МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
КАФЕДРА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем

Лабораторна робота №1

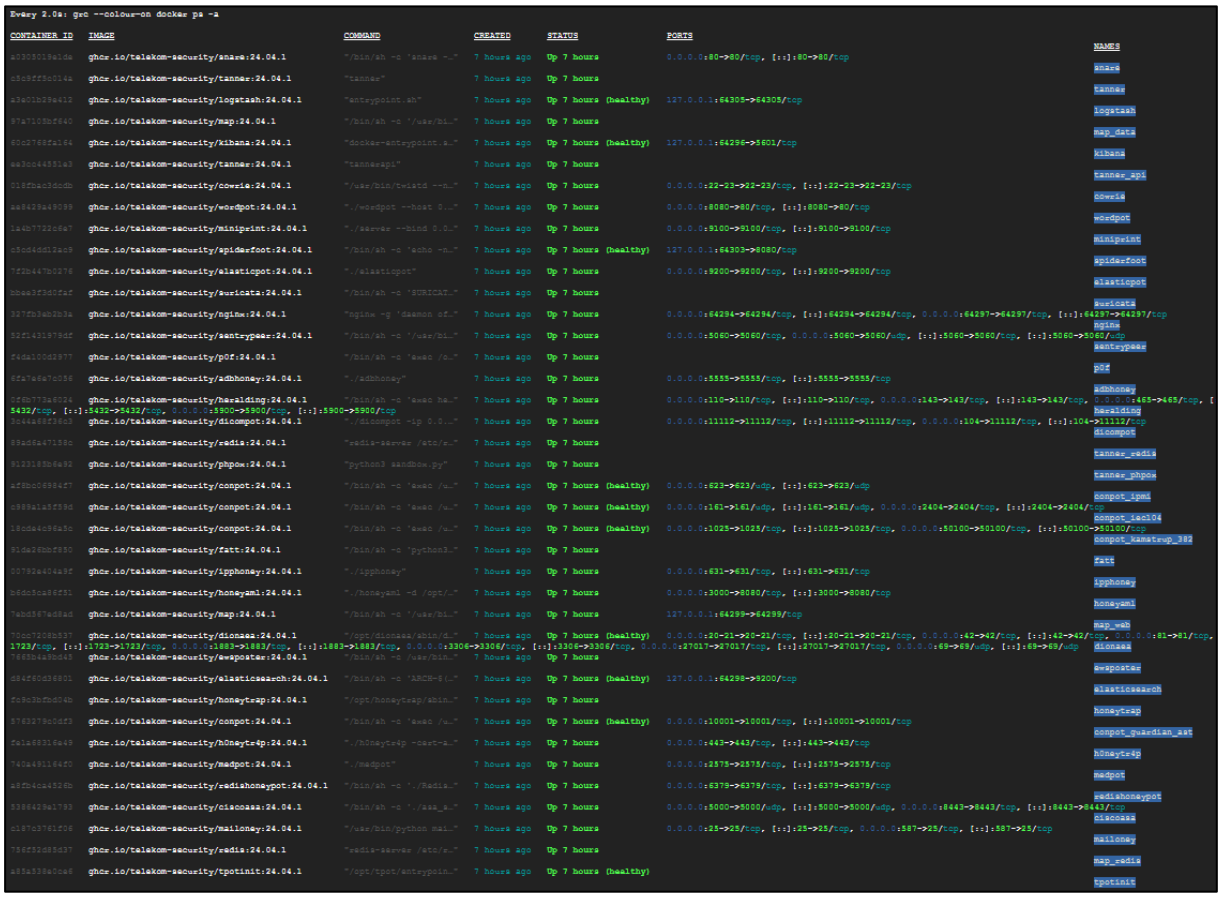
Моніторинг активності на T-Pot в GCP

Перевірив:
Полуциганова В. І.

Виконав:
студент І курсу
групи ФБ-41мп
Сахній Н. Р.

Київ 2025

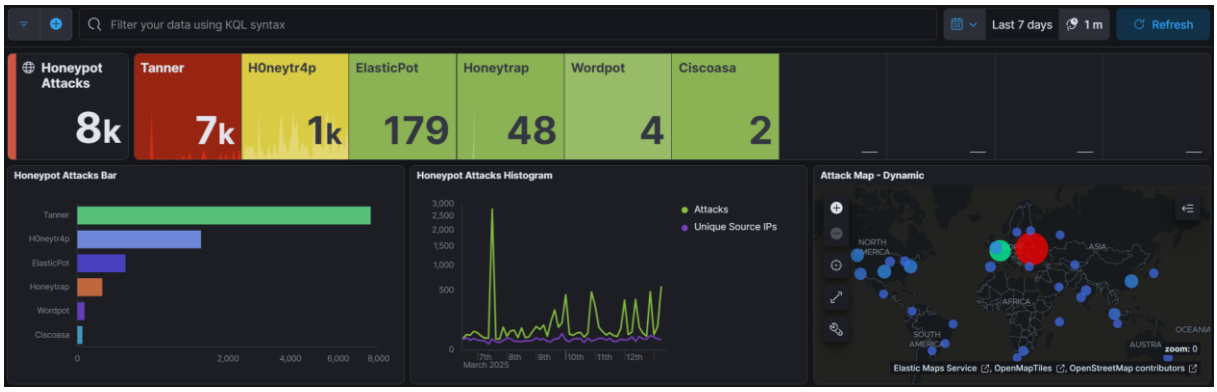
На основі логів тих запитів, які здійснювалися до наведених нижче приманок, було проведено аналіз даних на предмет виявлення зловмисної бот-активності або релевантних атрибутів, що сигналізували про атаки:



(Часовий проміжок аналізу активності: **06.03.2025–13.03.2025**)

a. Огляд розподілу атак по приманках

Загалом, за період дослідження було здійснено понад **8 тис.** підозрілих дій:

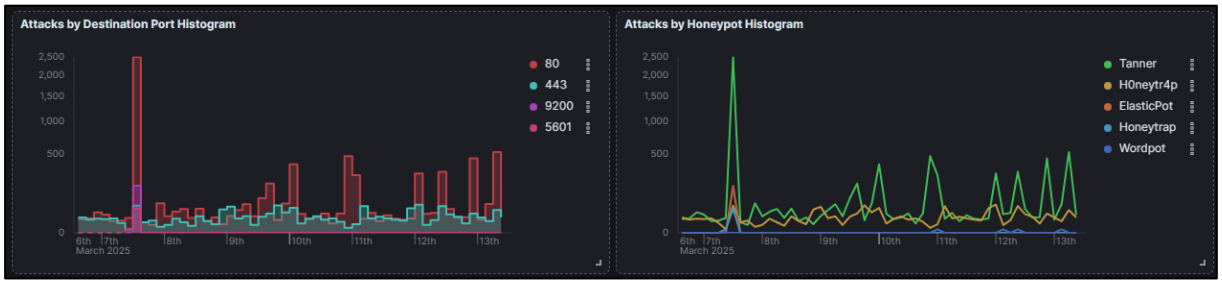


Із наведеного вище зображення помітно наступний розподіл по приманках:

- **Tanner: ~7 тис.** (82%) – (Імітація веб-сторінки GitLab -репозиторію);
- **H0neytr4p: ~1 тис.** (15%) – (Загальна приманка, що імітує відкриті порти та сервіси для виявлення шкідливих запитів від зловмисників);
- **ElasticPot: 179** (2%) – (Імітація пошукової системи Elasticsearch);
- **Honeytrap: 48** (1%) – (Приманка, яка може бути налаштована для емуляції різних мережевих сервісів, зокрема SSH, HTTP, FTP тощо);
- **Wordpot: 4** (~0%) – (Приманка для емуляції WordPress CMS);
- **Ciscoasa: 2** (~0%) – (Імітує міжмережевий екран Cisco ASA).

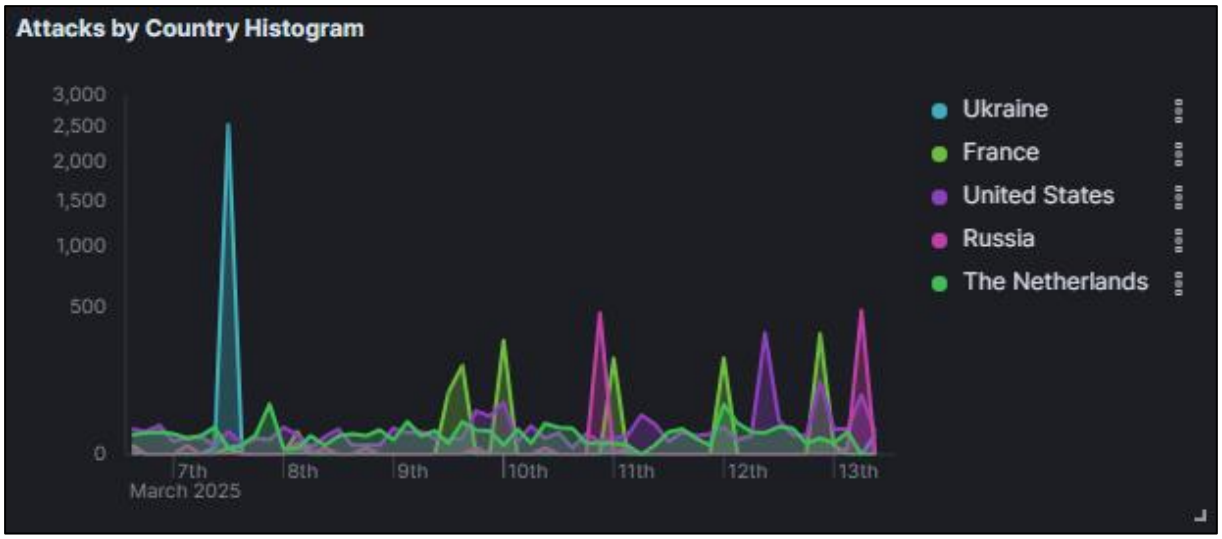
b. Огляд розподілу атак по портах

Переважно були “атаковані” сервіси, які розгорнуті на **80** та **443** портах:



c. Огляд розподілу атак по країнах

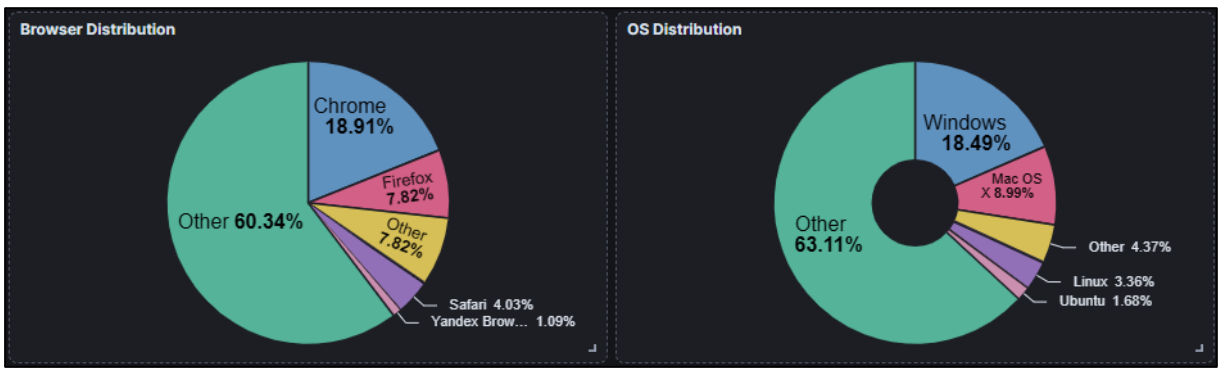
Загалом, найбільше нелегітимних дій було зафіксовано від таких країн як **France** (18%), **United States** (16%), **Russia** (13%) та **The Netherlands** (8%).



Окремо варто зауважити, що активність з **Ukraine (77.47.130.210)** становила 35% від усього трафіку, і вона була легітимна, оскільки здійснювалася в рамках проведення тестування на вразливості портів віртуальної машини:

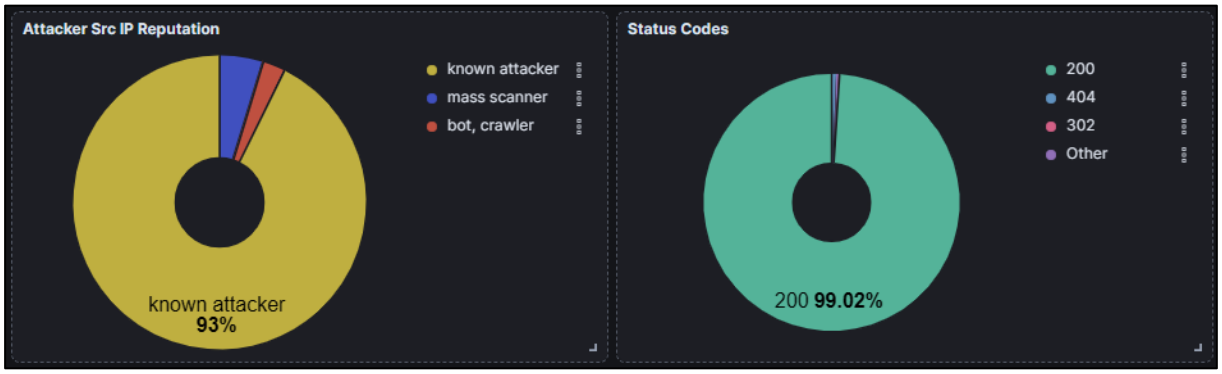
d. Огляд розподілу атак по User-Agent

Алгоритми T-Pot переважно не могли визначити тип ОС та браузера (>60%). Однак все ж були запити класифіковані як такі, що здійснювалися із використанням топ-браузера **Chrome** (19%) та топ-ОС **Windows** (19%):



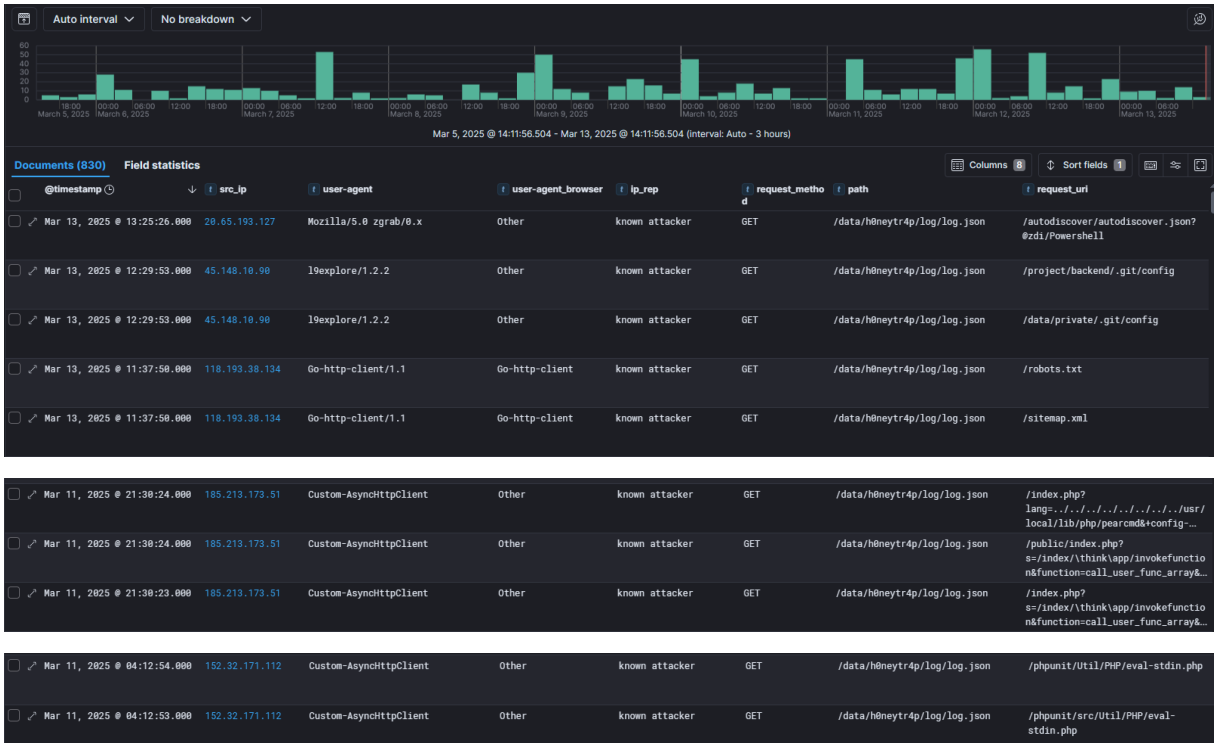
e. Перелік ботів та їх коди статусів

Засобами Suricata IDS було визначено, що 93% зафіксованих інцидентів класифікуються як активність відомих зловмисників (“**known attacker**”), 5% – як масове сканування (“**mass scanner**”), а 3% – як дії автоматизованих ботів-сканерів (“**bot, crawler**”). Майже всі запити отримували **200-ий** код:



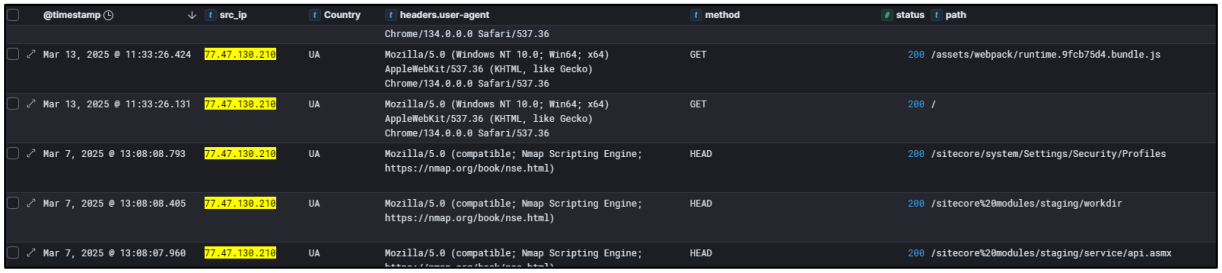
f. Задетектовані паттерни аномалій

Основна частина запитів була спрямована на **отримання доступу** до конфігураційних та системних PHP-файлів для виявлення їх присутності:



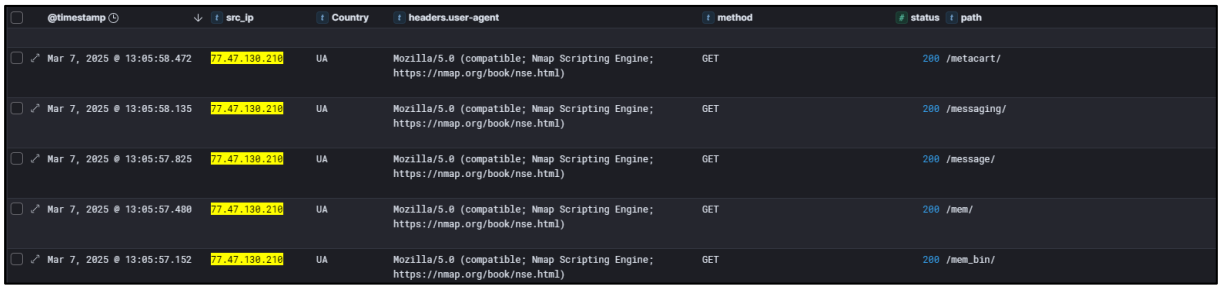
g. Активність від "пентестерів" :^)

При спробі замаскуватися деякі запити виконувалися від імені звичайного User-Agent, однак присутні атрибути того, що активність здійснювалася за допомогою інструментарію із категорії сканерів **"Nmap Script Engine"**:



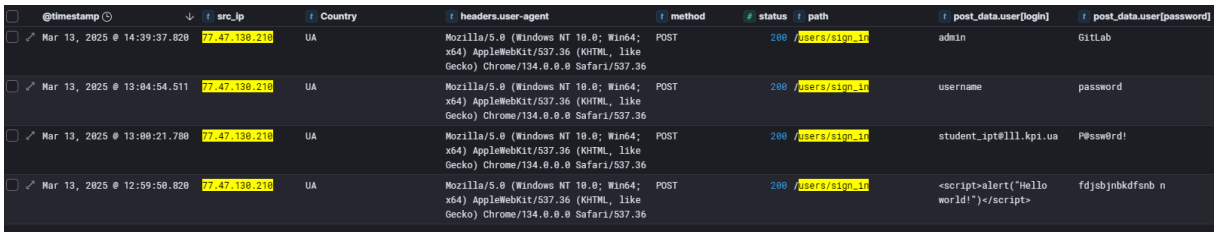
@timestamp	src_ip	Country	headers.user-agent	method	status	path
			Chrome/134.0.0.0 Safari/537.36			
Mar 13, 2025 @ 11:33:26.424	77.47.130.210	UA	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0.0 Safari/537.36	GET	200	/assets/webpack/runtime.9fcb75d4.bundle.js
Mar 13, 2025 @ 11:33:26.131	77.47.130.210	UA	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0.0 Safari/537.36	GET	200	/
Mar 7, 2025 @ 13:08:08.793	77.47.130.210	UA	Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)	HEAD	200	/sitecore/system/Settings/Security/Profiles
Mar 7, 2025 @ 13:08:08.405	77.47.130.210	UA	Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)	HEAD	200	/sitecore%20modules/staging/workdir
Mar 7, 2025 @ 13:08:07.960	77.47.130.210	UA	Mozilla/5.0 (compatible; Nmap Scripting Engine;	HEAD	200	/sitecore%20modules/staging/service/api.asmx

Також помітно, що фіксувалися активні спроби перебору імен директорій:



@timestamp	src_ip	Country	headers.user-agent	method	status	path
Mar 7, 2025 @ 13:05:58.472	77.47.130.210	UA	Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)	GET	200	/metacart/
Mar 7, 2025 @ 13:05:58.135	77.47.130.210	UA	Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)	GET	200	/messaging/
Mar 7, 2025 @ 13:05:57.825	77.47.130.210	UA	Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)	GET	200	/message/
Mar 7, 2025 @ 13:05:57.480	77.47.130.210	UA	Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)	GET	200	/mem/
Mar 7, 2025 @ 13:05:57.152	77.47.130.210	UA	Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)	GET	200	/mem_bin/

Окрім того були певні запити, що містили в собі паттерни XSS та Bruteforce:



@timestamp	src_ip	Country	headers.user-agent	method	status	path	post_data.user[login]	post_data.user[password]
Mar 13, 2025 @ 14:39:37.820	77.47.130.210	UA	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0.0 Safari/537.36	POST	200	/users/sign_in	admin	GitLab
Mar 13, 2025 @ 13:04:54.511	77.47.130.210	UA	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0.0 Safari/537.36	POST	200	/users/sign_in	username	password
Mar 13, 2025 @ 13:00:21.780	77.47.130.210	UA	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0.0 Safari/537.36	POST	200	/users/sign_in	student_ipt@lll.kpi.ua	P@ssw0rd!
Mar 13, 2025 @ 12:59:50.820	77.47.130.210	UA	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0.0 Safari/537.36	POST	200	/users/sign_in	<script>alert("Hello world!")</script>	fdjsbjnbkdfsnb n

Отже, в цілому можна зробити висновок, що набір приманок T-Pot зміг зібрати активність, яка загалом була злоякісною та нелегітимною. Оскільки, на сьогодні Інтернет-трафік близько на 50% складається із бот-активності, тому з метою покращення безпеки свого середовища обов'язково необхідне використання рішень із класу "Bot Mitigation".