

- проаналізувати принципи обміну даними між типовою інформаційною системою користувача й цифровим простором інтернет;
- проаналізувати принципи ідентифікації пристроїв комунікації в цифровому просторі;
- виконати фіксацію вихідних і вхідних з'єднань інформаційної системи з цифровим простором;
- провести аналіз з'єднань інформаційної системи користувача з цифровим простором;
- визначити критерії, що дозволяють класифікувати з'єднання інформаційної системи з цифровим простором.

Основна частина

1. Принцип обміну даними між ІС і цифровим простором

Класичне визначення комп'ютерної інформаційної системи (ІС) визначає її як систему, призначену для зберігання, пошуку й обробки інформації, і відповідні організаційні ресурси (людські, технічні, фінансові ресурси тощо), які забезпечують

і поширюють інформацію [1]. У прикладному сенсі аналізованої проблематики будемо розглядати ІС як апаратно-програмний комплекс, призначений для реалізації вимог користувачів у питаннях пошуку, отримання і зберігання інформації. Основним завданням таких ІС є задоволення інформаційних потреб користувачів у рамках вибраної ними предметної області. Найбільш масового поширення набули настільні та мобільні ІС, у яких усі апаратні і програмні компоненти для зв'язку розміщені в одному пристрої (комп'ютер, смартфон). Надалі називатимемо їх пристроями комунікації (ПрК) (рис. 1).

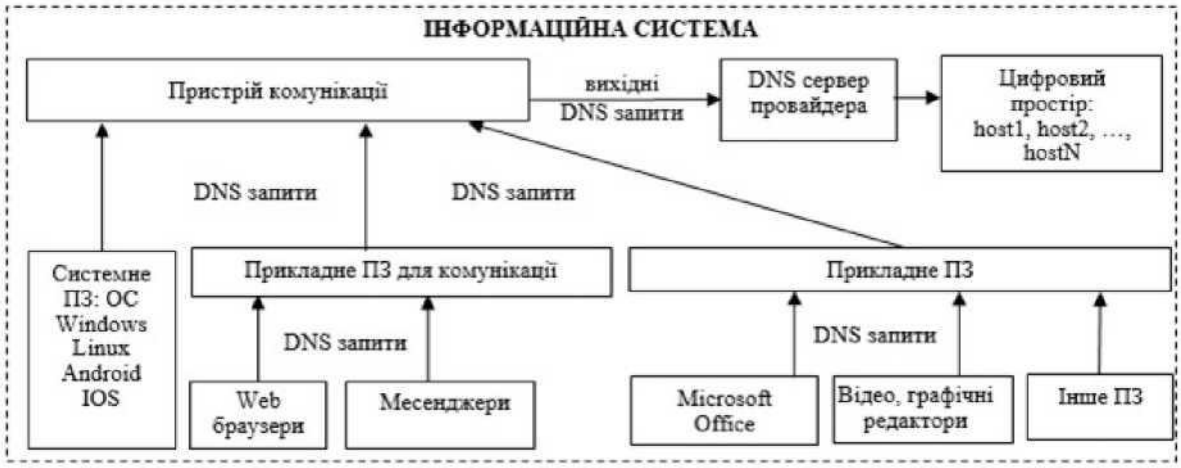

Рис. 1. Взаємодія модулів ІС із цифровим простором

Сучасний цифровий простір забезпечує вільний транскордонний обмін даними між ПрК користувача й хостами різного призначення. Фізичне підключення ПрК користувача (клієнта DNS) до цифрового простору й його подальше звернення до різних ресурсів починається з відсилання DNS запитів на DNS сервери. Детальний аналіз схеми обміну даними ПрК засвідчує, що всі запити клієнтів DNS фіксуються в журналах DNS сервера провайдера. їх аналіз дає вичерпну інформацію для провайдера і контролюючих його державних структур про дії користувача або його ПрК у цифровому просторі. Саме ця обставина дозволяє розглядати DNS запити користувачів як дані користувачів, до збирання, зберігання та аналізу яких з кожним роком виявляють дедалі більший інтерес ІТ-компанії і спецслужби різного призначення в усіх державах [2].

Обробка та аналіз отриманих даних виконується в автоматичному режимі й дозволяє однозначно встановити [3-5]:

- IP-адресу, з якої ПрК "заходить" в інтернет;
- операційну систему (ОС), під керуванням якої працює ПрК;
- встановлене прикладне програмне забезпечення (ПЗ);
- роздільну здатність екрану ПрК;
- пошукові запити користувача;
- сферу споживання;
- стосунки з фінансовими установами;
- час перебування на інтернет-сервісах;

- тематику переглянутого контенту;
- демографічні / гендерні показники користувальницької аудиторії;
- вікову групу, до якої можна віднести користувача, тощо.

Результати обробки таких даних нерозривно пов'язані з прив'язкою до ПрК, з якого вони взяті. Реалізація цього процесу ґрунтується на виконанні процесу ідентифікації ПрК.

2. Принципи ідентифікації пристроїв комунікації

У цифровому просторі формування цифрового відбитка ПрК користувача нерозривно пов'язане з його однозначною ідентифікацією. Ідентифікація ПрК виконується як активними, так і пасивними методами [6, 7].

Пасивна ідентифікація заснована на принципах збору інформації без відсилання спеціалізованих запитів до ПрК. Обов'язкові дані, що відправляються кожним ПрК містять інформацію про ОС, встановлене ПЗ, мережеві адаптери (MAC-адреса тощо).

Активна ідентифікація ґрунтується на принципах активної мережної взаємодії, які реалізуються через запуск JS-кодів з віддалених хостів. До одержуваної інформації можна віднести: розміри вікна застосунку, встановлений набір шрифтів, набір плагінів у веббраузері, мову ОС і часовий пояс, дані про апаратну конфігурацію ПрК тощо.

По суті, при ідентифікації ПрК виконується фіксація таких даних: MAC адреси мережевих адаптерів, версії ОС і встановленого ПЗ, за допомогою якого здійснюється комунікація з цифровим простором (веббраузери, месенджери тощо). Усі ці дані формують унікальний цифровий відбиток ПрК (рис. 2).

Рис. 2. Формування цифрового відбитка ПрК

Формування цифрового відбитка ПрК ґрунтується на колекціях наборів зібраних з нього даних (рис. 2), які об'єднуються і перетворюються на хеш-функ- цію - унікальний ID, який зберігається у зовнішніх базах даних, що переважно належать IT-компаніям. Одержані дані є унікальними і знеособленими для кожного ПрК [8].

Наявність цифрової камери в ПрК і, як наслідок, одержувані за її допомогою цифрові знімки, розміщувані в цифровому просторі, значно спрощують процес ідентифікації ПрК. Це пояснюється тим, що кожна цифрова камера має свої унікальні характеристики: рівень цифрового шуму й частотно контрастну характеристику оптичної системи й фотосенсора [9].

3. Фіксація вихідних з'єднань інформаційної системи з цифровим простором

Як показали численні дослідження, ПрК при підключенні до цифрового простору, його системне і прикладне ПЗ встановлює вихідні з'єднання не тільки з хостами своїх розробників, а й зі сторонніми хостами, які не мають до них прямого стосунку. Якщо з'єднання ПЗ з хостами розробників можна пояснити збором даних про його працездатність і режими функціонування, перевіркою ліцензійних умов використання, збором телеметричних даних або пошуком оновлених версій ПЗ, то з'єднання зі сторонніми хостами виглядають на цьому тлі більш ніж підозріло [10-12]. Тим більше, як засвідчує практика блокування таких з'єднань, працездатність ПЗ не порушує [13]. Так, наприклад, в мобільних ОС більшість застосунків при встановленні вимагають доступ до списку контактів, цифрової камери, файлової (фото) галереї тощо. Без цих дозволів такі застосунки часто неможливо навіть встановити, іноді вони частково або повністю втрачають свою функціональність. Саме така позиція розробників мобільних застосунків дозволяє отримати їм легальний доступ до широкого спектра даних користувачів. Про перелік збираних даних можна дізнатися з ліцензійної угоди до використовуваного ПЗ, яку більшість користувачів не вивчають й апріорі приймають її умови для отримання можливості його експлуатації.

Більше того, блокування більшості з'єднань системного і прикладного ПЗ з хостами розробників також не впливає на їх працездатність і функціональність.

Усі ці обставини обумовлюють потребу в:

- проведенні експериментальної фіксації всіх вихідних з'єднань ПрК з цифровим простором, що відбуваються під керуванням мобільних і стаціонарних систем;
- виконання їх аналізу, що дозволить класифікувати з'єднання на функціональні і сторонні. Класифікацію з'єднань варто провести на підставі пропонованих критеріїв:

1) під функціональними з'єднаннями розумітимемо такі, що забезпечують нормальне функціонування системного та прикладного ПЗ, а їх блокування призводить до порушення або втрати його працездатності;

2) під сторонніми з'єднаннями розумітимемо такі, що встановлюються з хостами, які не мають прямого стосунку до офіційних хостів системного і прикладного ПЗ.

Для дослідження ПрК під керуванням мобільної ОС Android і ПрК під керуванням стаціонарних ОС Windows 7/10 були використані такі засоби дослідження: мережевий екран No Root Firewall (ОС Android) [14]; розширення вбудованого мережевого екрану Windows Firewall Control (ОС Windows 7/10) [15], аналізатор мережевого трафіка Wireshark (ОС Windows 7/10) [16]. Класифікація з'єднань ПрК на базі пропонованих критеріїв була виконана на основі результатів експериментальної перевірки працездатності системного і прикладного ПЗ ПрК при виконанні послідовного примусового блокування його з'єднань. Отримані результати систематизовані і подані в табл. 1-4.

Таблиця 1

Функціональні і сторонні з'єднання ПрК під керуванням ОС Android

Системне і прикладне ПЗ		Вхідні / вихідні з'єднання (IP-адреси / домени хостів)		IT- компанії	Блокування функціо-нальних з'єднань (+/-)	Блокування сторонніх з'єднань (+/-)	Працездат-ність ПЗ (+/-)
		функціональні	сторонні				
Месенджери	Telegram	149.154.167.50:443	dns.google:443	Telegram Messenger Inc	—	+	+
		149.154.167.151:443	149.154.167.*:5222				
		149.154.167.96:443	149.154.165.*:5222				
		149.154.167.91:443	91.108.56.192:5222				
		149.154.167.55:443	104.16.248.249:443				
		149.154.167.51:443	196.55.217.71:443				
			5.28.194.8:443				
			5.28.194.8:5222				
	WhatsApp		* .static .sl-reverse .com:443	Facebook	-	+	+
		*.fbcdn.net:443	*.1e100.net:443				
			157.240.14.53:5222				
			169.63.76.65:5222				
	Viber	185.151.204.13:443	*.deploy.static. akamaitechno	Rakuten	-	+	+
		185.151.204.7:443	*.bc. googleusercontent. com:443				
		185.151.204.15:443	*.r.cloudfront.net:443				
		185.151.204.9:443	s3-website.eu-central-1 .amazonaws.com:80				
			*.1e100.net:443				
			52.0.252.2:5242				
Мобільні застосунки	Facebook	*.facebook.com:443 edge- star-mini- shv-01- waw1 .facebook.com:443	*.compute-1 .amazonaws.com:4244 104.16.221.74:443	Facebook	-	+	+
		edge-star-shv-01-waw1 .facebook.com:443	104.20.110.39:443				
		edge-mqtt-shv-01-waw1 .facebook.com:443	91.198.36.60:443				
		edge-mqtt-mini-shv-01-waw1 .facebook.com:443	104.16.199.73:443				
		*.fbcdn.net:443	*.utel.net.ua:443				
		facebook.dataline.net.ua:443	*.vps-default-host.net:443				
		edge-star-mini-shv-01-frx5.facebook.com:443	ua*.host.hit.gemius.pl:443				
		edge-mqtt-mini-shv-01-frx5.facebook.com:443	es49.mirohost.net:443				

Системне і прикладне ПЗ		Вхідні / вихідні з'єднання (IP-адреси / домени хостів)		IT- компанії	Блокування функціо-нальних з'єднань (+/-)	Блокування сторонніх з'єднань (+/-)	Працездат-ність ПЗ (+/-)
		функціональні	сторонні				
		edge-star-shv-01-otp1.facebook.com: 443	*.r. cloudfront. net :443				
		edge-star-mini-shv-01-otp1.facebook.com: 443	*.eu-west-1. compute .amazonaws .com:4244				
		facebook-casche.te.net.net:443	*.clients.your- server.de:443				
			*.ip.kyivstar.net:443				
			pl-sh.host4.biz:443				
			web580.default-host.net				
			*.dialup.umc.net.ua:443				
			*.1e100.net:443				
			te.net.net:443				

Таблиця 2

Функціональні і сторонні з'єднання в ОС Android

Сис-темне ПЗ	Служби / модулі системного ПЗ	Вхідні / вихідні з'єднання (IP-адреси хостів)		IT-компанії	Блоку-вання функціо-нальних з'єднань (+/-)	Блоку-вання сторонніх з'єднань (+/-)	Праце-здатність ПЗ (+/-)
		функціональні	сторонні				
ОС Android	analytics		47.241.109.173:443	Alibaba		+	+
			47.241.21.203:443			+	+
			47.241.67.215:443			+	+
			47.241.109.173:443			+	+
			47.241.109.173:443			+	+
			161.117.183.182:443	Alibaba Cloud		+	+
			107.155.53.108:443	Zenlayer (Kingsoft cloud corporation limited)		+	+
			107.155.53.85:443				
	msa		47.241.108.101:443	Alibaba		+	+
	Батарея і продуктивність, Безпека Геодані з декількох джерел Запис екрану Інтерфейс Стрічка віджетів Налаштування Звіт Керування викликами		47.241.69.153:443	Alibaba		+	+
			47.88.222.244:80			+	+
			65.9.71.10:443	Amazon CloudFront		+	+
			65.9.71.64:443			+	+
			65.9.71.75:443			+	+
			65.9.71.43:443			+	+
			161.117.96.220:443	Alibaba Cloud		+	+
			161.117.160.12:443			+	+
			161.117.204.141:443			+	+
			161.117.97.83:80			+	+
			161.117.71.89:80			+	+
			161.117.71.92:80			+	+
			161.117.97.84:80			+	+

Системне ПЗ	Служби / модулі системного ПЗ	Вхідні / вихідні з'єднання (IP-адреси хостів)		IT-компанії	Блокування функціональних з'єднань (+/-)	Блокування сторонніх з'єднань (+/-)	Працездатність ПЗ (+/-)
		функціональні	сторонні				
	Пристрої введення Сховище налаштувань		161.117.57.135:443			+	+
			161.117.94.82:443				
			161.117.183.226:443				
	Google Services, Framework Google Резервне копіювання Сервіси Google Play	142.251.1.188:443		Google	+		+
		172.253.113.188:5228			+		+
		142.250.203.138:443		Google Cloud	+		+
	МТР-хост Завантаження Сховище мультимедіа		161.117.71.156:443	Alibaba Cloud		+	+
			161.117.71.89:80			+	+
			161.117.71.92:80			+	+
			161.117.71.84:80			+	+
			161.117.71.83:80			+	+
			161.117.96.220:80			+	+
			161.117.94.82:80			+	+
			161.117.160.82:80			+	+
			47.74.233.137:80	Alibaba		+	+
			47.74.233.244:80			+	+
	Галерея (фото і відео)		161.117.97.84:80	Alibaba		+	+
			161.117.97.83:80			+	+
			161.117.71.92:80			+	+
			161.117.71.89:80			+	+
			161.117.204.141:80			+	+
			47.74.233.137:80			+	+
			47.88.222.244:80			+	+
			161.117.96.220:80	Alibaba Cloud		+	+
			161.117.94.82:80			+	+
			161.117.160.12:80			+	+

У табл. 3 наведено функціональні з'єднання ПрК під керуванням ОС Windows 7/10.

Таблиця 3

Функціональні і сторонні з'єднання КК в ОС Windows 7/10

Системне ПЗ	Служби / модулі системного ПЗ	Вхідні / вихідні з'єднання (IP-адреси хостів)		IT-компанії	Блокування функціональних з'єднань (+/-)	Блокування сторонніх з'єднань (+/-)	Працездатність ПЗ (+/-)
		функціональні	сторонні				
	svchost.exe	64.4.0.0 - 64.4.31.255		Microsoft Corporation	+		+
		65.55.32.0 - 65.55.47.255			+		+
		65.55.0.0 - 65.55.31.255			+		+
		65.55.128.0 - 65.55.255.255			+		+
		65.55.96.0 - 65.55.127.255			+		+
		64.4.0.0 - 64.4.31.255			+		+

Системне ПЗ	Служби / модулі системного ПЗ	Вхідні / вихідні з'єднання (IP-адреси хостів)		IT-компанії	Блокування функціональних з'єднань (+/-)	Блокування сторонніх з'єднань (+/-)	Працездатність ПЗ (+/-)
		функціональні	сторонні				
ОС Windows 7|10		64.4.48.0 - 64.4.63.255			+		+
		213.199.179.0 - 213.199.179.31			+		+
		52.167.0.0 - 52.167.255.255			+		+
		207.68.160.0 - 207.68.167.255			+		+
		204.79.196.0 - 204.79.197.255			+		+
		134.170.0.0 - 134.170.63.255			+		+
		134.170.176.0 - 134.170.191.255			+		+
		131.253.48.0 - 131.253.63.255			+		+
	svchost.exe	64.4.0.0 - 64.4.31.255			+		+
		65.55.32.0 - 65.55.47.255			+		+
		65.55.0.0 - 65.55.31.255			+		+
		65.55.128.0 - 65.55.255.255			+		+
		65.55.96.0 - 65.55.127.255			+		+
		64.4.0.0 - 64.4.31.255			+		+
		64.4.48.0 - 64.4.63.255			+		+
		213.199.179.0 - 213.199.179.31			+		+
		52.167.0.0 - 52.167.255.255			+		+
		207.68.160.0 - 207.68.167.255			+		+
		204.79.196.0 - 204.79.197.255			+		+
		134.170.0.0 - 134.170.63.255			+		+
		134.170.176.0 - 134.170.191.255			+		+
		131.253.48.0 - 131.253.63.255			+		+
	svchost.exe		23.57.96.0 - 23.57.111.255	Akamai Technologies, Inc.		+	+
			23.48.104.0 - 23.48.111.255			+	+
			23.36.32.0 - 23.36.47.255			+	+
			23.223.20.0 - 23.223.20.255			+	+
			23.218.192.0 - 23.218.223.255			+	+
			23.205.208.0 - 23.205.215.255			+	+
			23.204.64.0 - 23.204.79.255			+	+
			23.102.0.0 - 23.102.63.255			+	+
			2.22.61.0 - 2.22.61.255			+	+
			104.96.128.0 - 104.96.159.255			+	+
			172.228.0.0 - 172.231.255.255			+	+
	svchost.exe	207.46.220.0 - 207.46.223.255		Microsoft Azure	+		+
		207.46.112.0 - 207.46.119.255			+		+
		207.46.96.0 - 207.46.111.255			+		+
		157.55.48.0 - 157.55.63.255			+		+
		137.117.128.0 - 137.117.255.255			+		+
		137.116.0.0 - 137.116.127.255			+		+
		111.221.64.0 - 111.221.67.255			+		+
		191.237.208.0 - 191.237.223.255			+		+
		191.232.80.0 - 191.232.80.63			+		+
		191.232.138.0 - 191.232.139.255			+		+
		191.232.138.0 - 191.232.139.255			+		+
			195.138.255.0	Core Back Bone		+	+
			62.140.236.163	Fiord Networks, UAB		+	+
			62.140.236.170			+	+

Результати виконаного дослідження графіка системного і прикладного ПЗ ПрК з цифровим простором дозволили встановити IP-адреси і домени сервісів збору даних користувачів, які належать IT-компаніям, що є лідерами на цифровому

ринку даних користувачів. У табл. 4 подані доменні імена сервісів збору даних користувачів, що належать ІТ-компаніям.

Таблиця 4

Сервіси збору даних користувачів у цифровому просторі інтернет

ІТ-компанії	Сервіс збору даних	Домен	IP-адреса
Yandex LLC	Yandex Metrika	mc.yandex.ru	87.250.250.119
Google	Google Analytics	googletagmanager.com	142.250.185.200
	Google Cloud	googlesyndication.com	142.250.185.68
United Network LLC	Liveinternet	counter.yadro .ru	88.212.201.204
Mail.Ru LLC	Relap	relap.io	95.163.37.253
Mediascope Joint Stock Company	TNS-Counter	tns-counter.ru	194.226.130.226
Hetzner Online GmbH	Openstat	openstat.com	138.201.159.191
Rambler Internet Holding LLC	Rambler TOP	top100.rambler.ru	81.19.89.1
Amazon	Easycounter	easycounter.com	52.1.22.171

Збір даних, поданих у табл. 1-4, здійснювався шляхом комплексного моніторингу DNS трафіка різних стаціонарних і мобільних ПрК упродовж тривалого часу з використанням спеціалізованого прикладного ПЗ [14-16].

4. Аналіз з'єднань інформаційних систем з цифровим простором

Проаналізуємо отримані експериментальним шляхом домени та IP-адреси, з якими системне і прикладне ПЗ ПрК встановлює функціональні і сторонні з'єднання, для різних ОС (див. табл. 1-3).

Прикладне ПЗ операційної, системи Android (див. табл. 1):

- домен sl-reverse.com підключений до ns-серверів: networklayer.com, softlayer. net. Належить вебплатформі CSC Digital Brand Services, що спеціалізується на цифровому управлінні брендами й цифровому маркетингу;

- домен 1e100.net підключений до ns-серверів google.com. Належить компанії Google;

- домен akamaitechnologies.com підключений до ns-серверів akamaistream.net. Належить компанії Akamai Technologies - провайдеру платформи доставки контенту і застосунків для акселерації вебсайтів;

- домен te.net.net належить компанії Bodis LLC, яка надає послуги з моне- тизації та керування доменним трафіком;

- домен cloudfront.net підключений до ns-серверів: awsdns-35.org, awsdns-07.co.uk, awsdns-52.com, awsdns-19.net. Цей домен належить ІТ-компанії Amazon, що спеціалізується на наданні послуг у хмарних сервісах;

- домен host.hit.gemius.pl належить компанії Gemius, яка спеціалізується на дослідженнях області споживання засобів масової інформації й розробляє інструменти, використовувані для оптимізації рекламних кампаній;

- домени compute-1.amazonaws.com та eu-central-1.amazonaws.com належать ІТ-компанії Amazon;

- домен fbcdn.net підключений до ns-серверів: facebook.com. Належить соціальній мережі Facebook. Використовується для обслуговування доставки статичного контенту (відео та фотографії з CDN);
- домен clients.your-server.de належить IT-компанії Hetzner Online GmbH, яка надає послуги хмарного вебхостингу;
- домен pl-sh.host4.biz належить IT-компанії Host4Biz, яка надає послуги віртуального хостингу (Польща);
- домен es49.mirohost.net належить провайдеру інтернет-послуг Internet Invest Ltd (Україна).

Операційна система Android (див. табл. 2):

- IP-адреса 161.117.98.205 - системне ПЗ для "пошуку пристроїв". Власником є корпорація Alibaba Cloud, що надає хмарні послуги для постачальників та інтеграторів інтелектуальних систем інтернету речей;
- IP-адреса 47.241.108.101:443 - системне ПЗ "msa". Власник - компанія Alibaba, що працює у сфері електронної комерції і хмарних обчислень;
- IP-адреса 107.155.53.108 належить компанії Kingsoft Cloud, що спеціалізується на хмарних обчисленнях.

Операційна система Windows (див. табл. 3):

- модуль svchost.com здійснює звернення до пулу IP-адрес, що належать IT-компанії Akamai Technologies Inc. Core Back Bone, Fiord Networks UAB;
- модуль svchost.com здійснює звернення до пулу IP-адрес, що належать IT-компанії Microsoft та її підрозділу Microsoft Azure.

Аналіз отриманих результатів експериментальної перевірки працездатності системного і прикладного ПЗ ПрК при здійсненні блокування його функціональних і сторонніх з'єднань (див. табл. 1 - 3) виявив таке:

- прикладне ПЗ Facebook встановлює з'єднання з транзитними інтернет-провайдерами, а також із хостами, які належать організаціям, що спеціалізуються на монетизації доменного трафіка користувачів;
- прикладне ПЗ Telegram здійснює спробу перенаправления свого трафіка через DNS сервери компанії Google;
- все прикладне ПЗ, яке працює під керуванням ОС Android, при його активізації виконує вихідні з'єднання з хостом 1e100.net, що належить компанії Google;
- функціональні з'єднання модулів і служб системного ПЗ ОС Android (див. табл. 2) виконуються в автоматичному режимі при виявленні будь-якого підключення ПрК до цифрового простору інтернет, незалежно від використовуваного мережевого інтерфейсу;
- системне ПЗ ОС Android (див. табл. 2) встановлює сторонні з'єднання з IP-адресами, які належать IT-компаніям Kingsoft Cloud, Alibaba, Alibaba Cloud, Amazon CloudFront, що надають послуги з транзиту трафіка і хмарних обчислень;
- блокування встановлених функціональних і сторонніх з'єднань системного ПЗ ОС Android (див. табл. 2) не призводить до порушення його працездатності;
- системне ПЗ ОС Windows 7/10 (див. табл. 3) встановлює функціональні з'єднання з IP-адресами, які належать її розробнику - IT-компанії Microsoft;

- системне ПЗ ОС Windows 7/10 встановлює сторонні з'єднання з IP- адресами, які належать IT-компаніям Akamai Technologies Inc, Core Back Bone, Fiord Networks UAB, що надають послуги з транзиту трафіка, хмарних обчислень і доставки контенту;

- блокування функціональних і сторонніх з'єднань системного ПЗ ОС Windows 7/10 (див. табл. 3) не призводить до порушення його працездатності;

- усі функціональні і сторонні з'єднання системного і прикладного ПЗ ПрК, здійснювані через порти 80, 5222, 5242 і 4244, є незахищеними й підлягають примусовому блокуванню.

Висновки

1.Проаналізовано принципи обміну даними між типовою ІС і цифровим простором інтернет. Встановлено, що DNS запити системного і прикладного ПЗ ПрК передаються у відкритому вигляді і фіксуються в журналах DNS сервера провайдера, що апріорі знижує приватність користувачів. Визначено шляхи підвищення приватності користувачів за рахунок впровадження заходів щодо захисту їх DNS трафіка.

2.Проаналізовано принципи побудови цифрових відбитків ПрК. Показано, що процес побудови цифрових відбитків заснований на застосуванні методів ідентифікації. Встановлено, що виконання процесу однозначної ідентифікації ПрК нерозривно пов'язане з організацією процесу збору даних про апаратну і програмну конфігурації ПрК.

3.Виконано фіксацію вихідних і вхідних з'єднань стаціонарного, мобільного системного і прикладного ПЗ ПрК. На основі даних, отриманих з відкритих джерел, встановлено, що сторонні з'єднання системного і прикладного ПЗ ПрК встановлюються з хостами, які належать IT-компаніям, що надають послуги з транзиту, збору, обробки й монетизації даних користувачів.

4.Здійснено аналіз вихідних з'єднань стаціонарного і мобільного системного і прикладного ПЗ ПрК. Запропоновано критерії, що дозволяють однозначно класифікувати функціональні та сторонні з'єднання системного і прикладного ПЗ ПрК. Проведено експериментальну перевірку працездатності системного і прикладного ПЗ ПрК при організації блокування функціональних і сторонніх з'єднань ІС. Встановлено, що при виконанні їх блокування працездатність ІС не порушується.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ISO/IEC 2382:2015 Information technology - Vocabula. URL: https://www.iso.org/ru/standard/63598.html (дата звернення: 02.09.2021).

2.*Guelke, J. Leaking.* International Encyclopedia of Ethics. 2020. Vol. 6. P. 1-7. DOI: 10.1002/9781444367072.wbiee898.

3. *Chen X., Navidi T., Rajagopal R.* Generating private data with user customization. 2020. P. 1-28. URL: Available at: https://www.researchgate.net/publication/346614406_Generating_private_data_with_user_customization (дата звернення: 02.09.2021).

4.*Liu X., Li H, Lu X., Xie T., Mei Q., Feng F., Mei H.* Understanding Diverse Usage Patterns from Large-Scale Appstore-Service Profiles. 2018. IEEE Transactions on Software Engineering. Vol. 44(4). P. 384-411. DOI: 10.1109/TSE.2017.2685387.

5.*Stachl C., Quay A., Schoedel R., Gosling S., Harari G, Buschek D, Volkel S, Schuwerk T, Oldemeier M., Ullmann Th., Hussmann H., Bischl B, Buehner M.* Predicting personality from patterns

of behavior collected with smartphones. Proceedings of the National Academy of Sciences of the United States of America. 2020. Vol. 117(30). P. 17680-17687. DOI: 10.1073/pnas.1920484117.

6. *Salman O, Elhajj I., Kayssi A.* A review on machine learning-based approaches for Internet traffic classification. Annals of Telecommunications. 2020. Vol. 75. P. 673-710. DOI: 10.1007/s12243- 020-00770-7.

7. *Yousefnezhad N, Malhi A., Framling K.* Automated loT Device Identification Based on Full Packet Information Using Real-Time Network Traffic. Sensors. 2021. Vol. 21. P. 2660. DOI: 10.3390/ s21082660.

8. *Chen X., Qu, G.* Integrated Circuit Digital Fingerprinting-Based Authentication. Authentication of Embedded Devices. 2021. P. 3-27. DOI: 10.1007/978-3-030-60769-2_1.

9. *Задерейко А.В., Троянский А.В., Логинова Н.И., Трофименко Е.Г.* Проблемные аспекты деперсонализации цифровых изображений. Інформатика та математичні методи в моделюванні. 2017. Т. 7. № 1-2. С. 37-46.

10. *Zadereyko O.V., Trofymenko O.G., Loginova N.I.* Algorithm of user's personal data protection against data leaks in Windows 10 OS. Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Srodowiska. 2019. Vol. 9. P. 41-44.

11. *Shriya N, Megha G, Lakshmi I., Deepak S.* Detection of Data Leaks from Android Applications. Second International Conference on Inventive Research in Computing Applications (ICIRCA). 2020. P. 326-332. DOI: 10.1109/ICIRCA48905.2020.9183066.

12. *Naseri M, Borges N., Zeller A., Rouvoy R.* AccessiLeaks: Investigating Privacy Leaks Exposed by the Android Accessibility Service. Proceedings on Privacy Enhancing Technologies. 2019. Vol. 2. P. 291-305. DOI: 10.2478/popets-2019-0031.

13. *Zadereyko A., Prokop Y., Trofymenko O., Loginova N., Plachinda O.* Development of an algorithm to protect user communication devices against data leaks. Eastern-European Journal of Enterprise Technologies. 2021. Vol. 1/2 (109). P. 24-34. DOI: 10.15587/1729-4061.2021.225339.

14. No Root Firewall. URL: https://play.google.com/store/apps/details?hl=ru&id=app.greyshirts.firewall (дата звернення: 02.09.2021).

15. Windows Firewall Control. URL: https://binisoft.org/wfc (дата звернення: 02.09.2021).

16. Wireshark. URL: https://www.wireshark.org/ (дата звернення: 02.09.2021).

REFERENCES

1. ISO/IEC 2382:2015 Information technology – Vocabula. URL: https://www.iso.org/ru/standard/63598.html (Date of Application: 02.09.2021) [in English].

2. *Guelke, J.* (2020) Leaking. International Encyclopedia of Ethics. Vol. 6. P. 1–7. DOI: 10.1002/9781444367072.wbiee898 [in English].

3. *Chen, X., Navidi, T., Rajagopal, R.* (2020) Generating private data with user customization. P. 1–28. URL: https://www.researchgate.net/publication/346614406_Generating_private_data_with_user_customization (Date of Application: 02.09.2021) [in English].

4. *Liu, X., Li, H., Lu, X., Xie, T., Mei, Q., Feng, F., Mei, H.* (2018) Understanding Diverse Usage Patterns from Large-Scale Appstore-Service Profiles. IEEE Transactions on Software Engineering. Vol. 44(4). P. 384–411. DOI: 10.1109/TSE.2017.2685387 [in English].

5. *Stachl, C., Quay, A., Schoedel, R., Gosling, S., Harari, G., Buschek, D., Vulkel, S., Schuwerk, T., Oldemeier, M., Ullmann, Th., Hussmann, H., Bischl, B., Buehner, M.* (2020) Predicting personality from patterns of behavior collected with smartphones. Proceedings of the National Academy of Sciences of the United States of America. Vol. 117 (30). P. 17680–17687. DOI: 10.1073/pnas.1920484117 [in English].

6. *Salman, O., Elhajj, I.H., Kayssi, A.* (2020) A review on machine learning–based approaches for Internet traffic classification. *Annals of Telecommunications*. 2020. Vol. 75. P. 673–710. DOI: 10.1007/s12243-020-00770-7 [in English].

7. *Yousefnezhad, N., Malhi, A., Framling, K.* (2021) Automated IoT Device Identification Based on Full Packet Information Using Real-Time Network Traffic. *Sensors*. Vol. 21. P. 2660. DOI: 10.3390/s21082660 [in English].

8. *Chen, X., Qu, G.* (2021) Integrated Circuit Digital Fingerprinting-Based Authentication. Authentication of Embedded Devices. P. 3–27. DOI: 10.1007/978-3-030-60769-2_1 [in English].

9. *Zadereyko, O.V., Troyanskiy, A.V., Loginova, N.I., Trofimenko, E.G.* (2017) Problematic aspects of depersonalization digital ima[in English].ges. Informatics and Mathematical Methods in Simulation. Vol. 7. No 1–2. P. 37–46 [in English].

17.*Zadereyko, O.V., Trofymenko, O.G., Loginova, N.I.* (2019) Algorithm of user's personal data protection against data leaks in Windows 10 OS. Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Srodowiska. Vol. 9. P. 41-44 [in English].

18.*Shriya N., Megha G., Lakshmi I., Deepak S.* (2020) Detection of Data Leaks from Android Applications. Second International Conference on Inventive Research in Computing Applications (ICIRCA). P. 326-332. DOI: 10.1109/ICIRCA48905.2020.9183066 [in English].

19.*Naseri, M, Borges, N., Zeller, A., Rouvoy, R.* (2019) AccessiLeaks: Investigating Privacy Leaks Exposed by the Android Accessibility Service. Proceedings on Privacy Enhancing Technologies. Vol. 2. P. 291-305. DOI: 10.2478/popets-2019-0031 [in English].

20. *Zadereyko, A., Prokop, Y., Trofymenko, O, Loginova, N., Plachinda, O.* (2021) Development of an algorithm to protect user communication devices against data leaks. Eastern-European Journal of Enterprise Technologies. Vol. 1/2 (109). P. 24-34. DOI: 10.15587/1729-4061.2021.225339 [in English].

21. No Root Firewall. URL: https://play.google.com/store/apps/details?hl=ru&id=app.greyshirts.firewall (Date of Application: 02.09.2021) [in English].

22. Windows Firewall Control. URL: https://binisoft.org/wfc (Date of Application: 02.09.2021) [in English].

23. Wireshark. URL: https://www.wireshark.org/ (Date of Application: 02.09.2021) [in English].

UDC 004.738.2

Zadereiko Oleksandr,
PhD (Engineering), Associate professor of the Department of Information Technology, National University "Odessa Law Academy", Odesa, Ukraine, ORCID ID 0000-0003-0497-9861
Trofymenko Olena,
PhD (Engineering), Associate professor of the Department of Information Technology, National University "Odessa Law Academy", Odesa, Ukraine, ORCID ID 0000-0001-7626-0886
Prokop Yuliia,
PhD (Engineering), Senior Lecturer of the Department of Information Technology. State University of Intellectual Technologies and Communications, Odesa, Ukraine,
ORCID ID 0000-0002-6608-3668
Lohinova Nataliia,
PhD (Engineering), Associate professor of the Department of Information Technology, National University "Odessa Law Academy", Odesa, Ukraine, ORCID ID 0000-0002-9475-6188
Kukharenko Serhii,
PhD (Engineering), Associate professor of the Department of Information Technology, National University "Odessa Law Academy", Odesa, Ukraine, ORCID ID 0000-0001-7100-6408

ANALYSIS OF DATA LEAKS IN INFORMATION SYSTEMS

Research article investigates the principles of data exchange between the classical information system of the user, represented by stationary and mobile means of communication, and the digital space of the Internet. It has been established that the DNS traffic of a typical information system is carried out through the provider's DNS server, in which all DNS queries of the user, system, and application software of the communication device are recorded.

It was determined that such an organization of communication poses a threat to the privacy of users due to the possibility of access to the provider's DNS server logs by authorized government services.

Traffic was recorded for a typical user information system to identify ways of collecting data from stationary and mobile communication devices of users. An audit of outgoing and incoming connections of communication devices with digital space was carried out. It is determined that the system and application software of the communication device establishes connections with hosts that belong to IT companies providing services for the transit, collection, processing, and monetization of user data.

The suggested criteria made it possible to unambiguously classify functional and third-party connections of the system and application software of communication devices. The operability of the system and application software of communication devices after blocking functional and third-party connections of the information system was experimentally tested. It was found that when blocking third-party connections, the operability of the information system is not impaired.

The principles of constructing digital prints of a communication device are considered. It is shown that the process of building digital prints is based on the use of identification methods.

The principles of an identification of communication devices in the digital space are analyzed. It has been established that the process of unambiguous identification of a communication device is inextricably linked with the collection of the maximum possible information about the hardware and software configuration of the communication device.

Keywords: DNS query, DNS server, data leaks, DNS traffic, data leak analysis, communication device, device identification.

Отримано 28.09.2021