



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 I курсу

групи ФБ-41мп

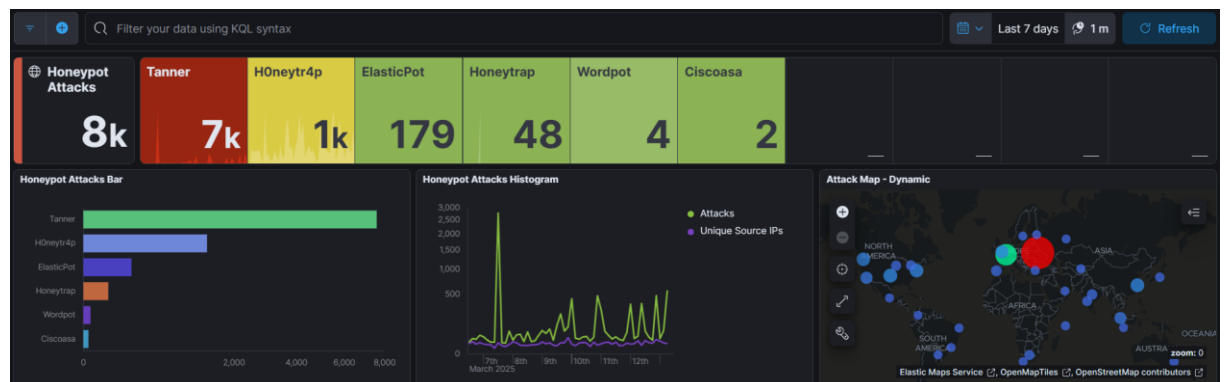
Сахній Н. Р.

Київ 2025

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS	IMAGE
437315176156	ghcr.io/telekom-security/tanner:24.04.1	"/bin/sh -c 'tanner -c'"	7 hours ago	Up 7 hours	0.0.0.0:80->80/tcp, [::]:80->80/tcp	tanner
45825520314	ghcr.io/telekom-security/tanner:24.04.1	"tanner"	7 hours ago	Up 7 hours		tanner
43610236412	ghcr.io/telekom-security/logstash:24.04.1	"entrypoint.sh"	7 hours ago	Up 7 hours (healthy)	127.0.0.1:64305->64305/tcp	logstash
87471210740	ghcr.io/telekom-security/map:24.04.1	"/bin/sh -c '/usr/bin'"	7 hours ago	Up 7 hours		map_data
80027495214	ghcr.io/telekom-security/kibana:24.04.1	"docker-entrypoint.sh"	7 hours ago	Up 7 hours (healthy)	127.0.0.1:64284->64801/tcp	kibana
863034433143	ghcr.io/telekom-security/tanner:24.04.1	"tannerapi"	7 hours ago	Up 7 hours		tanner_api
012901300100	ghcr.io/telekom-security/dowdie:24.04.1	"/usr/bin/twisted --n..."	7 hours ago	Up 7 hours	0.0.0.0:22->22->22/tcp, [::]:22->22->22/tcp	dowdie
0014233141393	ghcr.io/telekom-security/workspot:24.04.1	"/workspot --host 0.0..."	7 hours ago	Up 7 hours	0.0.0.0:8080->807/tcp, [::]:8080->807/tcp	workspot
144077320647	ghcr.io/telekom-security/minipoint:24.04.1	"./server --bind 0.0.0..."	7 hours ago	Up 7 hours	0.0.0.0:9100->9100/tcp, [::]:9100->9100/tcp	minipoint
450440121429	ghcr.io/telekom-security/apdsr-foot:24.04.1	"/bin/sh -c 'echo -e..."	7 hours ago	Up 7 hours (healthy)	127.0.0.1:64303->64800/tcp	apdsr-foot
7120144700278	ghcr.io/telekom-security/elasticoptr:24.04.1	"/elasticoptr"	7 hours ago	Up 7 hours	0.0.0.0:9200->9200/tcp, [::]:9200->9200/tcp	elasticoptr
004612503747	ghcr.io/telekom-security/auricata:24.04.1	"/bin/sh -c 'SURICAT..."	7 hours ago	Up 7 hours		auricata
327170136378	ghcr.io/telekom-security/nghttp:24.04.1	"nghttp -c 'daemon st..."	7 hours ago	Up 7 hours	0.0.0.0:64284->64284/tcp, [::]:64284->64284/tcp, 0.0.0.0:64287->64287/tcp, [::]:64287->64287/tcp	nghttp
450143137847	ghcr.io/telekom-security/sentry-pear:24.04.1	"/bin/sh -c 'sentry-..."	7 hours ago	Up 7 hours	0.0.0.0:5000->5000/tcp, 0.0.0.0:5006->5006/tcp, [::]:5006->5006/tcp, [::]:5006->5006/tcp	sentry-pear
744410002877	ghcr.io/telekom-security/pof:24.04.1	"/bin/sh -c 'sasl -c..."	7 hours ago	Up 7 hours		pof
074746747024	ghcr.io/telekom-security/rdnssync:24.04.1	"./rdnssync"	7 hours ago	Up 7 hours	0.0.0.0:5555->5555/tcp, [::]:5555->5555/tcp	rdnssync
070777474524	ghcr.io/telekom-security/hardening:24.04.1	"/bin/sh -c 'sasl ha..."	7 hours ago	Up 7 hours	0.0.0.0:1111->1111/tcp, [::]:1111->1111/tcp, 0.0.0.0:143->143/tcp, [::]:143->143/tcp, 0.0.0.0:445->445/tcp, [::]:445->445/tcp	hardening
54307tcp, [::]:54307tcp, 0.0.0.0:1800->1800/tcp, [::]:1800->1800/tcp	ghcr.io/telekom-security/dicompt:24.04.1	"/dicompt -p 0.0.0.0..."	7 hours ago	Up 7 hours	0.0.0.0:11112->11112/tcp, [::]:11112->11112/tcp, 0.0.0.0:104->104/tcp, [::]:104->104/tcp	dicompt
89404471330	ghcr.io/telekom-security/redis:24.04.1	"redis-server /etc/r..."	7 hours ago	Up 7 hours		redis
912131304693	ghcr.io/telekom-security/phpop:24.04.1	"python3 rediscon.py"	7 hours ago	Up 7 hours		redis-redis
458000494407	ghcr.io/telekom-security/compt:24.04.1	"/bin/sh -c 'sasl -c..."	7 hours ago	Up 7 hours (healthy)	0.0.0.0:622->623/tcp, [::]:622->623/tcp	compt_ipsec
498141473730	ghcr.io/telekom-security/nonpopt:24.04.1	"/bin/sh -c 'sasl -c..."	7 hours ago	Up 7 hours (healthy)	0.0.0.0:161->161/tcp, [::]:161->161/tcp, 0.0.0.0:2404->2404/tcp, [::]:2404->2404/tcp	compt_ipsec
180404464650	ghcr.io/telekom-security/compt:24.04.1	"/bin/sh -c 'sasl -c..."	7 hours ago	Up 7 hours (healthy)	0.0.0.0:1025->1025/tcp, [::]:1025->1025/tcp, 0.0.0.0:50100->50100/tcp, [::]:50100->50100/tcp	compt_kamnet_38
910410402830	ghcr.io/telekom-security/fatt:24.04.1	"/bin/sh -c 'python3..."	7 hours ago	Up 7 hours		fatt
027194447430	ghcr.io/telekom-security/lyphoney:24.04.1	"./lyphoney"	7 hours ago	Up 7 hours	0.0.0.0:631->631/tcp, [::]:631->631/tcp	lyphoney
946040447351	ghcr.io/telekom-security/honeyall:24.04.1	"/honeyall -d opt..."	7 hours ago	Up 7 hours	0.0.0.0:3000->3000/tcp, [::]:3000->3000/tcp	honeyall
744018744040	ghcr.io/telekom-security/map:24.04.1	"/bin/sh -c '/usr/bin..."	7 hours ago	Up 7 hours	127.0.0.1:64296->64289/tcp	map_web
700077003377	ghcr.io/telekom-security/dissana:24.04.1	"/opt/dissana/abn/ab..."	7 hours ago	Up 7 hours (healthy)	0.0.0.0:201-21->21->21/tcp, [::]:201-21->21->21/tcp, 0.0.0.0:442->442/tcp, [::]:442->442/tcp, 0.0.0.0:81->81/tcp, [::]:81->81/tcp	dissana
910101304141	ghcr.io/telekom-security/ewoscat:24.04.1	"/opt/ewoscat/ewoscat..."	7 hours ago	Up 7 hours	0.0.0.0:1701->1701/tcp, [::]:1701->1701/tcp, 0.0.0.0:	

а. Огляд розподілу атак по приманках

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

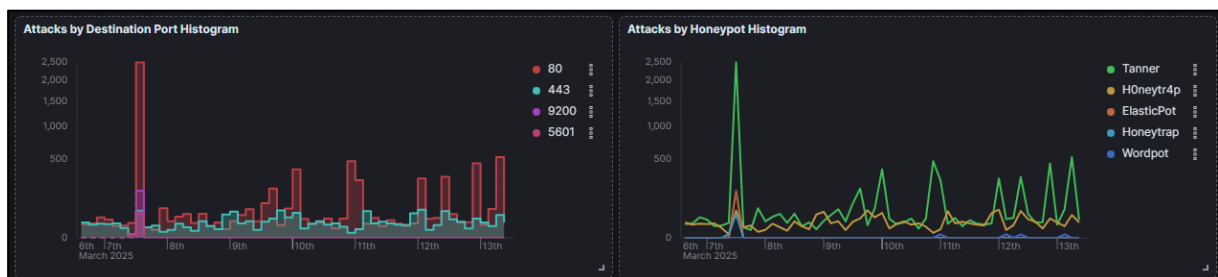


Із наведеного вище зображення помітно наступний розподіл по приманках:

- **Tanner:** ~7 тис. (82%) – (Імітація веб-сторінки GitLab -репозиторію);
- **Honeytr4p:** ~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).

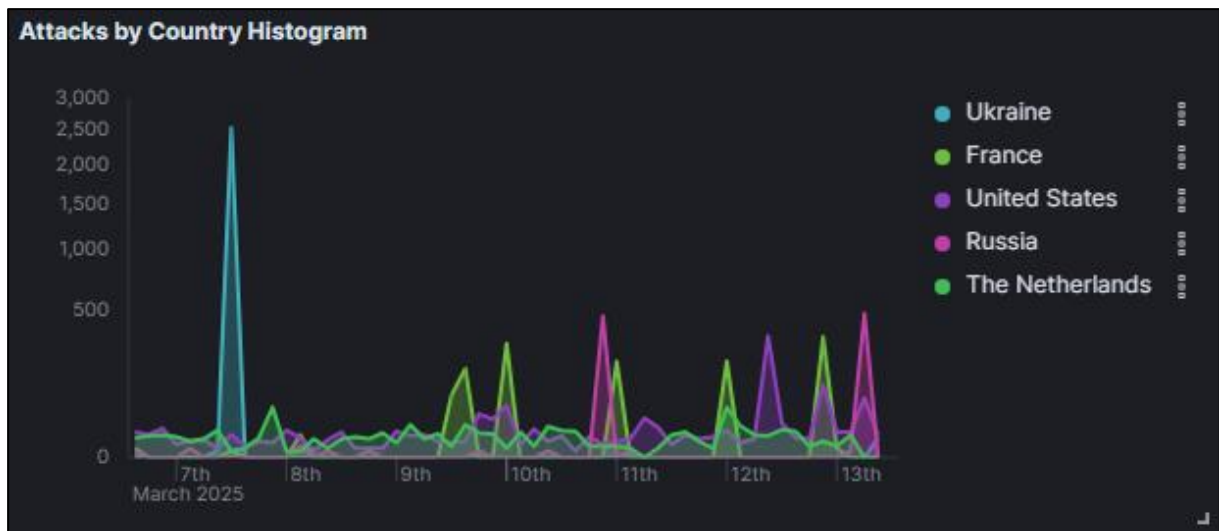
б. Огляд розподілу атак по портах

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

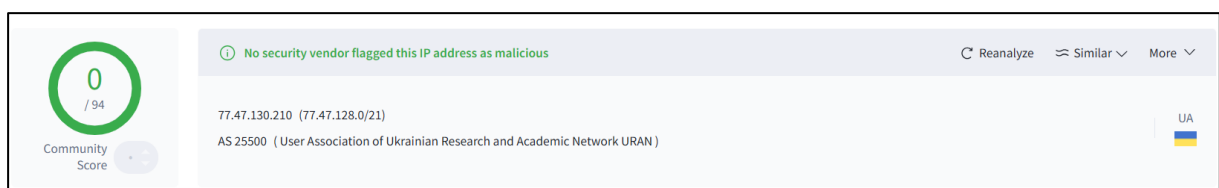


в. Огляд розподілу атак по країнах

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

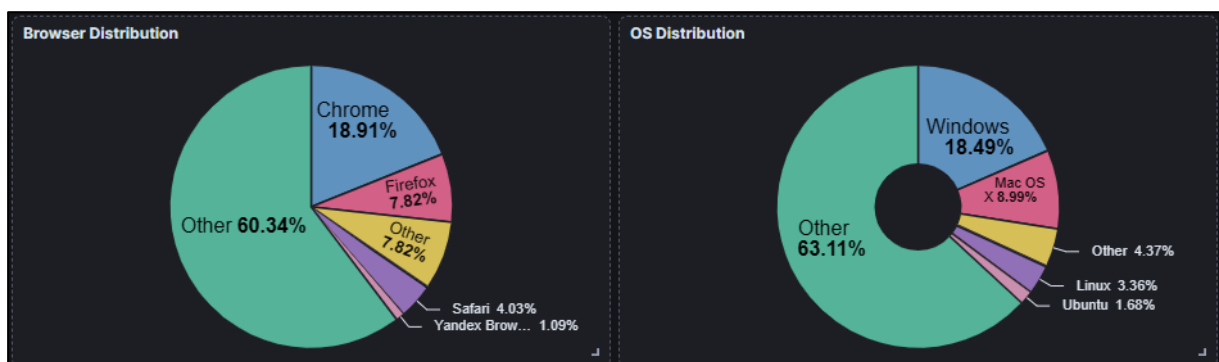


Окремо варто зауважити, що активність з **Ukraine (77.47.130.210)** становила 35% від усього трафіку, і вона була легітимна, оскільки здійснювалася в рамках проведення тестування на вразливості портів віртуальної машини:



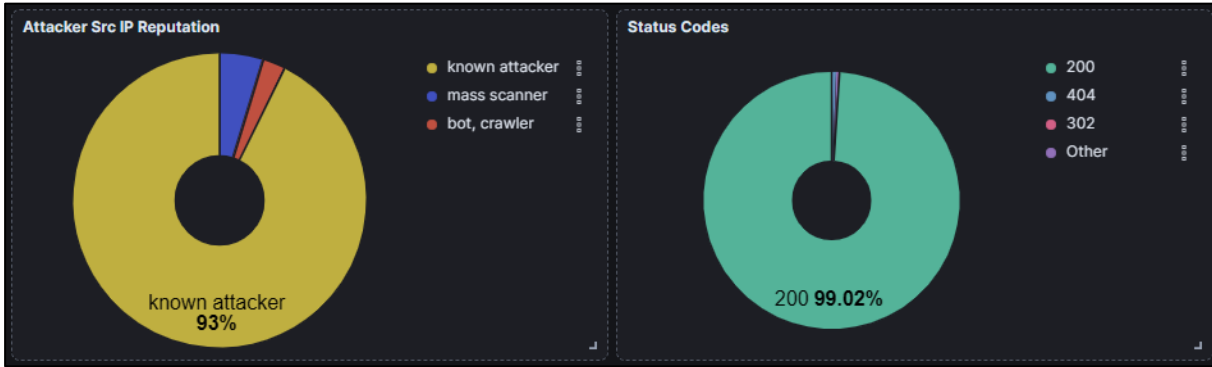
d. Огляд розподілу атак по User-Agent

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%):



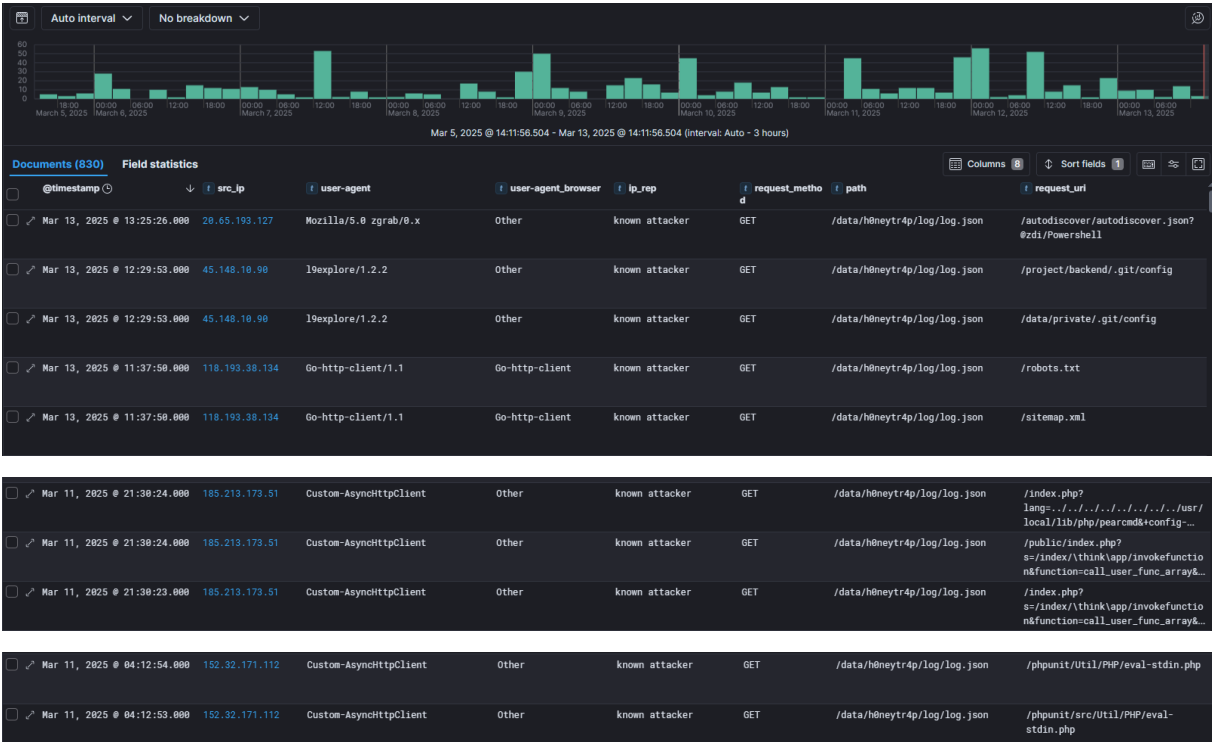
е. Перелік ботів та їх коди статусів

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:



ф. Задетектовані паттерни аномалій

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



г. 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
Mar 13, 2025 @ 11:33:26.424	77.47.138.210	UA	Chrome/134.0.0 Safari/537.36			
Mar 13, 2025 @ 11:33:26.131	77.47.138.210	UA	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0 Safari/537.36	GET	200	/assets/webpack/runtime.9fcb75d4.bundle.js
Mar 7, 2025 @ 13:08:08.793	77.47.138.210	UA	Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)	HEAD	200	/sitecore/system/Settings/Security/Profiles
Mar 7, 2025 @ 13:08:08.485	77.47.138.210	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	77.47.138.210	UA	Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)	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	77.47.138.210	UA	Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)	GET	200	/metacart/
Mar 7, 2025 @ 13:05:58.135	77.47.138.210	UA	Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)	GET	200	/messaging/
Mar 7, 2025 @ 13:05:57.825	77.47.138.210	UA	Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)	GET	200	/message/
Mar 7, 2025 @ 13:05:57.488	77.47.138.210	UA	Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)	GET	200	/mem/
Mar 7, 2025 @ 13:05:57.152	77.47.138.210	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	77.47.138.210	UA	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0 Safari/537.36	POST	200	/users/sign_in	admin	GitLab
Mar 13, 2025 @ 13:04:54.511	77.47.138.210	UA	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0 Safari/537.36	POST	200	/users/sign_in	username	password
Mar 13, 2025 @ 13:00:21.780	77.47.138.210	UA	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0 Safari/537.36	POST	200	/users/sign_in	student_ip1@111.kpi.ua	P@ssw@rd!
Mar 13, 2025 @ 12:59:58.820	77.47.138.210	UA	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0 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”.