UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH
Kompetenčné centrum kybernetickej bezpečnosti na UPJŠ

2025

Aktuálne kybernetické bezpečnostné hrozby 10/2024 – 4/2025 (analytický materiál)

Projekt Kompetenčné centrum kybernetickej bezpečnosti na UPJŠ (KCKB UPJŠ) financovaný Európskou úniou z prostriedkov Plánu obnovy a odolnosti Slovenskej republiky, kód projektu: 17R05-04-V01-00007.

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

OBSAH

ÚVOD

Tento dataset predstavuje ucelený súbor časových záznamov o sieťovej aktivite a kybernetických útokoch zachytených pomocou distribuovaného systému honeypotov v období od novembra 2024 do apríla 2025. Hlavným cieľom zberu dát bolo monitorovanie reálnych hrozieb v nekontrolovanom sieťovom prostredí a analýza správania botnetov alebo individuálnych útočníkov.

Dataset je štruktúrovaný do štyroch hlavných oblastí:

1. Analýza senzorov: Údaje zo šiestich špecializovaných honeypotov (Cowrie, Dionaea, Heralding, Honeytrap, Tanner, Mailoney) emulujúcich rôzne zraniteľné služby.
2. Cielené porty: Sledovanie intenzity útokov na najčastejšie zneužívané sieťové porty (22, 23, 445, 1433, 5900).
3. Intenzita a unikátnosť: Porovnanie celkového objemu útokov s počtom unikátnych zdrojových IP adries, čo umožňuje rozlíšiť medzi cielenými útokmi a distribuovanými kampaňami.
4. Geografická distribúcia: Mapovanie útokov na krajiny pôvodu pre identifikáciu regionálnych trendov v kybernetickej kriminalite.

Dáta sú predspracované do 30-minútových intervalov, čo umožňuje efektívnu časovú analýzu, detekciu anomálií a trénovanie modelov strojového učenia pre oblasť detekcie prienikov (IDS). Záznamy boli zbierané z obdobia od začiatku októbra 2024 do apríla 2025, avšak dáta od októbra do novembra neboli honeypotmi zaznamenané.

1 PREDSTAVENIE KC KB UPJŠ

Kompetenčné centrum kybernetickej bezpečnosti na Univerzite Pavla Jozefa Šafárika v Košiciach (KC KB UPJŠ) predstavuje kompetenčné centrum, v rámci ktorého sú realizované aktivity zamerané na vzdelávanie, výskum a expertnú činnosť v oblasti informačnej a kybernetickej bezpečnosti, ochrany dát, kyberkriminality a ochrany pred dezinformáciami. Súčasne KC KB UPJŠ realizuje medzinárodnú spoluprácu s akademickými partnermi zo zahraničia a poskytuje konzultácie pre možnosť prípravy a podania projektov v oblasti kybernetickej bezpečnosti.

Vytvorenie KC KB UPJŠ reflektuje viacero problémov, ktoré možno v súčasnosti identifikovať v oblasti informačnej a kybernetickej bezpečnosti (ďalej aj „KIB“):

- zvýšenie bezpečnostného povedomia relevantných subjektov zahŕňajúcich predovšetkým zamestnancov verejnej správy a študentov vysokoškolského a stredoškolského štúdia,
- vzdelávanie a výchova nových odborníkov pôsobiacich v tejto oblasti,
- výskum kybernetických hrozieb a identifikácia adekvátnych reakcií na tieto hrozby,
- zvýšenie operatívnej bezpečnosti v rámci verejnej správy poskytovaním expertných činností zo strany CSIRT tímu.

V rámci KC KB UPJŠ sa pripravoval študijný plán magisterského stupňa študijného programu aplikovaná informatika, ktorého jedna vetva sa zameriava na kybernetickú bezpečnosť. K tomuto študijnému plánu budú vytvorené, resp. modifikované viaceré predmety. Súčasne sa ako výstup kompetenčného centrá vytvára ponuka **vzdelávania** pre rôzne cieľové skupiny zamestnancov verejnej správy.

V kontexte projektu sa súčasne posilňuje **spolupráca so strednými školami**, najmä vo forme činnosti **KyberTímov**, ich vzdelávania a následného zapojenia do šírenia bezpečnostného povedomia medzi širokou verejnosťou.

V rámci vzdelávacích aktivít sa sumarizujú nové poznatky a skúsenosti z oblasti KIB, ale aj príbuzných oblastí. Tie sú aktuálne doplnené o rôzne formy zážitkového vzdelávania.

V rámci **výskumnej** činnosti dochádza v už existujúcich výskumných oblastiach k publikovaniu viacerých vedeckých výstupov a k vytvoreniu nových možných výskumných spoluprác na posilnenie výskumného a vývojového potenciálu KC KB UPJŠ.

Nemenej dôležitým výstupom projektu je doplnenie výbavy a vzdelávanie univerzitného CSIRT tímu a možnosť poskytovania **expertných činností** pre akreditované CSIRT tímy v SR za účelom rýchlejšej a adekvátnejšej reakcie na kybernetické bezpečnostné incidenty.

2 T-POT

T-Pot je honeypot platforma, cez ktorú vieme monitorovať a analyzovať útoky na infraštruktúru. Využíva pri tom viacero honeypotov, ktoré sú určené na simuláciu zraniteľného prostredia, prilákať útočníkov. Cieľom T-Pot je zachytávať metódy útokov, správanie útočníkov a zároveň poskytovať cenné dáta pre ďalšiu analýzu a zlepšenie bezpečnosti. T-Pot využíva široké spektrum honeypotov, z ktorých každý je navrhnutý na simuláciu konkrétneho typu služby alebo prostredia:

- **Cowrie** je zo skupiny honeypotov so strednou až vysokou úrovňou interakcie zameraný na služby SSH a Telnet. Zaznamenáva útoky hrubou silou na tieto služby. Vďaka nemu vieme aj analyzovať správanie útočníka, keďže zachytáva pokusy o vykonanie príkazov, vykonané príkazy aj logy o nahraných a stiahnutých súboroch.
- **Dionaea** emuluje Windows prostredie a služby so zraniteľnosťami a odchytáva malvér, ktorý ich zneužíva.
- **Heralding** je určený na zbieranie prihlasovacích údajov. Registruje pokusy o prihlásenie a teda deteguje brute-force útoky, zaznamenáva aj použité používateľské mená a heslá, čo sa dá využiť v prehľadoch o najčastejšie používaných heslách.
- **Mailoney** je SMTP honeypot s nízkou interakciou špecializovaný na mailové služby. Emuluje rôzne typy zraniteľností.
- **Tanner** sleduje útoky na službu RDP.
- **Adbhoney** je honeypot s nízkou úrovňou interakcie, špecificky navrhnutý na detekciu útokov zameraných na zariadenia s otvoreným portom 5555. Tento port je štandardne využívaný pre Android Debug Bridge (ADB)
- **Honeytrap** pôsobí ako bežiaca TCP alebo UDP služba. Je to honeypot s nízkou interakciou, ktorý bol vytvorený s myšlienkou odchytávania útokov na TCP a UDP služby.
- **ConPot** je ICS/SCADA honeypot, ktorý simuluje zraniteľné ICS/SCADA protokoly, a tak zhromažďuje informácie o motívoch a metódach útočníkov zameraných na priemyselné riadiace systémy.
- **CitrixHoneypot** je honeypot špecificky navrhnutý na emuláciu Citrix Gateway VPN, aby detegoval útoky na Citrix remote access.
- **ElasticPot** simuluje zraniteľný Elasticsearch server zverejnený na internete.
- **RedisHoneypot** simuluje zraniteľný Redis databázový server s neautorizovaným prístupom.
- **CiscoASA** honeypot je navrhnutý na detegovanie CVE-2018-0101, čo je zraniteľnosť týkajúca sa DoS a remote code execution.
- **DDoSPot** monitoruje Distributed Denial of Service (DDoS) útoky založené na UDP.

3 GRAFICKÁ VIZUALIZÁCIA CEZ KIBANA

Na vizualizáciu získaných dát z honeypotov sa používa nástroj Kibana, ktorý poskytuje dashboard, na ktorom vieme pozorovať dáta v rôznych preddefinovaných grafoch, ako aj vytvárať vlastné vizualizácie podľa potreby. Vďaka tomu je možné analyzovať trendy, vzory útokov a identifikovať potenciálne hrozby rýchlejšie a efektívnejšie.

Ako ukážka, schéma na Obr. č. 1 je zameraná na prehľad 10 honeypotov na ktoré sa útočí najviac. Hodnota zaznamenáva celkový počet útokov na daný honeypot za nejaké časové obdobie. Podľa názvu honeypotu vieme určiť aké typy útokov sú najčastejšie, keďže každý honeypot je zväčša zameraný na niečo špecifické.

Obr. č. 1 – Vizualizácia v Kibane, reprezentujúca 10 honeypotov, na ktoré sa najviac útočí.

Z tejto vizualizácie boli vytiahnuté dáta, týkajúce sa útokov na jednotlivé honeypoty, ktoré sledovali počet pokusov o útok zachytených rôznymi systémami honeypot v rôznych časových intervaloch. Nižšie je opísaný dataset z týchto dát.

4 Útoky na Honeypoty

Charakteristika datasetu: Viacrozmerný

Oblasť: Kybernetická bezpečnosť

Typ príznakov: Dátum a čas, Celé číslo

Počet inštancií: 7248

Počet príznakov: 7

Chýbajúce hodnoty: Nie

Časový rozsah: 4.11.2024 – 3.4.2025

Zdroj dát: Honeypoty

Tento dataset predstavuje počet pokusov o útok zachytených rôznymi systémami honeypot v rôznych časových intervaloch. Každý riadok zodpovedá konkrétnemu časovému obdobiu a každý príznak zaznamenáva počet útokov detegovaných konkrétnym systémom honeypot.

Názov premennej	Typ premennej	Chýbajúce údaje	Opis
Timestamp	Dátum a čas	Nie	Dátum a čas záznamu
Attack_counts_Cowrie	Celé číslo	Nie	Počet útokov zaznamenaných honeypotom Cowrie
Attack_counts_Dionaea	Celé číslo	Nie	Počet útokov zaznamenaných honeypotom Dionaea
Attack_counts_Heralding	Celé číslo	Nie	Počet útokov zaznamenaných honeypotom Heralding
Attack_counts_Honeytrap	Celé číslo	Nie	Počet útokov zaznamenaných honeypotom Honeytrap
Attack_counts_Tanner	Celé číslo	Nie	Počet útokov zaznamenaných honeypotom Tanner
Attack_counts_Mailoney	Celé číslo	Nie	Počet útokov zaznamenaných honeypotom Mailoney

Tab. č. 1 – Tabuľka premenných pre dataset Útoky na Honeypoty

Nasledujúca tabuľka sumarizuje popisnú štatistiku pre jednotlivé premenné datasetu. Tieto údaje umožňujú kvantifikovať priemernú záťaž monitorovaných senzorov a identifikovať extrémne výkyvy v aktivite útočníkov, ktoré môžu signalizovať prebiehajúce distribuované útoky alebo šírenie škodlivého kódu v sieti.

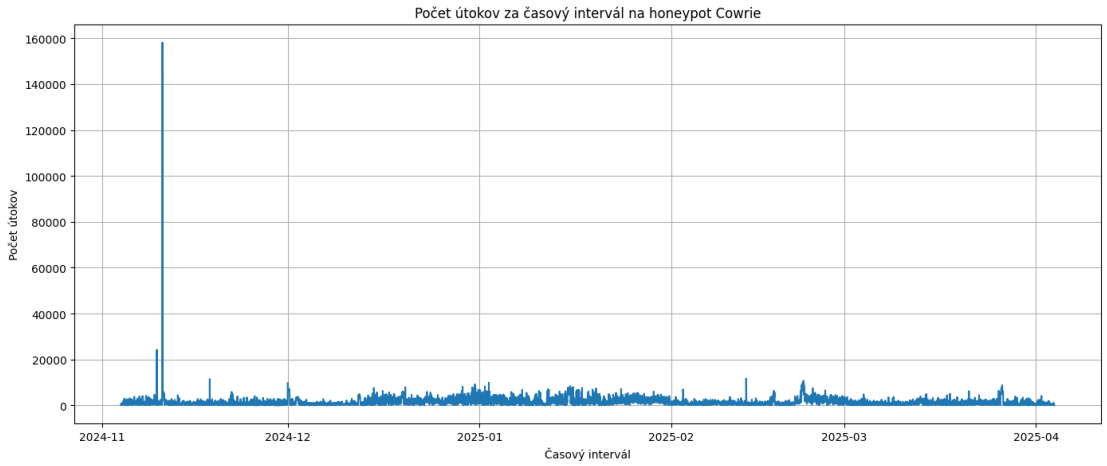
	Attack_counts_Cowrie	Attack_counts_Dionaea	Attack_counts_Heralding	Attack_counts_Honeytrap	Attack_counts_Tanner	Attack_counts_Mailoney
Počet	7248	7248	7248	7248	7248	7248
Priemer	1514	306,8	144,01	3,9	29,11	27,52
Štandardná odchýlka	2580	872,83	493,57	13,19	207,77	30,31
Minimálna hodnota	9	0	0	0	0	0
Maximálna hodnota	158130	5617	3102	627	7130	593

Tab. č. 2 – Štatistika pre dataset Útoky na Honeypoty

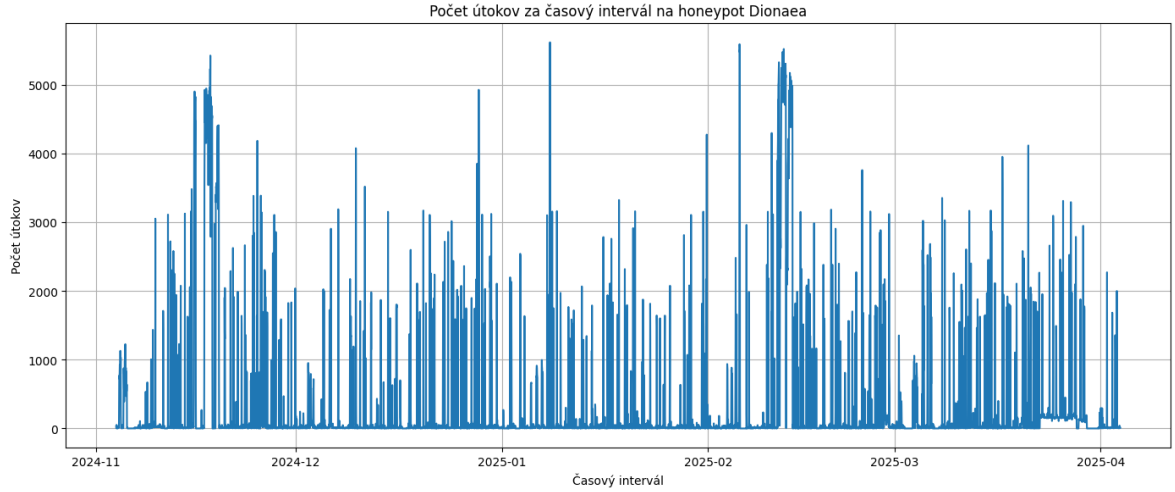
Výsledky sa dajú interpretovať tak, že honeypot Cowrie s priemernou hodnotou 1514 útokov na jeden časový interval je najvyťaženejší senzor. To potvrdzuje, že útoky na protokoly SSH a Telnet boli v dobe zachytenia dát najrozšírenejšou formou automatizovaných hrozieb.

Taktiež pri všetkých honeypotoch je štandardná odchýlka výrazne vyššia ako samotný priemer. Tento jav indikuje, že útoky nie sú rozložené rovnomerne, ale prebiehajú v intenzívnych nárazových vlnách.

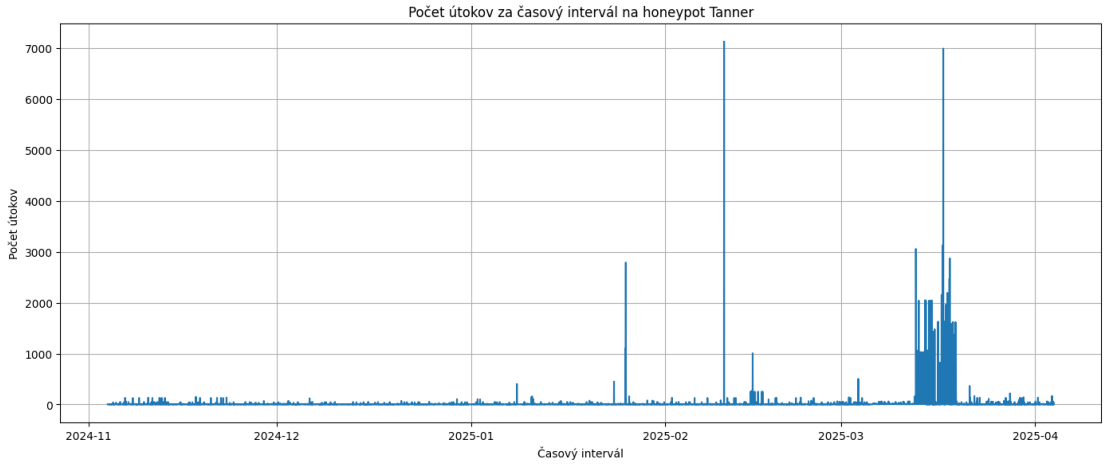
Maximum pri honeypote Cowrie (158130), hodnota pravdepodobne predstavuje masívny distribuovaný brute-force útok alebo rozsiahle skenovanie botnetom v jednom konkrétnom časovom okne. Toto maximum sa pravdepodobne dá namapovať na obdobie, kedy bola znížená funkčnosť univerzitného firewall-u a útoky boli vtedy častejšie. Nižšie sú uvedené grafické znázornenia počtu útokov pre každý z honeypotov.



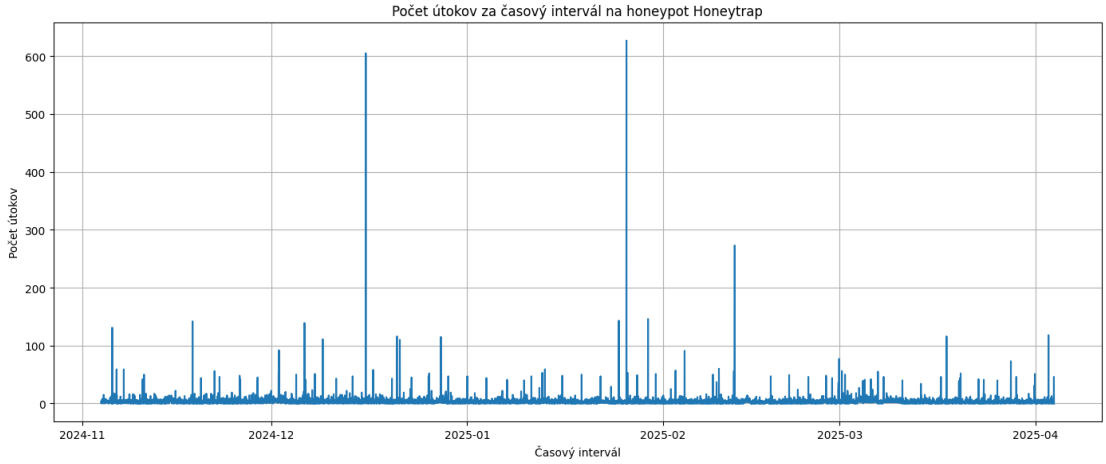
Obr. č. 2 – Počet útokov za časový interval na honeypot Cowrie



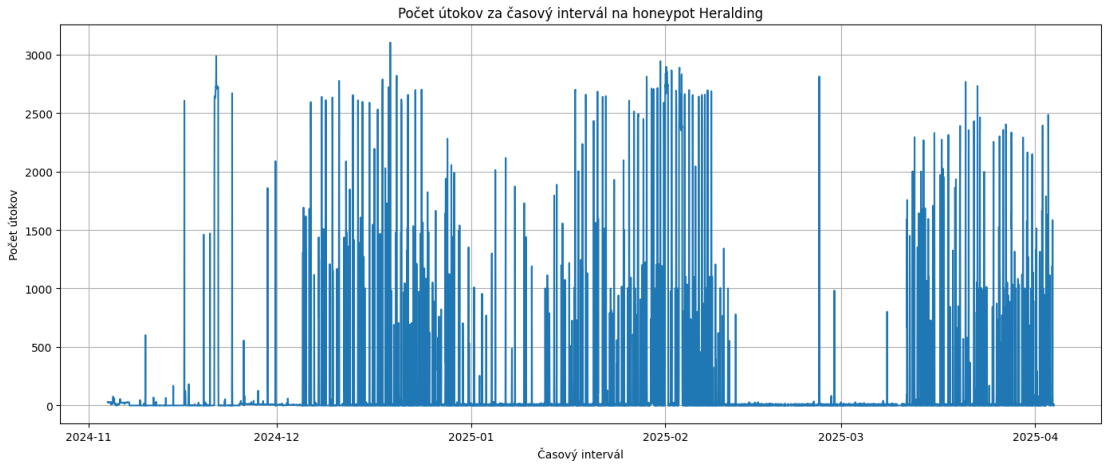
Obr. č. 3 – Počet útokov za časový interval na honeypot Dioanea



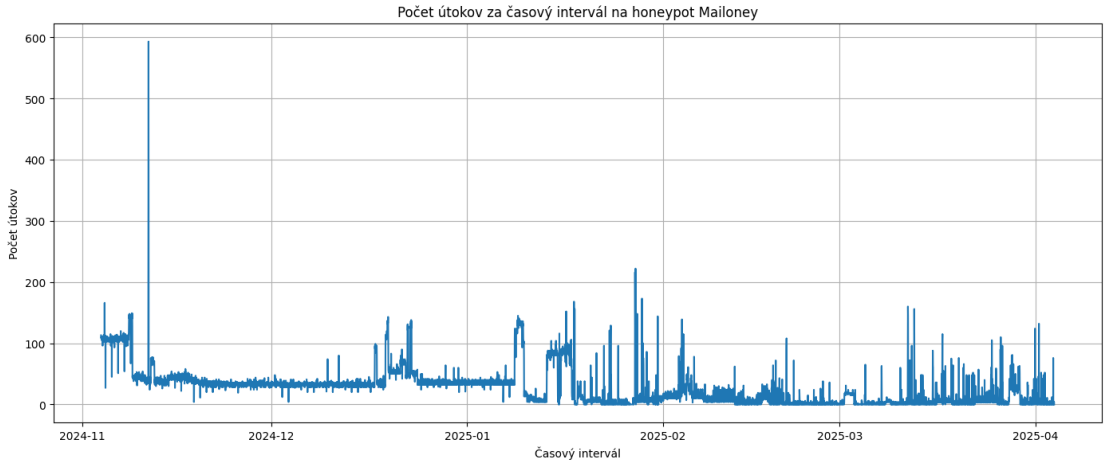
Obr. č. 4 – Počet útokov za časový interval na honeypot Tanner



Obr. č. 5 – Počet útokov za časový interval na honeypot Honeytrap



Obr. č. 6 – Počet útokov za časový interval na honeypot Heralding



Obr. č. 7 – Počet útokov za časový interval na honeypot Mailoney

5 ÚTOKY NA PORTY

Pri útokoch pozorujeme na aké cieľové porty sa útočí najčastejšie. Histogram nám napomáha pri vizualizácii, na aké cieľové služby a protokoly sa útočníci zameriavajú. Špecificky vidíme, že sa útočí na porty 445, 22, 5900, 1433, 23. Jednotlivé porty môžu mať viacero využití, no väčšinou sa viažu na štandardizované služby. Port 445 je bežne používaným portom pre TCP/UDP komunikáciu, hlavne v súvislosti so Server Message Block (SMB), ktorá sa používala na zdieľanie súborov vo Windows NT/2K/XP. V dnešnej dobe by mal byť port 445 zablokovaný na úrovni firewallu, aby sa minimalizovalo riziko zneužitia zraniteľností spojených so službou SMB. Port 5900 sa zväčša používa na vzdialené pripojenie k ploche, používaním VNC (Virtual Network Computing) protokolu. V prípade portu 1433 ide o štandardný port pre komunikáciu s SQL Server. Port 23 je zaužívaným portom pre službu Telnet, ktorá má viacero bezpečnostných zraniteľností, najmä kvôli absencii šifrovania. Port 22 je zaužívaným portom pre Secure Shell (SSH), čo je služba, ktorá nahradila Telnet a poskytuje šifrovanie komunikácie. Je cieľom útokov, vďaka svojej rozšírenosti v sieťových prostrediach, preto sa útočníci snažia získať prístup do nej napríklad cez brute-force útoky.

CHARAKTERISTIKA DATASETU: Viacrozmerný

OBLASŤ: Kybernetická bezpečnosť

TYP PRÍZNAKOV: Dátum a čas, Celé číslo

POČET INŠTANCIÍ: 7248

POČET PRÍZNAKOV: 6

CHÝBAJÚCE HODNOTY: Nie

ČASOVÝ ROZSAH: 4.11.2024 – 3.4.2025

ZDROJ DÁT: Honeypoty

Tento dataset obsahuje časové záznamy pokusov o útok zachytených monitorovacím systémom honeypot. Každý riadok zodpovedá konkrétnemu časovému obdobiu a každý príznak predstavuje počet detegovaných útokov na špecifické porty, ktoré sú bežnými cieľmi útočníkov.

Názov premennej	Typ premennej	Chýbajúce údaje	Opis
Timestamp	Dátum a čas	Nie	Dátum a čas záznamu
Attack_counts_22	Celé číslo	Nie	Počet útokov na port 22
Attack_counts_23	Celé číslo	Nie	Počet útokov na port 23
Attack_counts_445	Celé číslo	Nie	Počet útokov na port 445
Attack_counts_1433	Celé číslo	Nie	Počet útokov na port 1433
Attack_counts_5900	Celé číslo	Nie	Počet útokov na port 5900

Tab. č. 3 – Tabuľka premenných pre dataset Útoky na porty

Nasledujúca tabuľka sumarizuje popisnú štatistiku pre jednotlivé premenné datasetu. Tieto údaje umožňujú kvantifikovať priemernú záťaž monitorovaných senzorov a identifikovať extrémne výkyvy v aktivite útočníkov, ktoré môžu signalizovať prebiehajúce distribuované útoky alebo šírenie škodlivého kódu v sieti.

	Attack_counts_22	Attack_counts_23	Attack_counts_445	Attack_counts_1433	Attack_counts_5900
Počet	7248	7248	7248	7248	7248
Priemer	116.59	34.86	175.21	126.08	142.64

Štandardná odchýlka	151.33	38.62	524.6	694.42	493.75
Minimálna hodnota	1	0	0	0	0
Maximálna hodnota	1670	868	5613	5579	3102

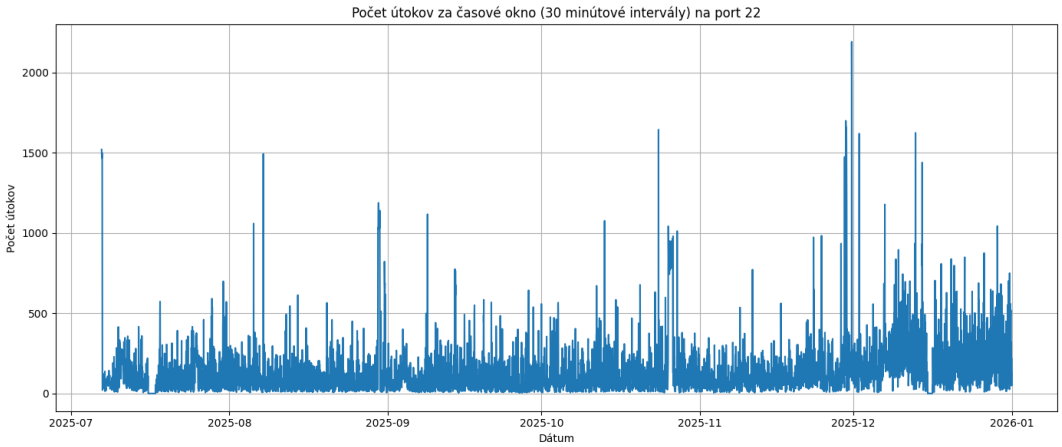
Tab. č. 3 – Štatistika pre dataset Útoky na porty

S priemerným počtom 175,21 útokov na záznam ide o najčastejší cieľ. Keďže ide o port využívaný na zdieľanie súborov vo Windowse, vysoké čísla naznačujú pretrvávajúcu snahu o šírenie ransomvéru a botnetov.

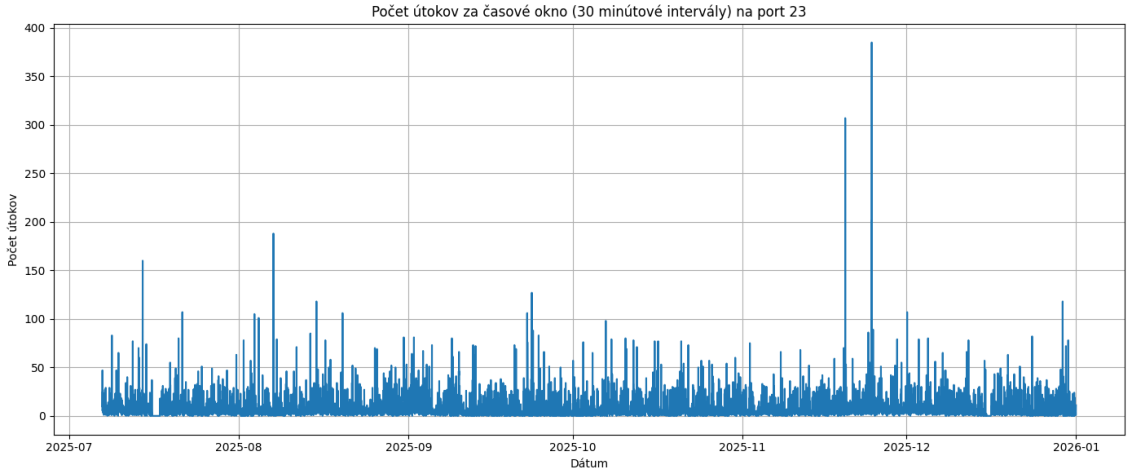
Podobne ako pri útokoch na všetky honeypoty štandardná odchýlka pri portoch 445 a 1433 naznačuje, že útoky nie sú plynulé, ale prebiehajú v masívnych, nárazových vlnách. Maximálna hodnota 5613 útokov za jeden záznam pri porte 445 je dôkazom.

Hoci má port 22 vysoký priemer jeho minimálna hodnota nikdy neklesla na nulu. To znamená, že pokusy o brute-force na SSH prebiehajú prakticky nepretržite, čo nie je pri univerzitnom prostredí prekvapivé.

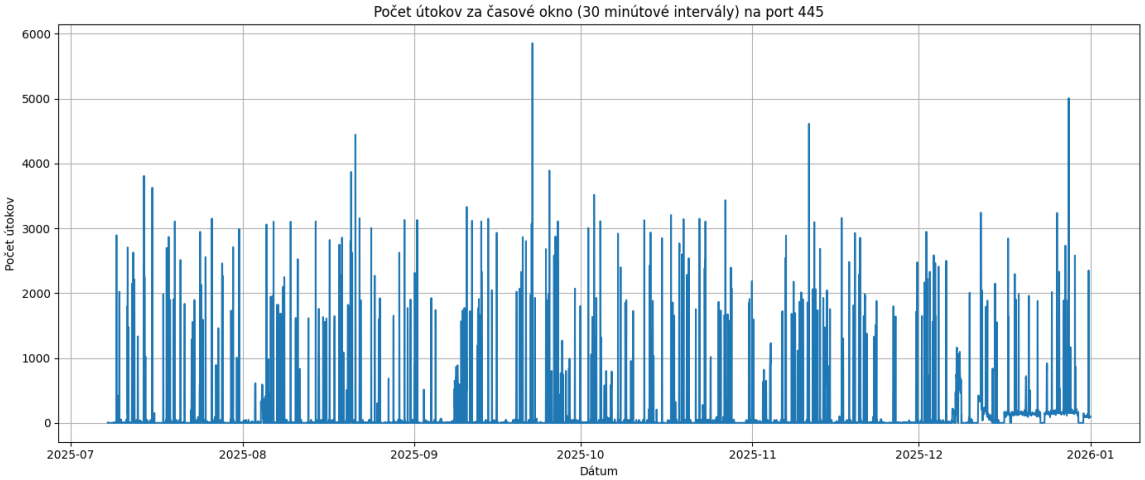
Pod útokom sú aj porty 1433 a 5900 vykazujú veľmi podobné vzorce správania a to relatívne nízky medián, ale obrovské maximá, čo svedčí o cielených skenovacích kampaniach.



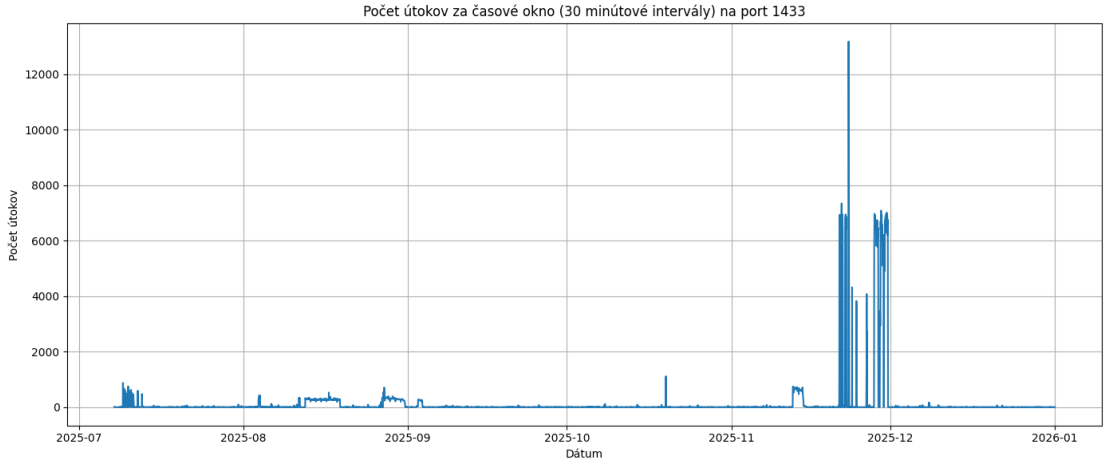
Obr. č. 8 – Počet útokov za časové okno na port 22



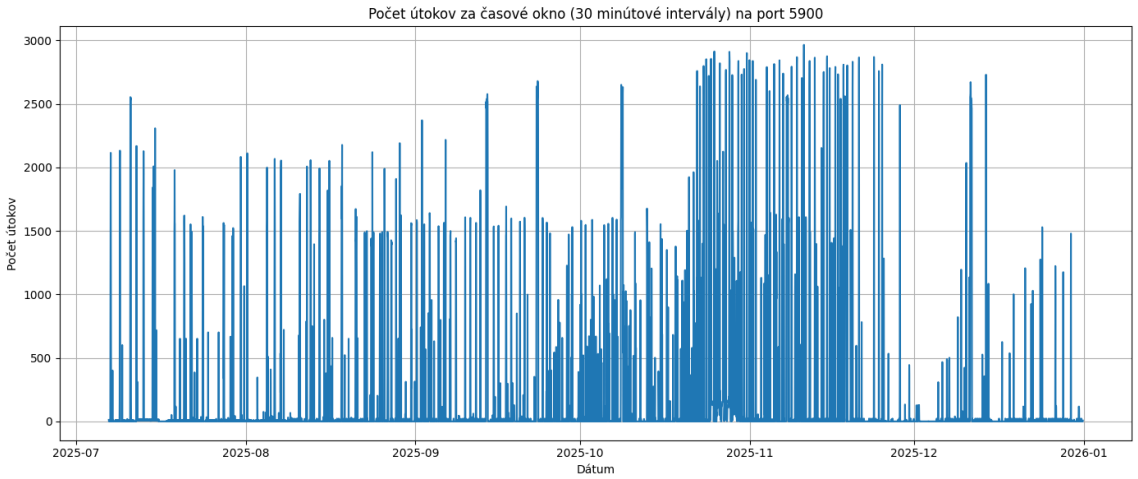
Obr. č. 9 – Počet útokov za časové okno na port 23



Obr. č. 10 – Počet útokov za časové okno na port 445



Obr. č. 11 – Počet útokov za časové okno na port 1433



Obr. č. 11 – Počet útokov za časové okno na port 5900

6 Počet všetkých útokov a unikátnych zdrojových IP adries

Pri tomto datasete špecificky pozorujeme počet útokov, no zároveň počet unikátnych zdrojových IP adries, takže či útoky pochádzajú od nejakého nového zariadenia, alebo ide o opakované aktivity známych útočníkov. Taktiež vidíme, či útoky prebiehajú konštantne alebo vo vlnách. Výrazný nárast počtu unikátnych zdrojových IP adries môže indikovať potenciálne zlyhanie alebo nedostatočnú účinnosť existujúcich bezpečnostných mechanizmov.

Charakteristika datasetu: Viacrozmerný

Oblasť: Kybernetická bezpečnosť

Typ príznakov: Dátum a čas, Celé číslo

Počet inštancií: 7248

Počet príznakov: 3

Chýbajúce hodnoty: Nie

Časový rozsah: 4.11.2024 – 3.4.2025

Zdroj dát: Honeypoty

Tento dataset predstavuje časové dáta o počte útokov a počte unikátnych IP adries zapojených do pokusov o útok v rámci konkrétnych časových intervalov.

Názov premennej	Typ premennej	Chýbajúce údaje	Opis
Timestamp	Dátum a čas	Nie	Dátum a čas záznamu

Attack_counts	Celé číslo	Nie	Počet pokusov o útok zachytený za daný časový interval
Unique_ips	Celé číslo	Nie	Počet unikátnych IP adries zapojených do pokusov o útok

Tab. č. 4 – Tabuľka premenných pre dataset Počet všetkých útokov a unikátnych zdrojových IP adries

Nasledujúca tabuľka sumarizuje popisnú štatistiku pre jednotlivé premenné datasetu. Tieto údaje umožňujú kvantifikovať priemernú záťaž monitorovaných senzorov a identifikovať extrémne výkyvy v aktivite útočníkov, ktoré môžu signalizovať prebiehajúce distribuované útoky alebo šírenie škodlivého kódu v sieti.

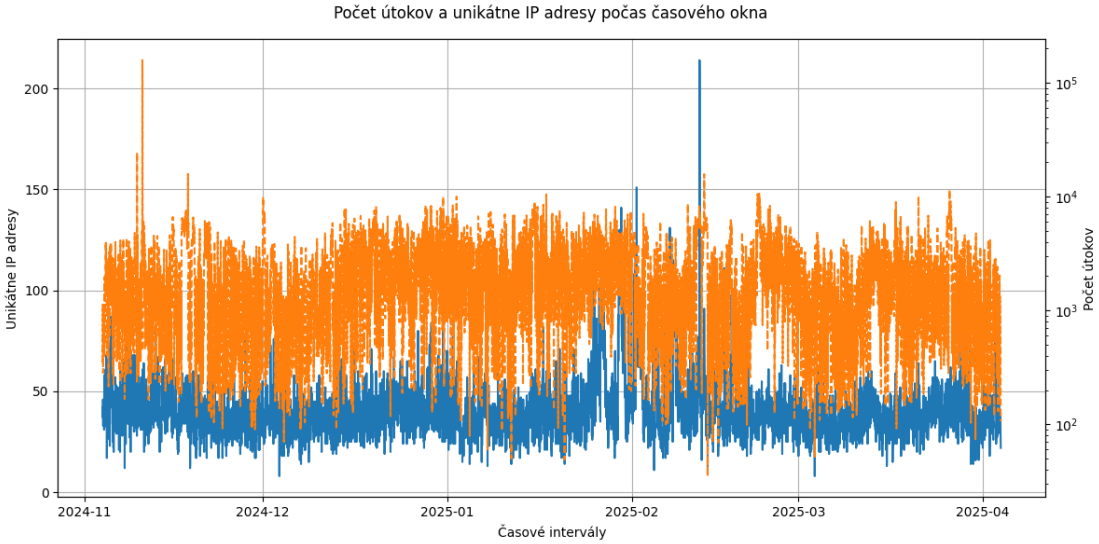
	Attack_counts	**Unique_ips**
Počet	7248	7248
Priemer	2037.65	40.37
Štandardná odchýlka	2732.53	14.16
Minimálna hodnota	35	8
Maximálna hodnota	158217	214

Tab. č. 5 – Štatistika pre dataset Počet všetkých útokov a unikátnych zdrojových IP adries

Priemerný počet útokov v porovnaní s priemerným počtom unikátnych IP adries naznačuje, že jedna IP adresa vykoná v priemere približne 50 útokov v rámci sledovaného intervalu. To svedčí o vysokej miere automatizácie (skripty, botnety).

Štandardná odchýlka (Attack_counts) je vyššia ako samotný priemer. To znamená, že aktivita útočníkov nie je konštantná, ale prebieha v nárazových vlnách, čo je pre DDoS alebo brute-force útoky typické.

Štandardná odchýlka (Unique_ips) u unikátnych IP adries je relatívne nízka v pomere k priemeru. To naznačuje, že hoci intenzita útokov prudko kolíše, infraštruktúra útočníkov (počet zapojených zariadení) zostáva stabilnejšia.



Obr. č. 12 – Počet útokov a unikátne IP adresy počas časového okna

7 POČET ÚTOKOV PODĽA KRAJINY PÔVODU

Počet útokov z krajín v tomto datasete nepredstavuje útoky konkrétnych skutočných útočníkov, ale krajiny zariadení, ktoré boli infikované a zneužité na vykonávanie útokov. Tieto útoky sú zväčša automatizované a prebiehajú cez botnety alebo malvér. Dataset teda neukazuje, že konkrétna krajina útočí viac než iná, ale skôr zobrazuje geografické umiestnenie zariadení, ktoré boli infikované a využité na útoky.

CHARAKTERISTIKA DATASETU: Viacrozmerný

OBLASŤ: Kybernetická bezpečnosť

TYP PRÍZNAKOV: Dátum a čas, Celé číslo, Kategorický

POČET INŠTANCIÍ: 45577

POČET PRÍZNAKOV: 3

CHÝBAJÚCE HODNOTY: Nie

ČASOVÝ ROZSAH: 4.11.2024 – 3.4.2025

ZDROJ DÁT: Honeypoty

Tento dataset predstavuje časové dáta o počte útokov a počte unikátnych IP adries zapojených do pokusov o útok v rámci konkrétnych časových intervalov.

Názov premennej	Typ	Chýbajúce hodnoty	Opis

Timestamp	Dátum a čas	Nie	Dátum a čas záznamu
Attacks	Celé číslo	Nie	Počet pokusov o útok zachytený za daný časový intervál
Country	Kategorický	Nie	Zdrojová krajina útoku

Tab. č. 6 – Štatistika pre dataset Počty útokov podľa krajiny pôvodu

Nasledujúca tabuľka sumarizuje popisnú štatistiku pre jednotlivé premenné datasetu. Tieto údaje umožňujú kvantifikovať priemernú záťaž monitorovaných senzorov a identifikovať extrémne výkyvy v aktivite útočníkov, ktoré môžu signalizovať prebiehajúce distribuované útoky alebo šírenie škodlivého kódu v sieti.

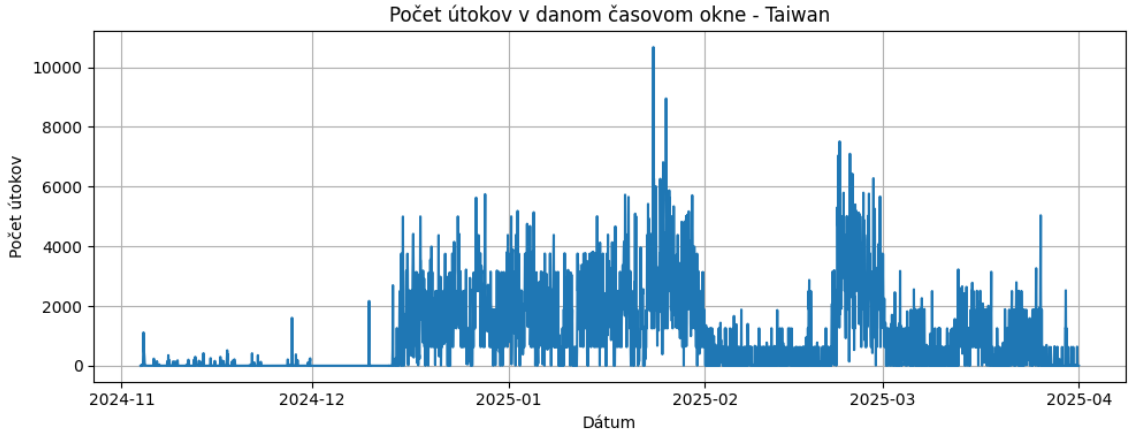
Krajina	**Počet**	**Priemer**	**Štandardná odchýlka**	**Minimálna hodnota**	**Maximálna hodnota**	**Počet útokov podľa krajiny**
Čína	7213	162.83	303.2	1	4338	1174484
Estónsko	415	911.1	992.83	1	3102	378106
Francúzsko	3663	344.162	1002.54	1	7114	1260667
Nemecko	4475	113.73	2734.02	1	155349	508930
India	6285	108.55	304.95	1	4575	682237
Indonézia	2850	125.46	213.01	1	3031	357563
Rusko	5191	91.77	286.69	1	4417	476393
Južná Kórea	4046	99.6	219.45	1	2726	402975
Taiwan	4240	826.52	816.9	1	6289	3504450
Spojené štáty	7198	161.58	434.56	1	5190	1163085

Tab. č. 7 – Štatistika pre dataset Počty útokov podľa krajiny pôvodu

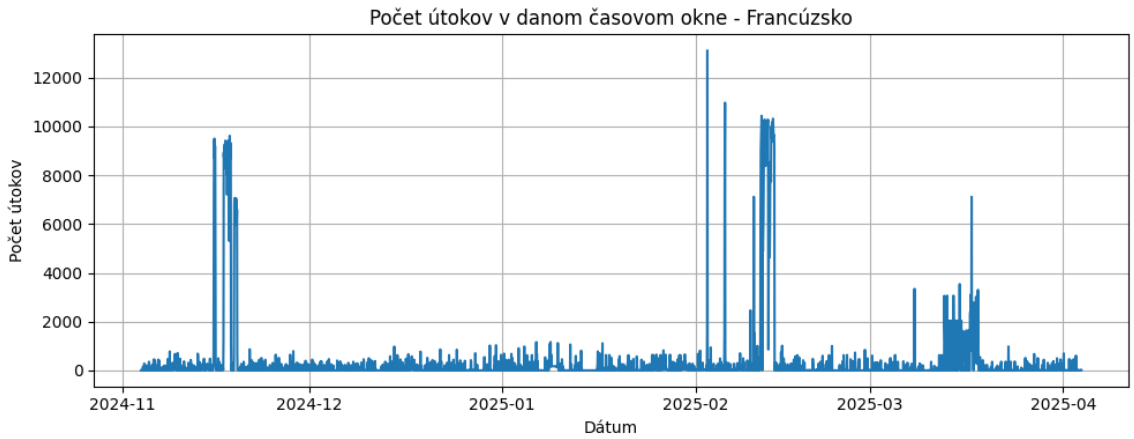
Hoci Čína a USA majú najvyšší počet záznamov (inštancií v čase), Taiwan je jednoznačným lídrom v celkovom objeme útokov. Je teda možné že Taiwan môže hostovať infraštruktúru, ktorá je buď extrémne zraniteľná, alebo cielene využívaná automatizované skenovanie.

Priemerný počet útokov z Nemecka je relatívne nízky, no obrovská štandardná odchýlka a maximum naznačujú krátkodobé, ale masívne DDoS útoky alebo nárazové kampane malvéru, ktoré sa výrazne vymykajú bežnému šumu.

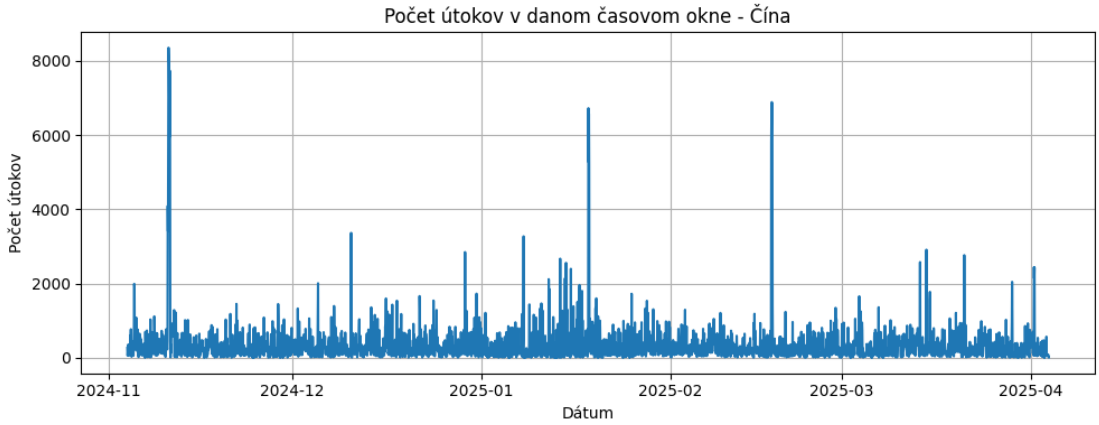
Čína, USA, India majú vysoký počet záznamov, čo značí neustálu prítomnosť v sieti. Vzhľadom na obrovskú populáciu a počet zariadení v týchto krajinách je prirodzené, že tvoria stabilný základ botnetov.



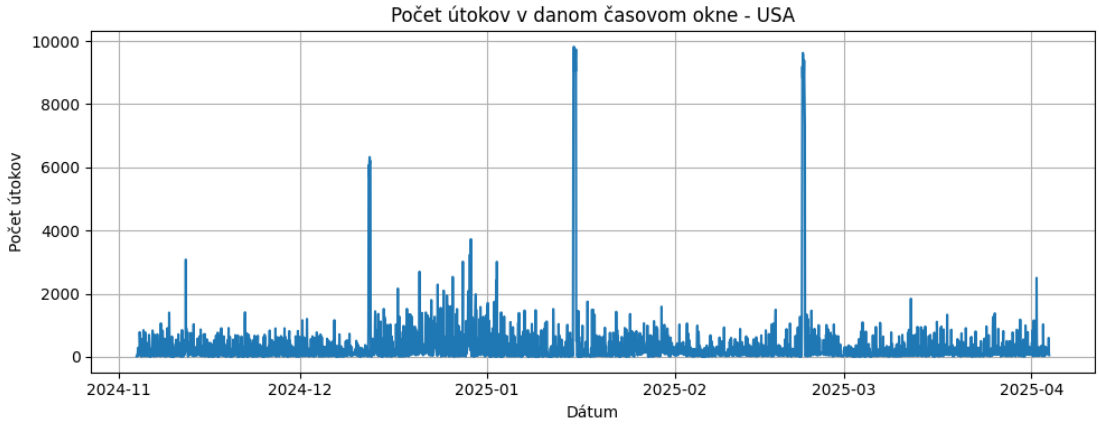
Obr. č. 13 – Počet útokov v danom časovom okne z krajiny Taiwan



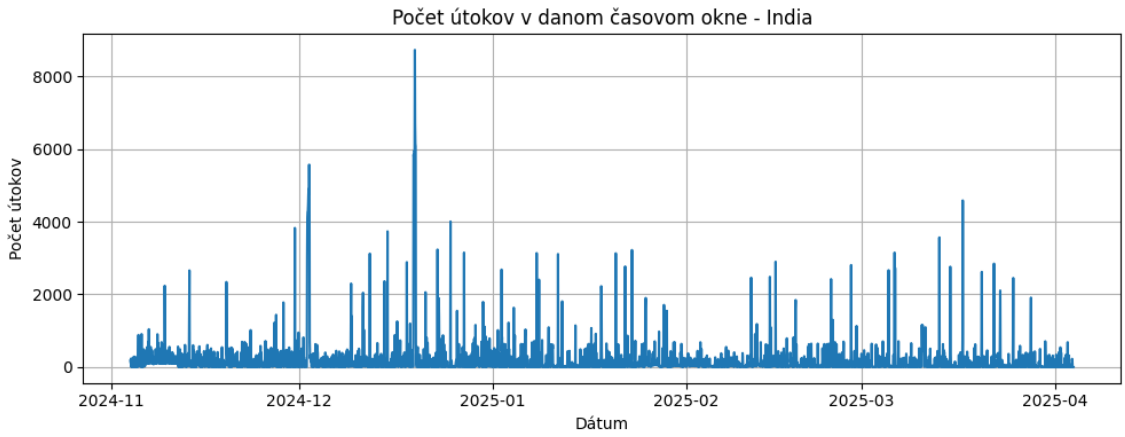
Obr. č. 14 – Počet útokov v danom časovom okne z krajiny Francúzsko



Obr. č. 15 – Počet útokov v danom časovom okne z krajiny Čína

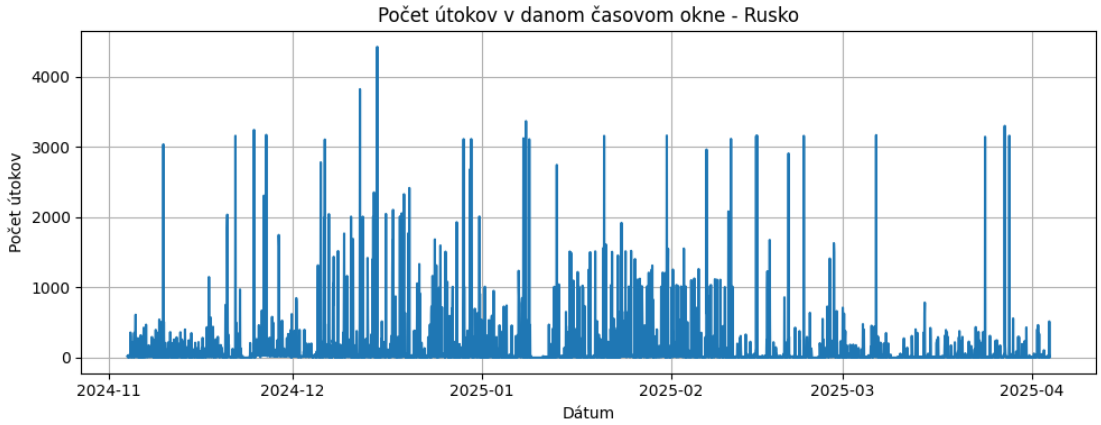


Obr. č. 16 – Počet útokov v danom časovom okne z krajiny USA

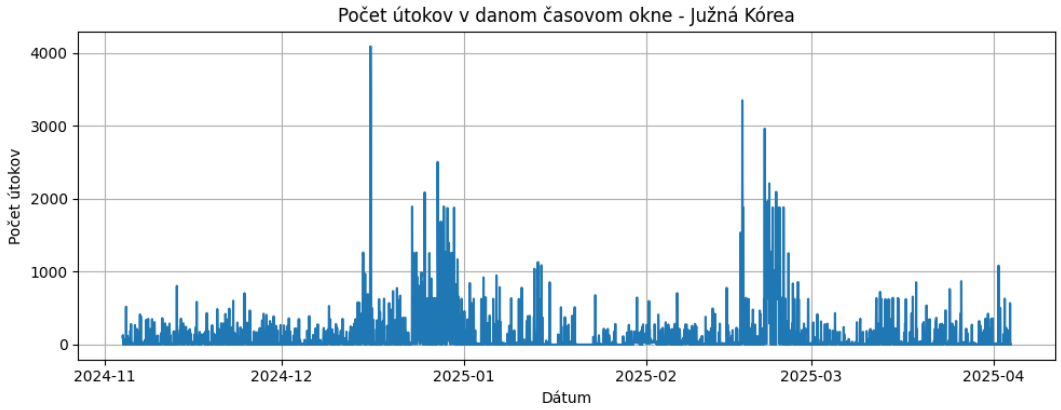


Obr. č. 17 – Počet útokov v danom časovom okne z krajiny India

Obr. č. 18 – Počet útokov v danom časovom okne z krajiny Nemecko

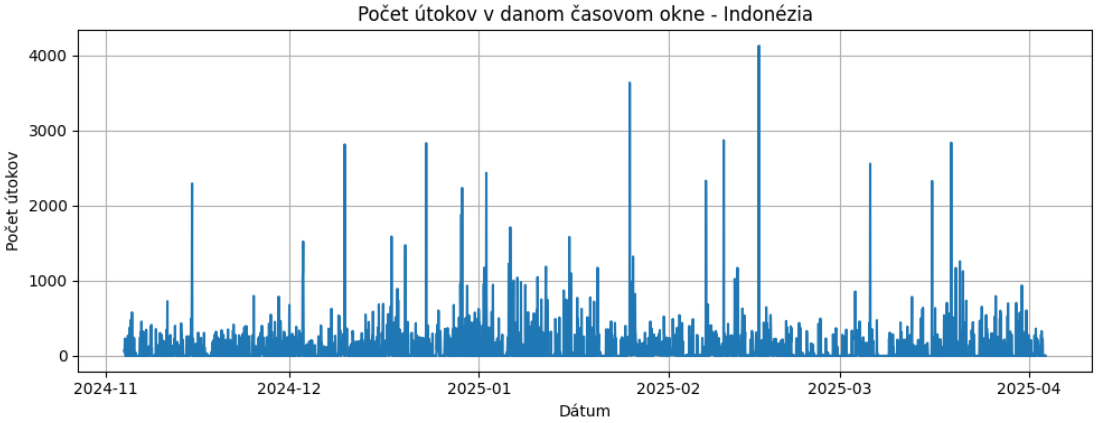


Obr. č. 19 – Počet útokov v danom časovom okne z krajiny Rusko



Obr. č. 20 – Počet útokov v danom časovom okne z krajiny Južná Kórea

Obr. č. 21 – Počet útokov v danom časovom okne z krajiny India



Obr. č. 21 – Počet útokov v danom časovom okne z krajiny Indonézia

ZÁVER

Honeypoty sú dôležitým nástrojom na monitorovanie aktuálneho stavu kybernetických hrozieb v reálnom čase. Na základe získaných dát z obdobia od novembra 2024 do apríla 2025 je možné definovať nasledujúce závery. Najvyťaženejším senzorom bol honeypot Cowrie, zameraný na protokoly SSH a Telnet. Extrémne vysoký nepomer medzi počtom útokov a unikátnymi IP adresami nám potvrdzuje činnosť botnetov a skriptov, ktoré sú automatizované.

Pri cieľových portoch boli najčastejším čieľom útokov port 445 (SMB), takže je pravdepodobné, že útočníci sa snažili šíriť ransomvér a zneužívať zraniteľnosti v rámci zdieľania súborov. Port 22 (SSH) vykazuje nepretržitú aktivitu, čo reprezentuje nepretržituú snahu o brute-force útoky. Databázové a VNC služby (1433, 5900) sú cieľom nárazových, vysoko intenzívnych kampaní, čo svedčí o cielenom hľadaní zle zabezpečených dátových úložísk.

Z geografického hľadiska dominujú krajiny s rozsiahlou infraštruktúrou (Čína, USA, India), avšak extrémne objemy dát zaznamenané z oblastí ako Taiwan naznačujú prítomnosť botnetov, ktoré sú aktívne využívané na distribuované útoky.