

- HanzoInjection (<https://github.com/P0cL4bs/hanzoInjection>);
- Invoke-Obfuscation (<https://github.com/danielbohannon/Invoke-Obfuscation>).

У вихідному RAT файлі 51 антивірус сервісу VirusTotal з 71 виявив шкідливий код, результати сканування модифікованих різними обфускаторами файлу RAT наведений у Табл. 1.

**Таблиця 1 – Результати виявлення антивірусами сервісу
VirusTotal шкідливого обфускованого коду**

Обфускатор коду	Кількість антивірусів, що сканували обфускований код	Кількість антивірусів, що виявили шкідливий обфускований код
Shellter	67	22 (33%)
FuckThatPacker	69	11 (16%)
Chimera	61	4 (7%)
HanzoInjection	60	0
Invoke-Obfuscation	71	9 (13%)

Загалом, усі обфускатори показали деяку ефективність у маскуванні сигнатури коду, але модифікований HanzoInjection шкідливий код не був виявлений жодним антивірусом сервісу VirusTotal, що підтверджує необхідність використання комплексних систем захисту, які враховують не тільки відомі сигнатури коду, а і інші чинники.

Список використаних джерел:

5. What is Remote Access Trojan (RAT)? URL: <https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-remote-access-trojan/> (дата звернення 21.11.2022).

УДК 004.9

НОСОВ ВІТАЛІЙ ВІКТОРОВИЧ

кандидат технічних наук, доцент,

*професор кафедри протидії кіберзлочинності факультету № 4
Харківського національного університету внутрішніх справ*

УСЕНКО АРІНА ОЛЕГІВНА

курсантка 3 курсу факультету № 4

Харківського національного університету внутрішніх справ

ОЦІНКА ХАРАКТЕРИСТИК СЕРВІСІВ ДЕЯКИХ РОЗШИРЕНЬ БРАУЗЕРУ GOOGLE CHROME З ПРИХОВУВАННЯ IP АДРЕСИ СИСТЕМИ

Одним із основних ідентифікаторів клієнта при з'єднанні з вебресурсом є IP адреса системи, за якою збирається інформація про можливого користувача або здійснюється обмеження доступу до вебресурсів. На сьогодні найбільш вживаним браузером для доступу до вебресурсів з часткою світового ринку 65,52% є Google Chrome [1], в якому можна встановити певний тип розширення (extension), що декларує приховування IP адреси системи при з'єднанні з вебресурсом.

Розробники таких розширень позначають їх як VPN або Proху, але, строго кажучи, всі вони є тільки Proху, оскільки спрямовують трафік до проміжного вузла мережі за прикладним (http/https) або сеансовим (SOCKS4/SOCKS5) протоколами. Для підключення до серверу VPN (віртуальної приватної мережі) потрібна або окрема клієнтська програма або вже наявні в операційній системі відповідні сервіси, які спрямовують увесь трафік системи до серверу VPN за протоколами мережевого/канального рівня (OpenVPN, L2TP/IPSec, і ін.).

Розширення Google Chrome доступні для встановлення у виділеному репозиторії chrome web store³, де зазначений їх опис і характеристики. На сьогодні загальна кількість розширень у chrome web store близько 188620 [2], і серед них було виявлено 210 розширень Proху, аналіз споживчих характеристик яких дозволив виділити чотири з найбільшою кількістю користувачів (табл. 1).

Таблиця 1 – Рейтинг розширень Proху

³ <https://chrome.google.com/webstore/category/extensions>

Назва	Кількість користувачів	Середня оцінка (макс. 5 балів)	Кількість оцінок
Touch VPN ⁴	7000000+	4,6	77978
Hola VPN ⁵	4000000+	4,9	355997
1clickVPN ⁶	4000000+	4,8	32447
VeePN ⁷	3000000+	4,7	7438

За середньою оцінкою користувачів і кількістю оцінок першим у рейтингу є розширення Hola VPN, а за кількістю користувачів - Touch VPN.

Також можна оцінити функціональність і доступність (безплатне використання) сервісів зазначених розширень (табл. 2).

Таблиця 2 – Функціональність і доступність сервісів розширень Proxy

Характеристика	Розширення			
	Touch VPN	Hola VPN	1clickVPN	VeePN
Платні функції	так	так	так	так
Додаткова анонімізація, блокування реклами	так	так	ні	так
Шифрування трафіку	так	ні	так	так
Блокування витоку IP адреси через WebRTC ⁸	так	так (платно)	ні	так
Кількість безкоштовних/платних локацій проксі сервера	6/	200+/-	1/9	6/89+

Найбільш доступними і функціональним є сервіси розширення Touch VPN і VeePN. Сервіс розширення Hola VPN має найбільшу кількість вибору безплатних локацій проксі, а 1clickVPN має найменшу кількість функцій.

⁴ <https://chrome.google.com/webstore/detail/touch-vpn-secure-and-unli/bihmplhobchoageeokmgdbihknkjbknd>

⁵ <https://chrome.google.com/webstore/detail/hola-vpn-the-website-unbl/gkojfkhleikighikafcpjkiklfbnlmeio>

⁶ <https://chrome.google.com/webstore/detail/1clickvpn-free-vpn-for-ch/fcfhplplocckackoneafokcmbjfbkenj>

⁷ <https://chrome.google.com/webstore/detail/free-vpn-for-chrome-vpn-p/majdfhpaihoncoakbjgdbhglocklcnog>

⁸ <https://proxy6.net/en/privacy>

Варто зазначити, що кожний провайдер проксі сервісу декларує власну політику приватності щодо збору, зберігання і поширення унікальних даних користувачів.

Список використаних джерел:

1. MOST POPULAR WEB BROWSERS IN 2022. URL: <https://www.oberlo.com/statistics/browser-market-share> (дата звернення 26.11.2022).

2. Google Chrome Statistics. URL: <https://truelist.co/blog/google-chrome-statistics/> (дата звернення 26.11.2022).

УДК 004.336

ОРЛОВ РОМАН РУСЛАНОВИЧ

магістр факультету № 5 за спеціальністю «Кібербезпека» Харківського національного університету внутрішніх справ, лейтенант поліції, старший інспектор управління протидії кіберзлочинам в м. Києві Департаменту кіберполіції НПУ

ОКУШКО АНДРІЙ ВАСИЛЬОВИЧ

кандидат юридичних наук, полковник поліції, заступник начальника Управління протидії кіберзлочинам в м. Києві Департаменту кіберполіції НПУ України

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН У ДІЯЛЬНОСТІ ПРАВООХОРОНИХ ОРГАНІВ ТА ПРОТИДІЇ КІБЕРЗЛОЧИНАМ

Безсумнівно, блокчейн — революційне явище, по значущості, яке можна порівняти з геніальним винаходом ХХ століття — Інтернетом. Це призвело до того, що технологія блокчейн створила платформу нового виду «Інтернету» та сприяла появі децентралізованих сервісів. На відміну від централізованого підходу, нові послуги базуються на децентралізованій розподіленій мережі, яка може використовуватися для різних цілей, включаючи кібербезпеку. На сьогоднішній день блокчейн найбільше затребуваний у фінансовому секторі (створення цифрових валют, здійснення транзакцій, обмін та зберігання