

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ
УКРАЇНСЬКА АСОЦІАЦІЯ З ПРИКЛАДНОЇ ГЕОМЕТРІЇ
ВІЙСЬКОВА АКАДЕМІЯ (М. ОДЕСА)
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ**

ГРАФІЧНІ ТЕХНОЛОГІЇ МОДЕЛЮВАННЯ ОБ'ЄКТІВ, ПРОЦЕСІВ ТА ЯВИЩ

**Збірник тез доповідей
Міжнародної науково-практичної конференції**

23-24квітня 2020 року

м. Одеса

СЕКЦІЯ 5
СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ У СЕКТОРІ БЕЗПЕКИ І ОБОРОНИ:
ПРОБЛЕМИ ТА РОЗВИТОК

Задерейко О.В., к.т.н., доц.

Логінова Н.І., к.пед.н., доц.

Трофименко О.Г., к.т.н., доц.

Національний університет «Одеська юридична академія»

АНАЛІЗ ВІРОГІДНИХ ВИТОКІВ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ КОРИСТУВАЧІВ
У МОБІЛЬНИХ ЗАСТОСУНКАХ

Повсюдне використання мобільних застосунків для оперативного отримання інформації та миттєвої комунікації значно збільшує ймовірність витоку конфіденційної інформації користувачів. Це обумовлює необхідність виявлення всіх вихідних інтернет - з'єднань мобільних застосунків і подальшого їх детального аналізу з точки зору забезпечення максимально можливої конфіденційності користувачів.

Мета дослідження – проаналізувати обмін даними мобільних застосунків соціальних мереж і месенджерів з адресним простором інтернету та виявити вірогідні витoki конфіденційної інформації користувачів.

Об'єкт дослідження – мобільна операційна система Android 10, месенджери Whats App, Viber, та Telegram, соціальні мережі Facebook та Instagram.

У дослідженні було застосовано NoRoot Firewall – мережевий екран (брандмауер) для Android, який дозволяє контролювати мобільний і Wi-Fi трафік на смартфоні або планшеті.

Результати дослідження. Шляхом 30-тиденної фіксації трафіка мобільних застосунків було виявлено список доменів сторонніх серверів, з якими вони виконували обмін даними, а саме: *.bc.googleusercontent: port 443; *.1e100.net: port 443; sl-reverse.com: port 443; *.compute-1.amazonaws.com: port 4244; *.r.cloudfront.net: port 443. Аналіз інформації з відкритих джерел про виявлені домени показав таке:

- домен **sl-reverse.com**: підключений до ns-серверів networklayer.com та softlayer.net і належить вебплатформі CSCDigitalBrandServices, яка спеціалізується на керуванні цифровими брендами та на цифровому маркетингу;
- домен **1e100.net** - підключений до ns-серверів google.com і належить корпорації Google;
- домен **googleusercontent.com** - підключений до ns-серверів google.com і належить корпорації Google;
- домен **akamaitechnologies.com** - підключений до ns-серверів akamaistream.net і належить компанії AkamaiTechnologies, яка є провайдером платформи доставки контенту і застосунків для акселерації вебсайтів;
- домен **cloudfront.net** - підключений до ns-серверів awsdns-35.org, awsdns-07.co.uk, awsdns-52.com та awsdns-19.net; належить корпорації Amazon, яка спеціалізується на наданні послуг у хмарних сервісах.

Висновки. По-перше, виявлені при тривалому дослідженні трафіка сторонні сервери, з якими досліджувані мобільні застосунки та месенджери обмінюються даними, орендують компанії, що надають послуги зі збирання, накопичення та оброблення даних з використанням хмарних технологій. Такий обмін даними з високою ймовірністю може спричинити неконтрольовані витoki конфіденційної інформації користувачів.

По-друге, вибіркове блокування мережевого трафіка на сторонні ір-адреси серверів дозволить:

- запобігти витокам конфіденційної інформації користувачів;
- зберегти передумови функціонування та працездатності мобільних застосунків;
- суттєво скоротити обсяг трафіка даних, що дозволить скоротити витрати користувачів на його оплату провайдерам.

**ГРАФІЧНІ ТЕХНОЛОГІЇ МОДЕЛЮВАННЯ
ОБЄКТІВ, ПРОЦЕСІВ ТА ЯВИЩ**

**Збірник тез доповідей
Міжнародної науково-практичної конференції**

23-24квітня 2020 року

**Редакційна група за якість матеріалів відповідальності не несе.
Матеріали доповідей авторів надано у вигляді, відповідно
до заявок на участь у конференції.
Дякуємо авторам за дотримання рекомендованого шаблону та обсягу виступів.**

Відповідальний за випуск – Трушков Г.В.
Комп'ютерний набір Радченко І.Г.,
Комп'ютерна верстка Труш С.Й.

Здано до набору 15.05.2020 р. Підписано до друку 19.05.2020 р.
Формат паперу 297х420/2. Авт. арк. – 5,54. Обл. вид. арк. – 5,64. Друк. арк. – 30,5.
Умов. друк. арк. – 7,15. Папір офсетний. Гарнітура Times New Roman.
Замовлення № 164 -2020 РВВ ВА. Наклад – 100 прим.

Віддруковано у друкарні Військової академії (м. Одеса)
65009, м. Одеса, вул. Фонтанська дорога, 10.