Analýza bezpečnostných udalostí z pohľadu času a priestoru

Pavol Sokol
Pavol Jozef Šafárik University in Košice
Prírodovedecká fakulta, Ústav informatiky

Kto sme?

Laboratórium kybernetickej bezpečnosti

- Výskum
- Vzdelávanie
- Operatívna činnosť – CSIRT-UPJS

Výskumné zámery

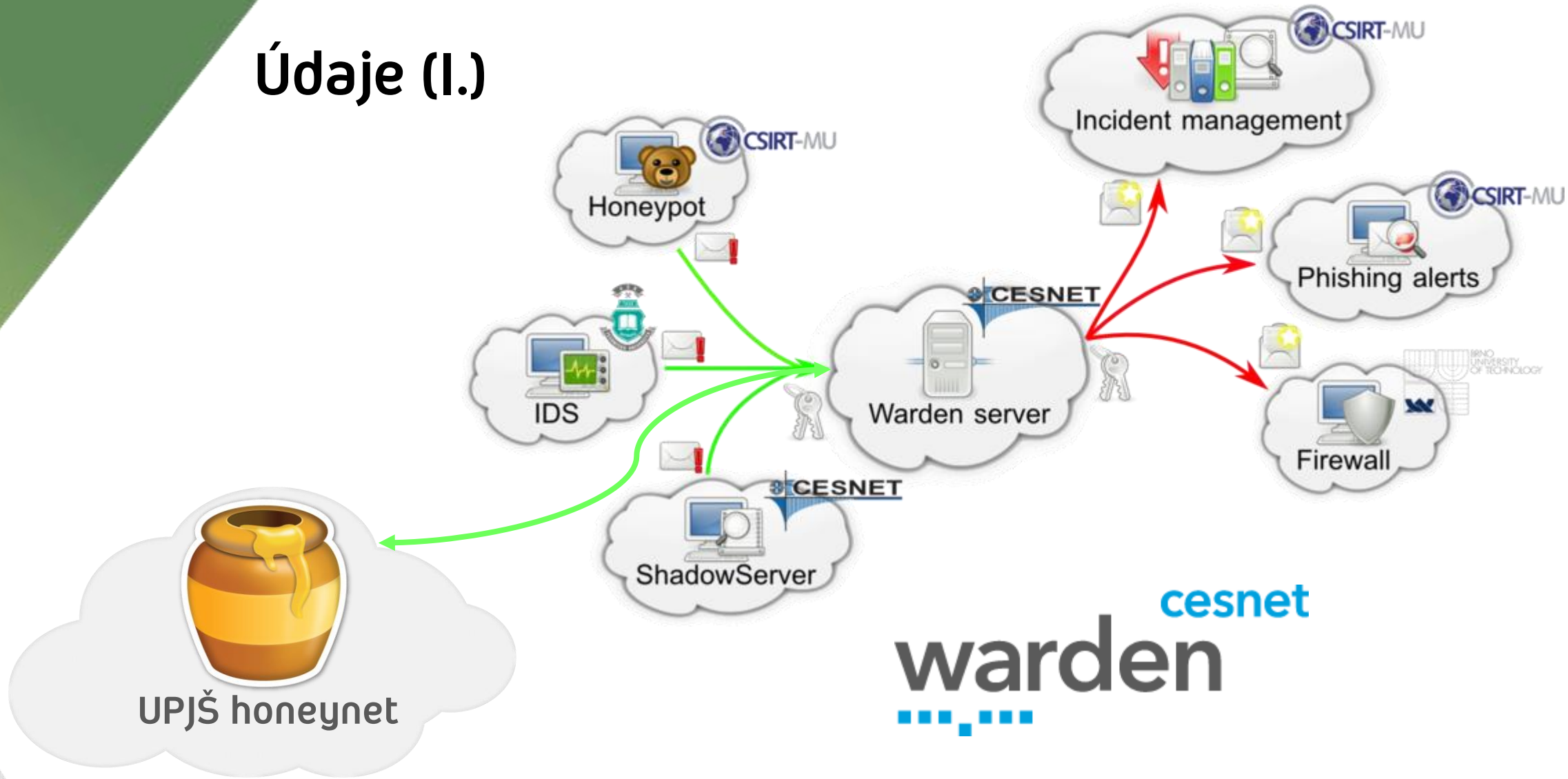
Detekcia a predikcia bezpečnostných útokov a udalostí

Analýza bezpečnostných hrozieb

Modelovanie správania útočníkov

Honeypoty (pasce na útočníkov)

Údaje (I.)



Zdroj: https://warden.cesnet.cz/cs/architecture

Údaje (II.)

Čas

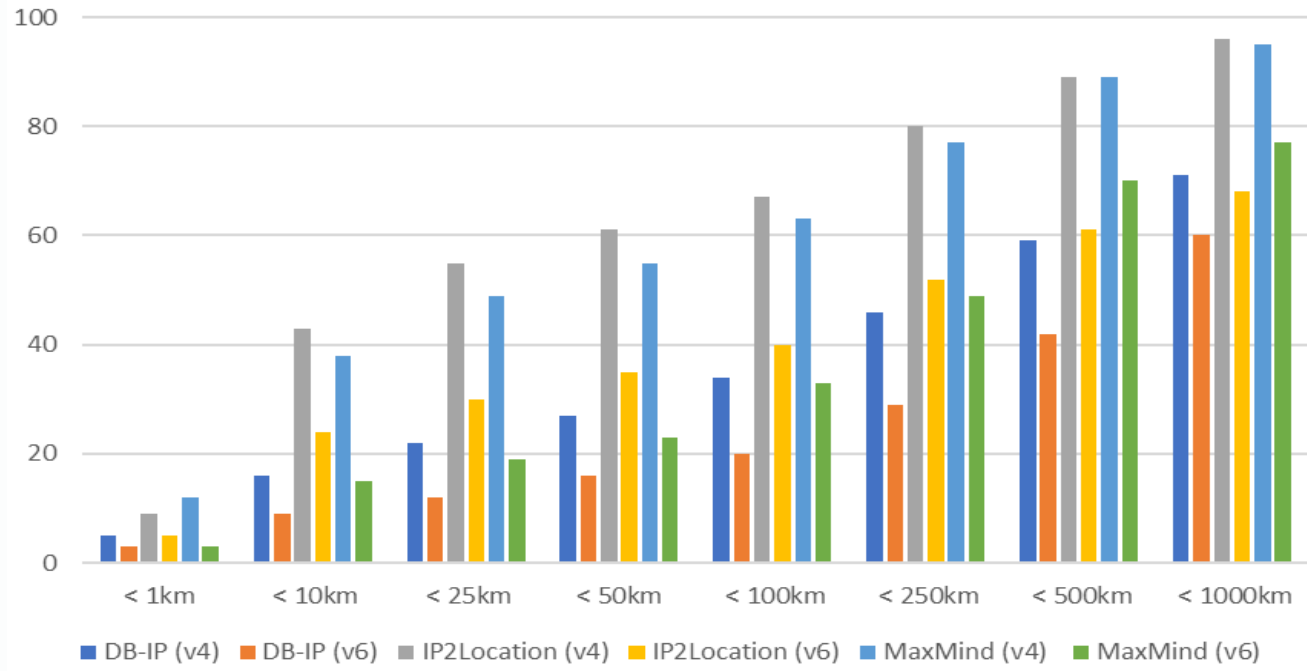
Geolokácia


```
{
 "Format": "IDEA0",
 "ID": "4390fc3f-c753-4a3e-bc83-1b44f24baf75",
 "CreateTime": "2019-06-03T10:00:02Z",
 "DetectTime": "2019-06-03T10:00:07Z",
 "EventTime": "2019-06-03T07:36:00Z",
 "Category": ["Fraud.Phishing"],
 "Ref": ["cve:CVE-1234-5678"],
 "Confidence": 1,
 "Note": "Synthetic example",
 "ConnCount": 20,
 "Source": [
    {
       "Type": ["Phishing"],
       "IP4": ["192.168.0.10/25"],
       "Hostname": ["example.com"],
       "URL": ["http://example.com/cgi-bin/killemall"],
       "Proto": ["tcp", "http"],
    }
 ], ...
 "Node": [
    {
       "Name": "cz.cesnet.kippo-honey",
       "Type": ["Protocol", "Honeypot"],
       "SW": ["Kippo"],
       "AggrWin": "00:05:00"
    }
 ]
}
```

Geolokácia

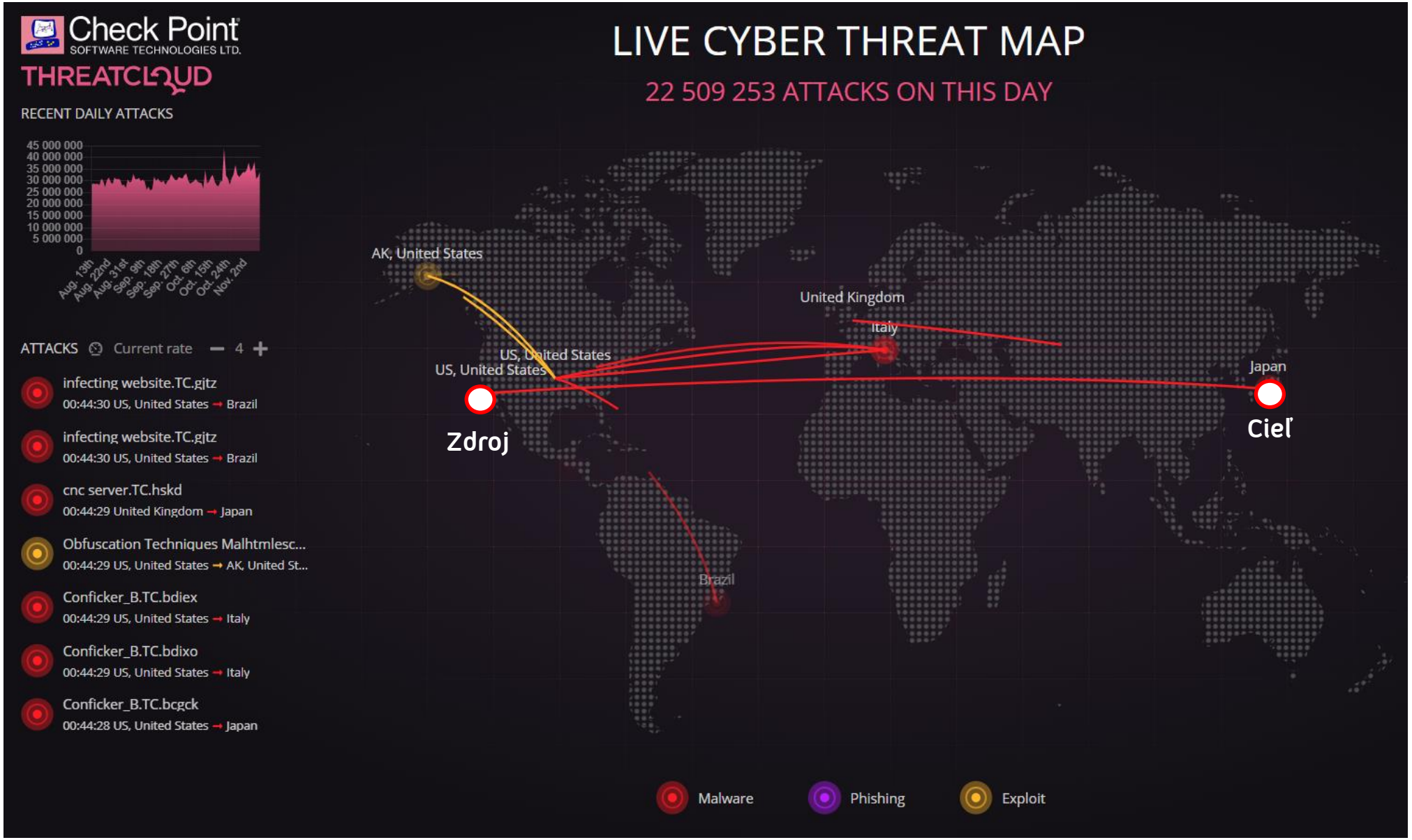
Geolokačné databázy


```
{
    "query": "158.197.16.80",
    "status": "success",
    "continent": "Europe",
    "continentCode": "EU",
    "country": "Slovakia",
    "countryCode": "SK",
    "region": "KI",
    "regionName": "Kosice",
    "city": "Košice",
    "district": "Kosice",
    "zip": "040 12",
    "lat": 48.7192,
    "lon": 21.2512,
    "timezone": "Europe/Bratislava",
    "offset": 3600,
    "currency": "EUR",
    "isp": "Zdruzenie pouzivatelov Slovenskej akademickej datovej
siete",
    "org": "P. J. Safarik University in Kosice",
    "as": "AS2607 Zdruzenie pouzivatelov Slovenskej akademickej datovej
siete",
    "asname": "SANET",
    "mobile": false,
    "proxy": false,
    "hosting": false
}
```

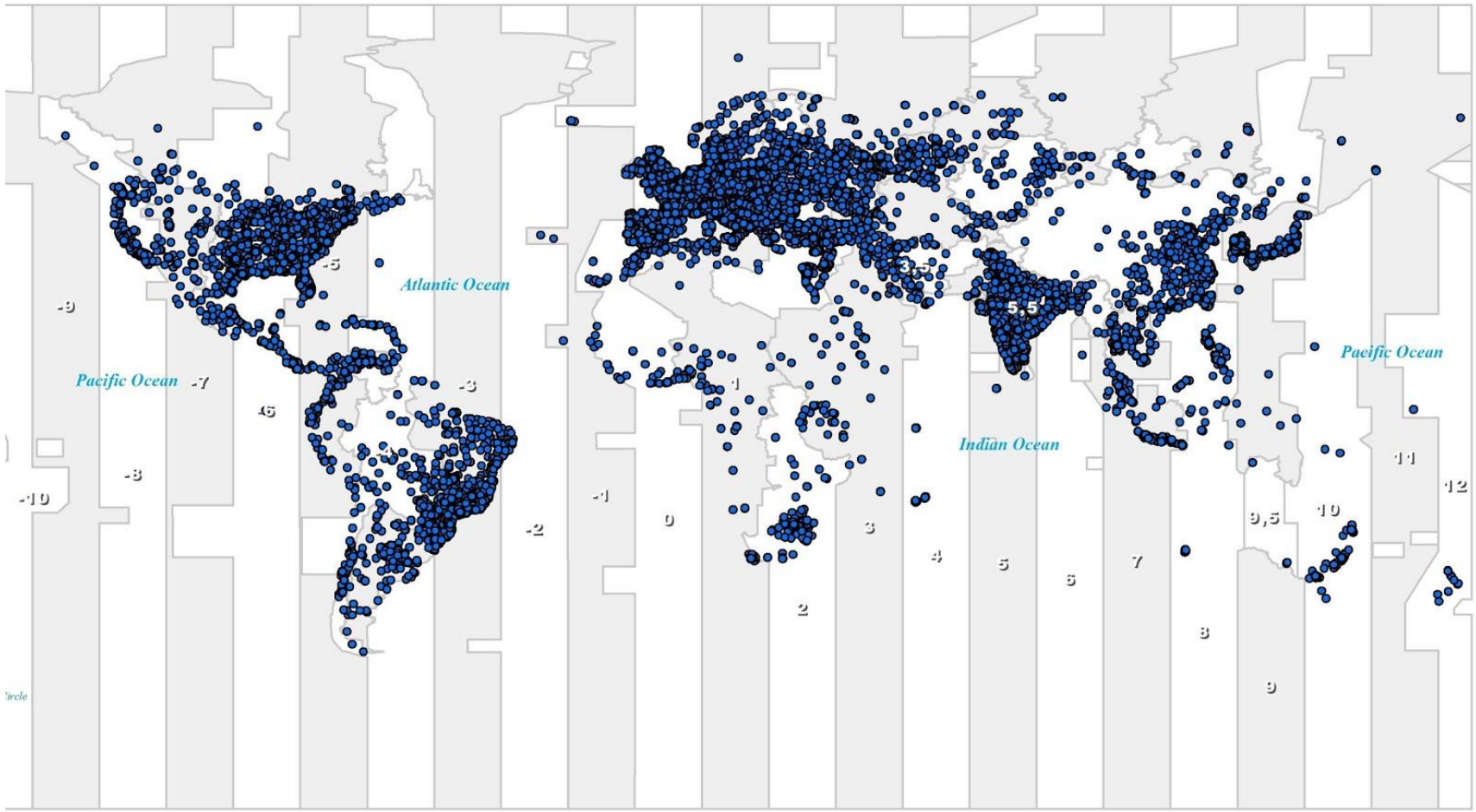
Zdroj: KESTER, Jan-Jelle. Comparing the Accuracy of IPv4 and IPv6 Geolocation Databases. Methodology, 2016, 10.11: 12-17.

Útok v priestore a čase

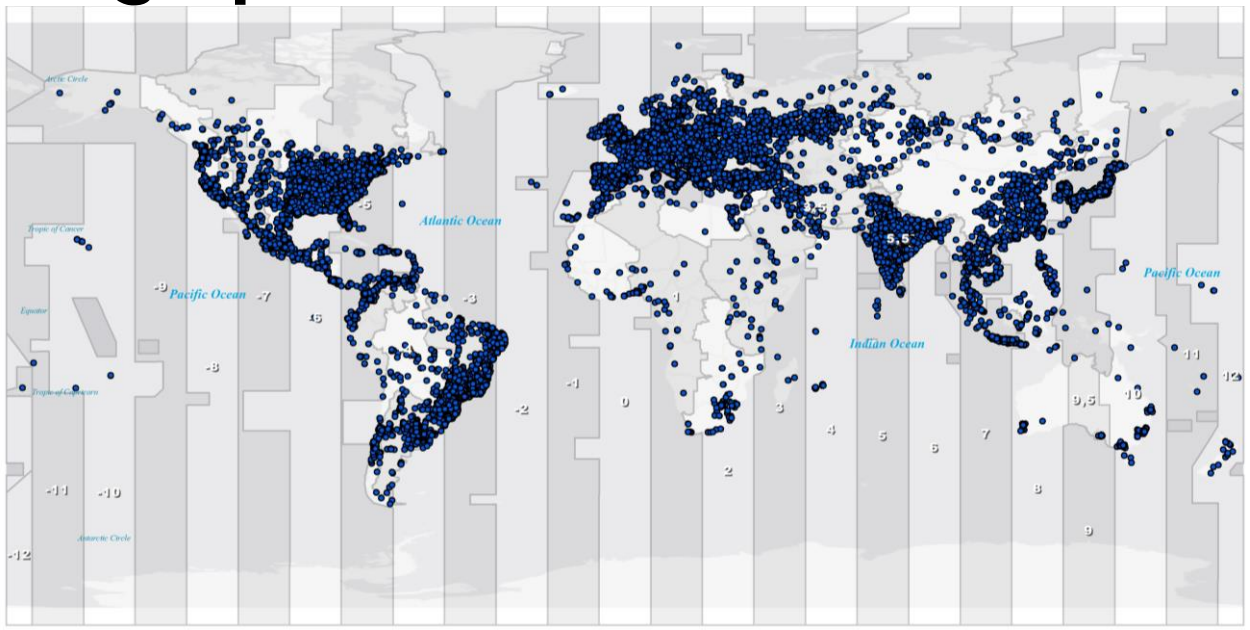


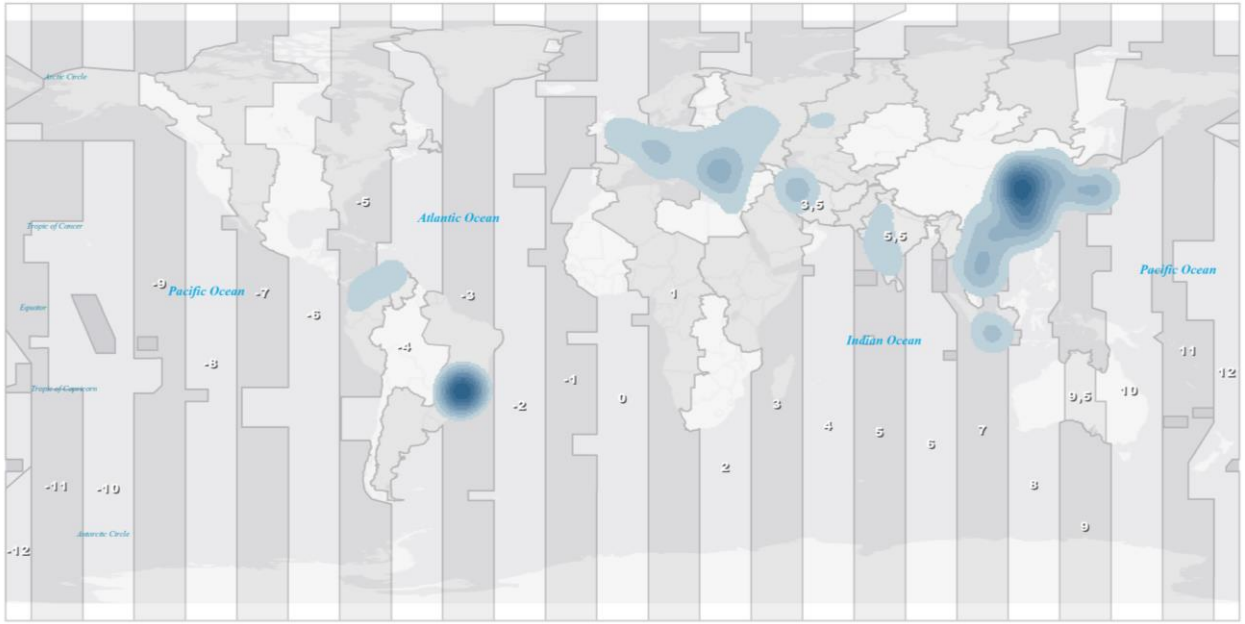
Zdroj: https://threatmap.checkpoint.com/

Priestorový apekt (I.)



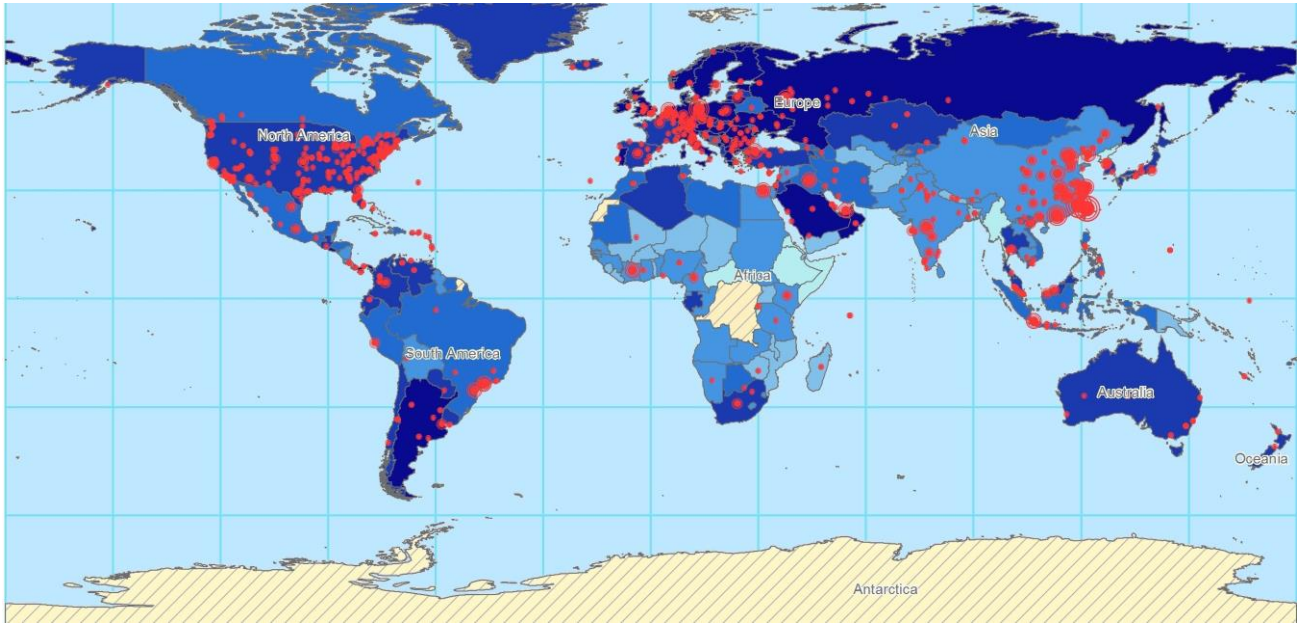
Priestorový apekt (II.)



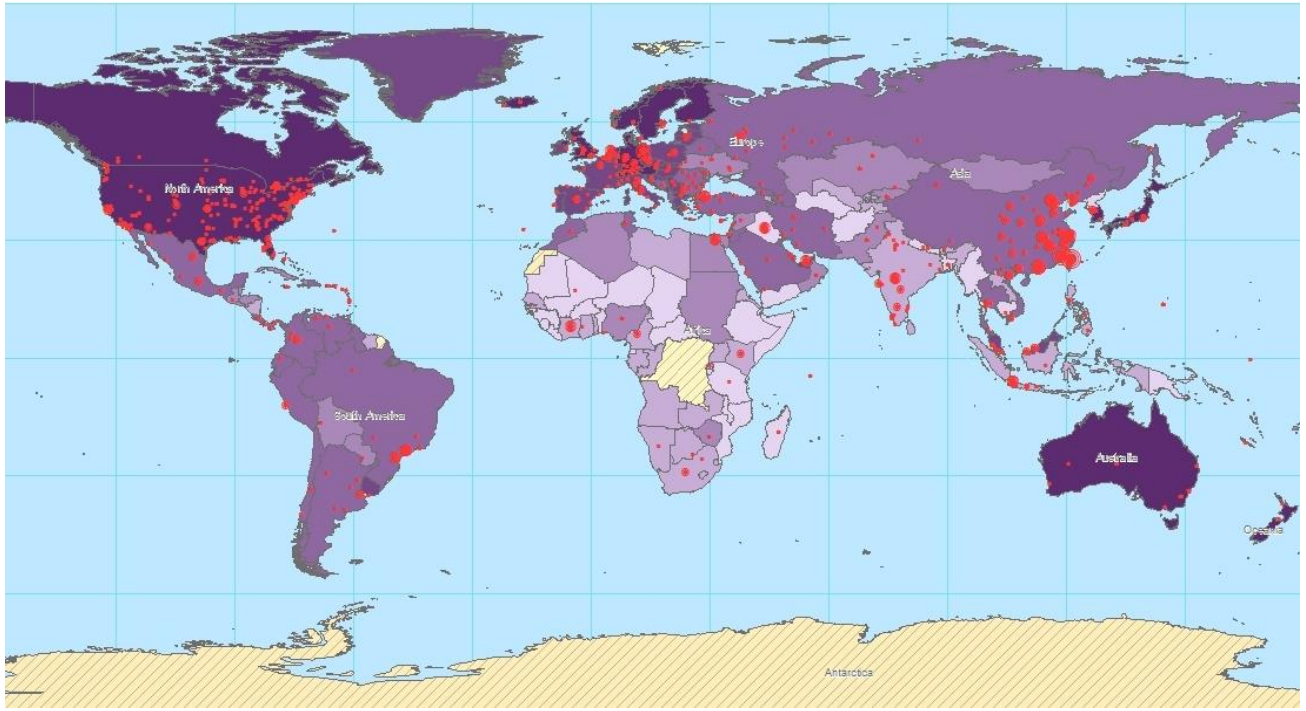


Priestorový apekt (III.)

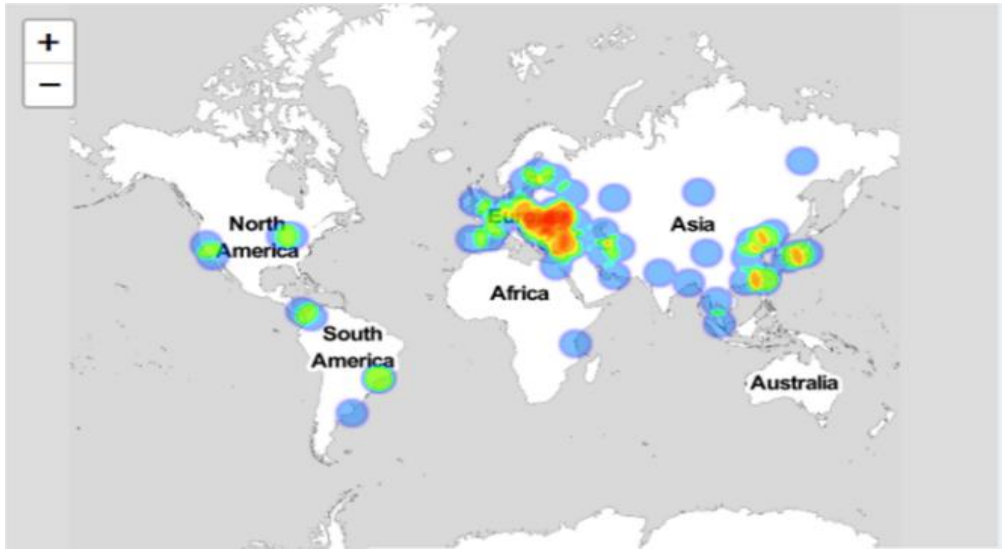
Počet pokusov o útok a počet používateľov mobilných zariadení (2015)



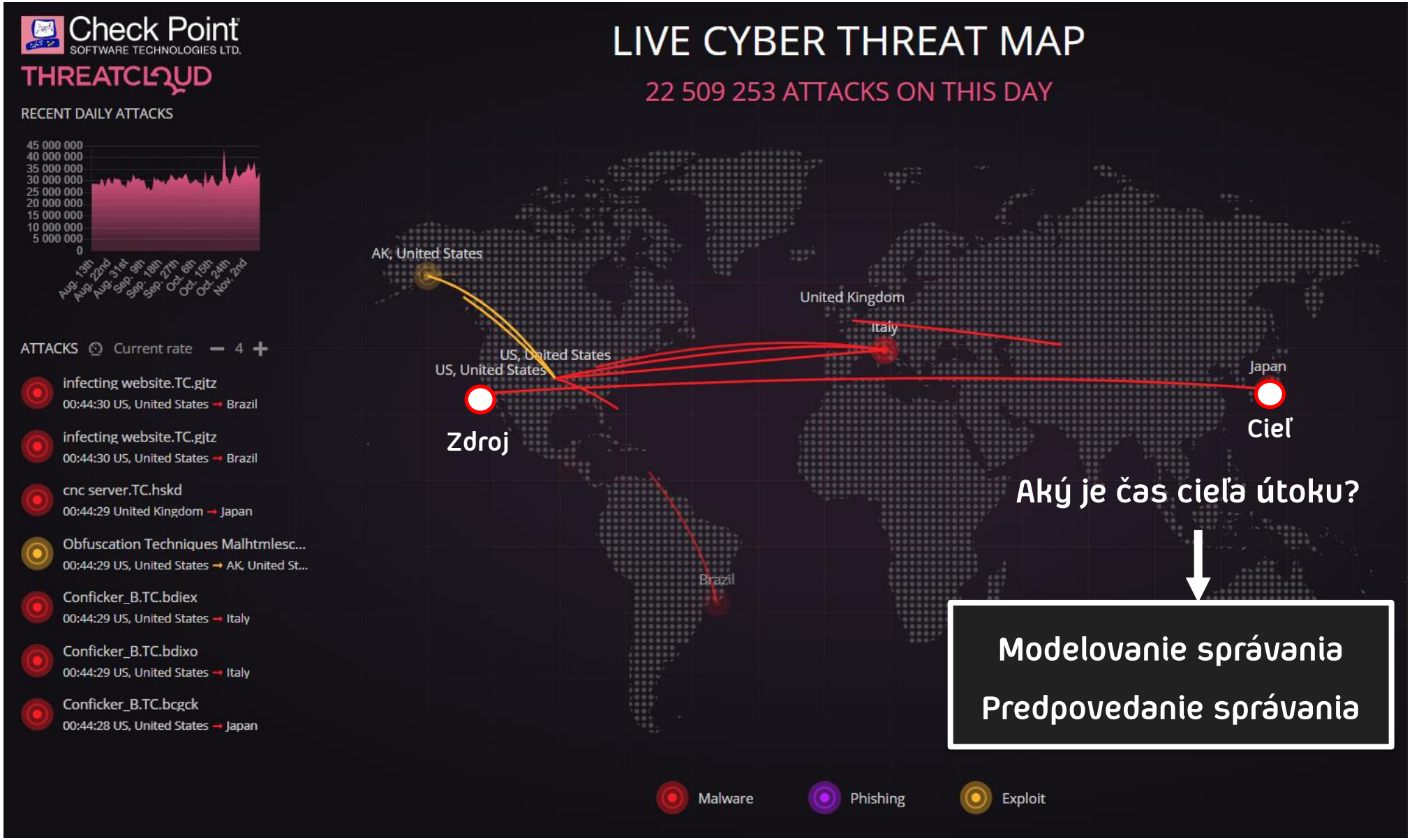
Počet pokusov o útok a počet používateľov internetu (2015)



Priestorový apekt (IV.)



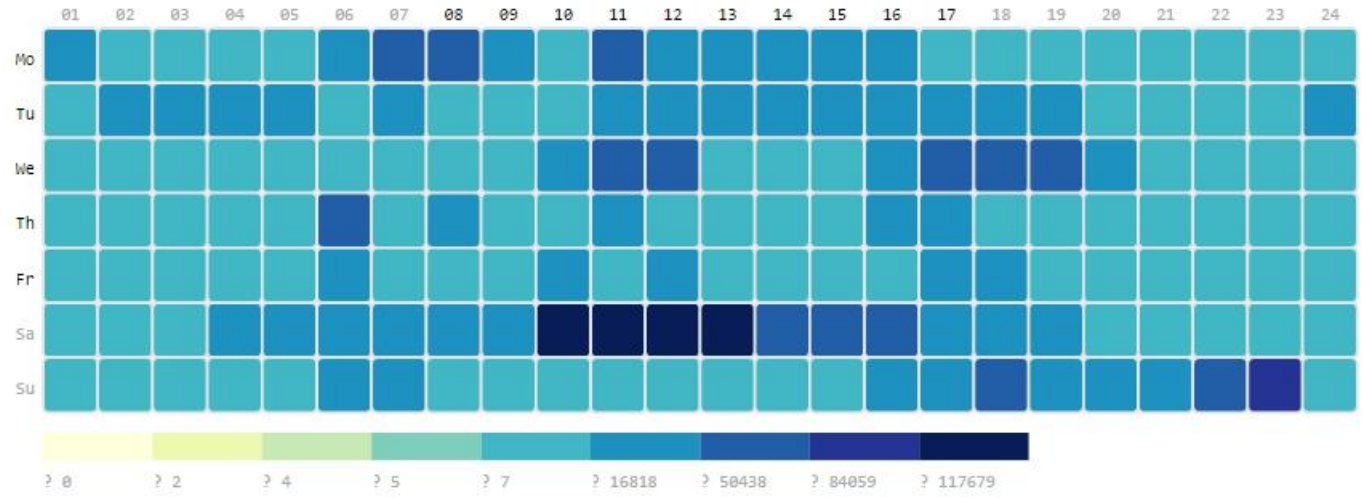
Časový aspekt (I.)



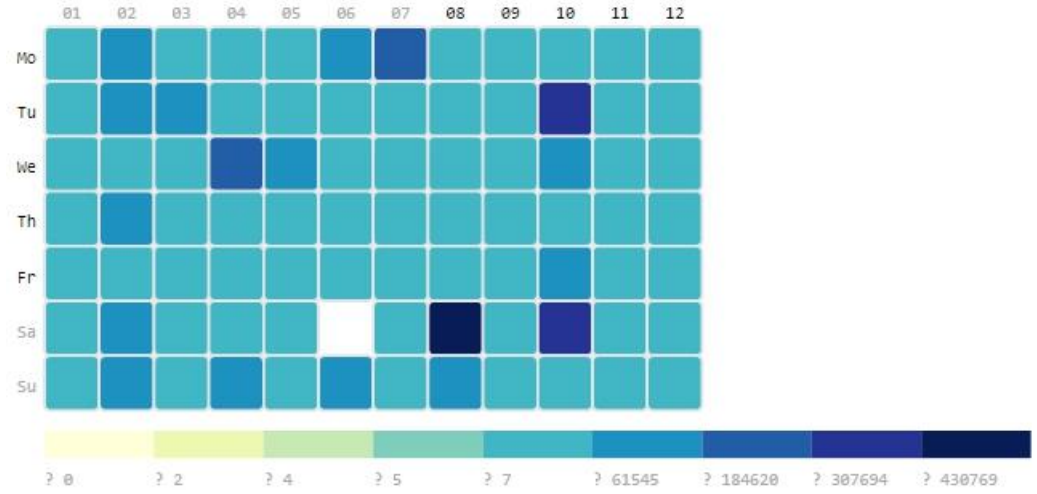
Zdroj: https://threatmap.checkpoint.com/

Časový aspekt (II.)

Deň v týždni a hodina

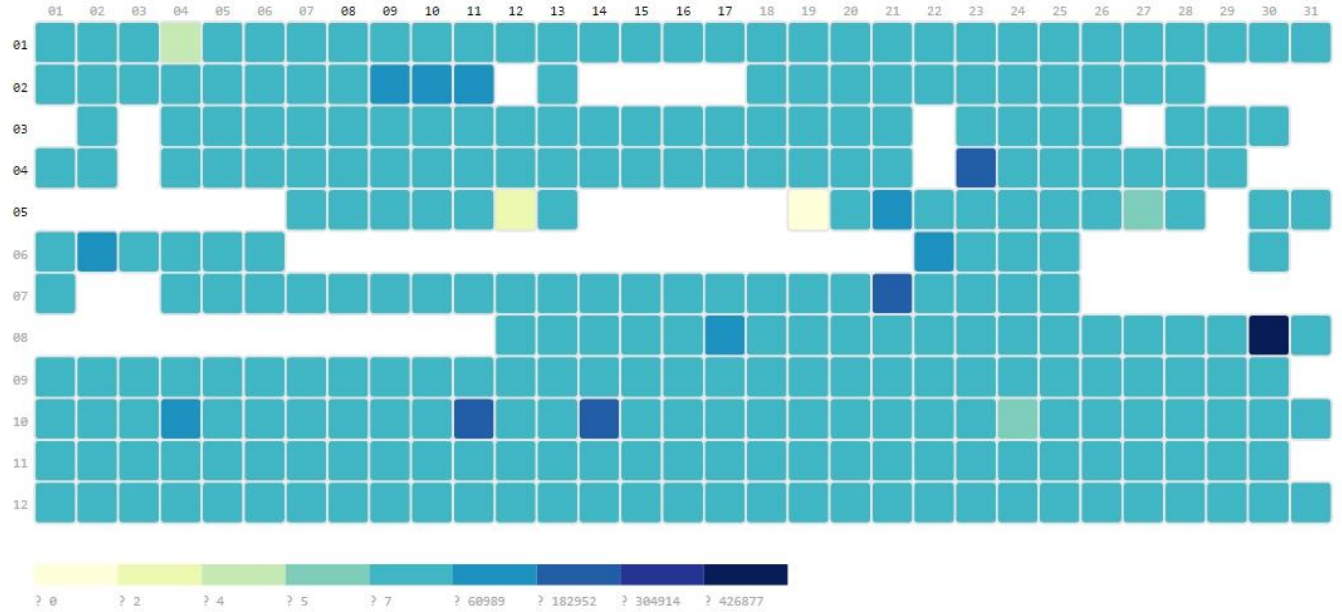


Deň v týždni a mesiac

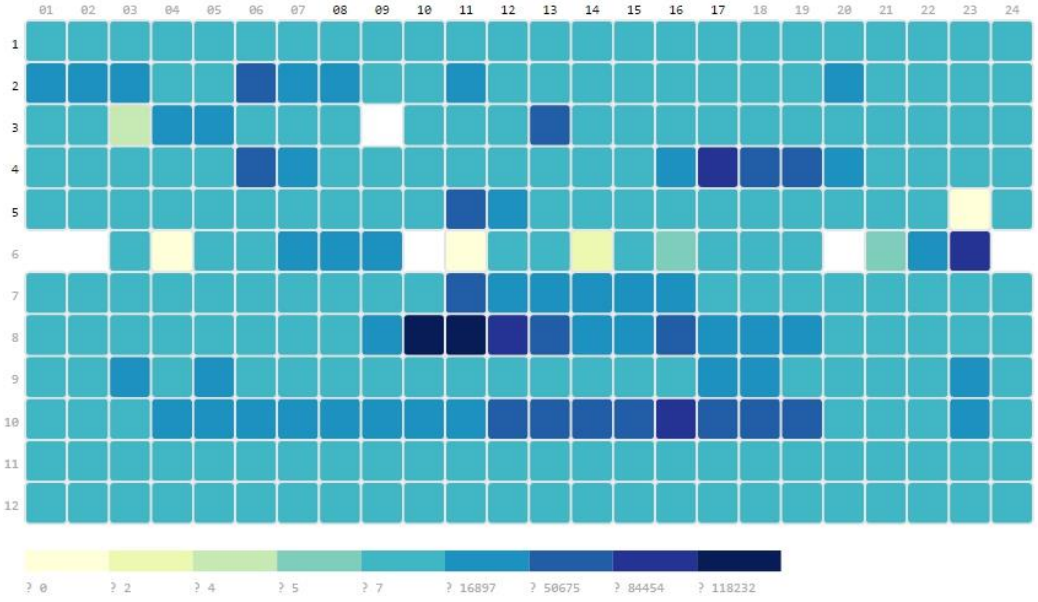


Časový aspekt (III.)

Mesiac a deň

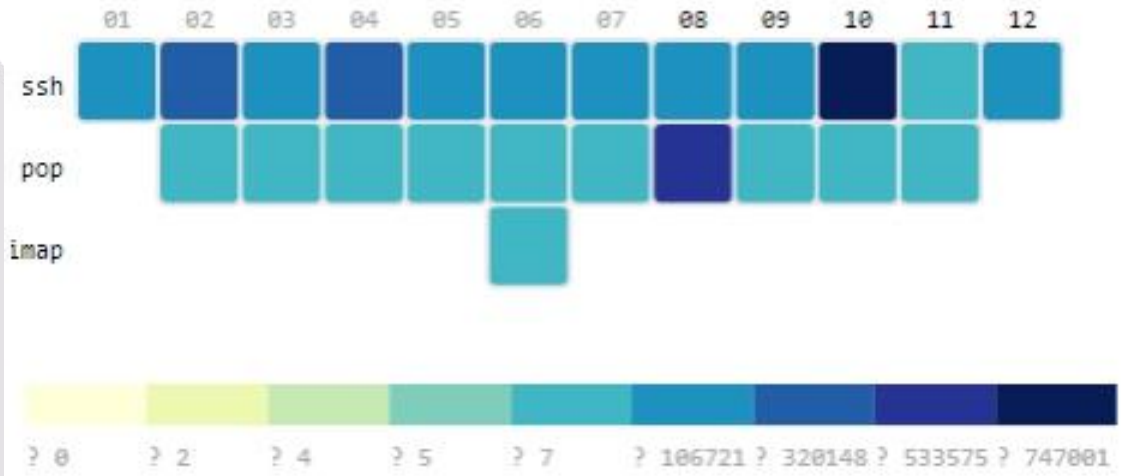


Mesiac a hodina



Časový aspekt - zraniteľnosti

SSH — Október 2014 — CVE-2014-7169
POP3 — August 2014 — CVE-2014-3891



CVE-2014-7169 Detail

Current Description

GNU Bash through 4.3 bash43-025 processes trailing strings after certain malformed function definitions in the values of environment variables, which allows remote attackers to write to files or possibly have unknown other impact via a crafted environment, as demonstrated by vectors involving the ForceCommand feature in OpenSSH sshd, the mod_cgi and mod_cgid modules in the Apache HTTP Server, scripts executed by unspecified DHCP clients, and other situations in which setting the environment occurs across a privilege boundary from Bash execution. NOTE: this vulnerability exists because of an incomplete fix for CVE-2014-6271.

+View Analysis Description

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 2.0 Severity and Metrics:

NIST: NVD **Base Score:** 10.0 HIGH **Vector:** (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVE-2014-3891 Detail

Current Description

Buffer overflow in RimArts Becky! Internet Mail before 2.68 allows remote POP3 servers to execute arbitrary code via a crafted response.

+View Analysis Description

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 2.0 Severity and Metrics:

NIST: NVD **Base Score:** 6.8 MEDIUM **Vector:** (AV:N/AC:M/Au:N/C:P/I:P/A:P)

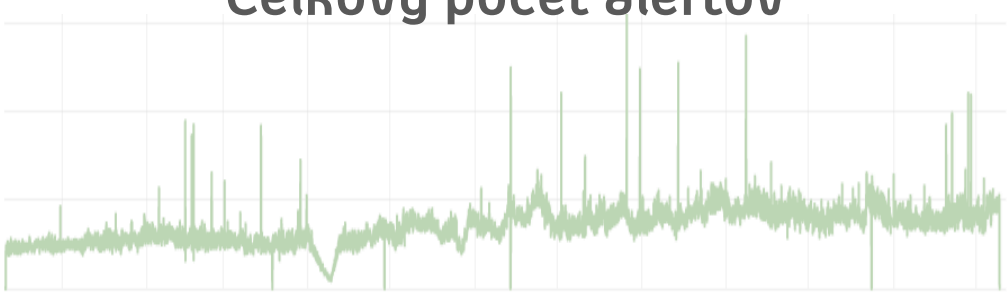
NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

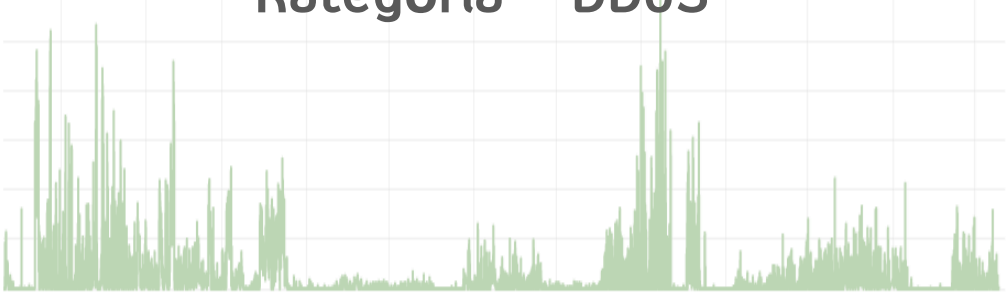
Časový aspekt – časové rady (I.)

Časový aspekt – časové rady (II.)

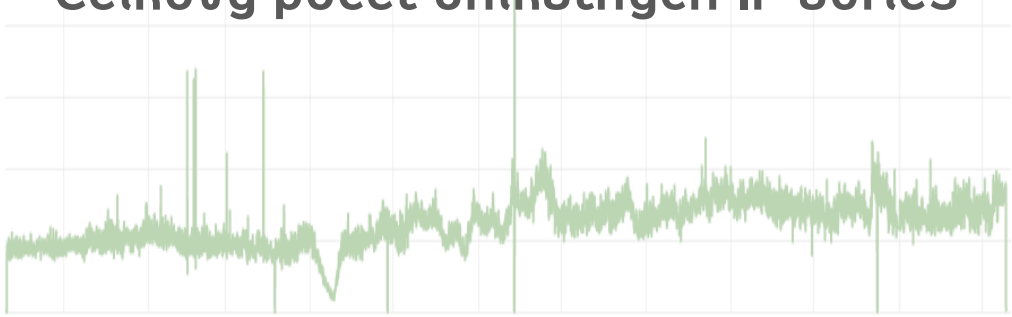
Celkový počet alertov



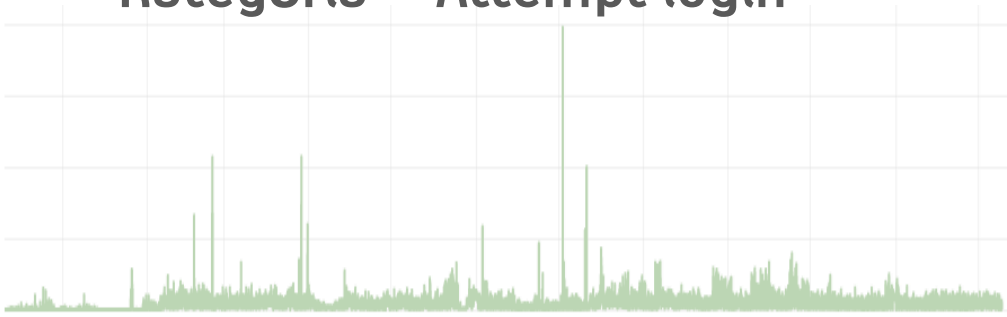
Kategória – DDoS



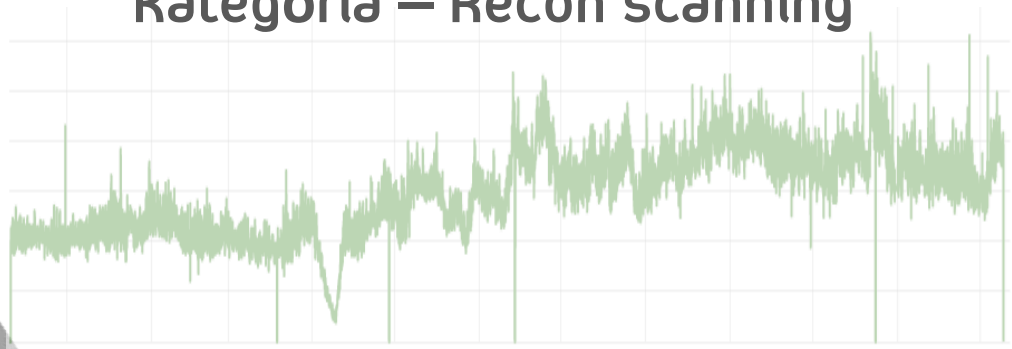
Celkový počet unikátnych IP adries



Kategória – Attempt login

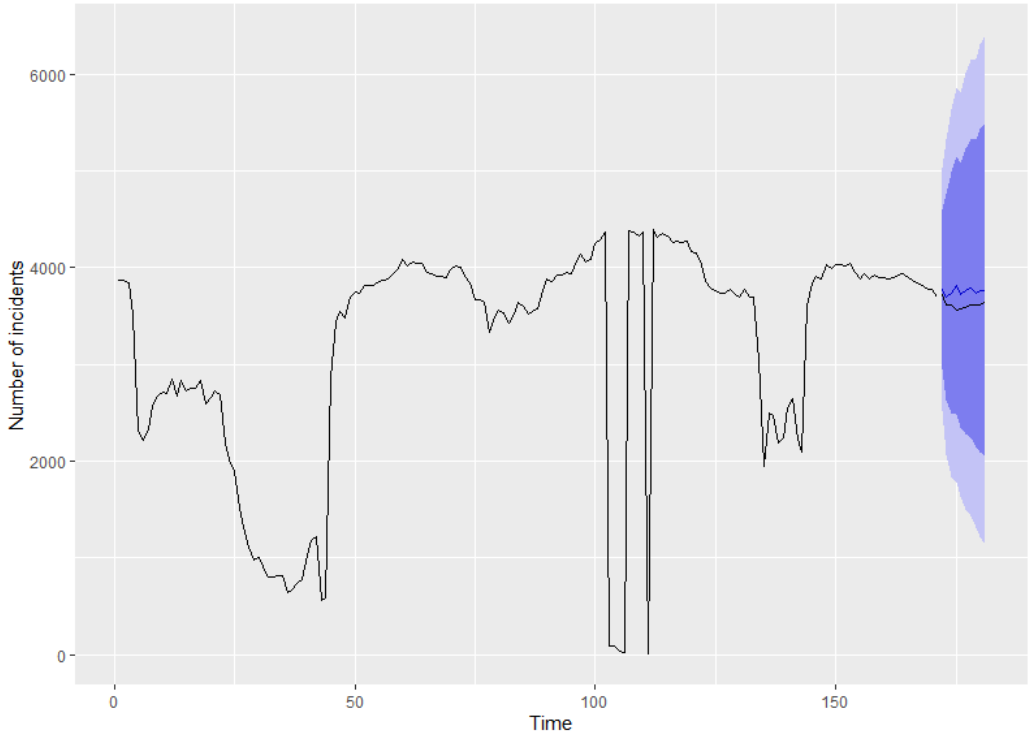


Kategória – Recon scanning



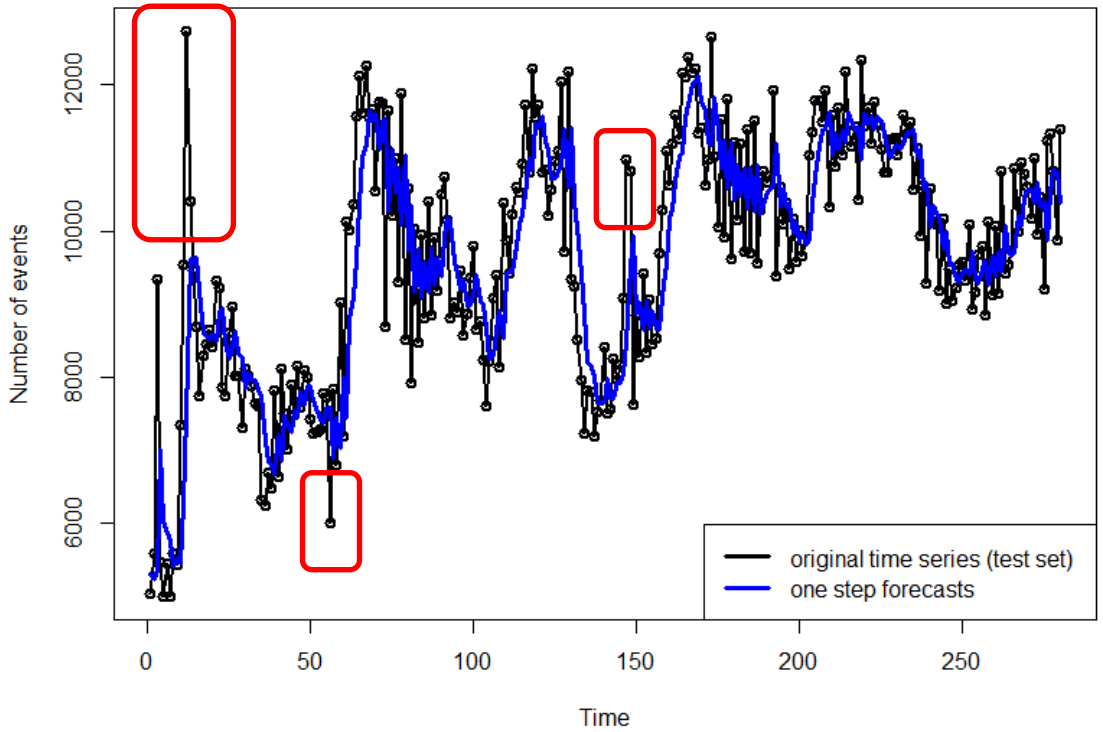
Časový aspekt – časové rady (III.)

Intervalová predikcia (10 krokov, 30 minút)

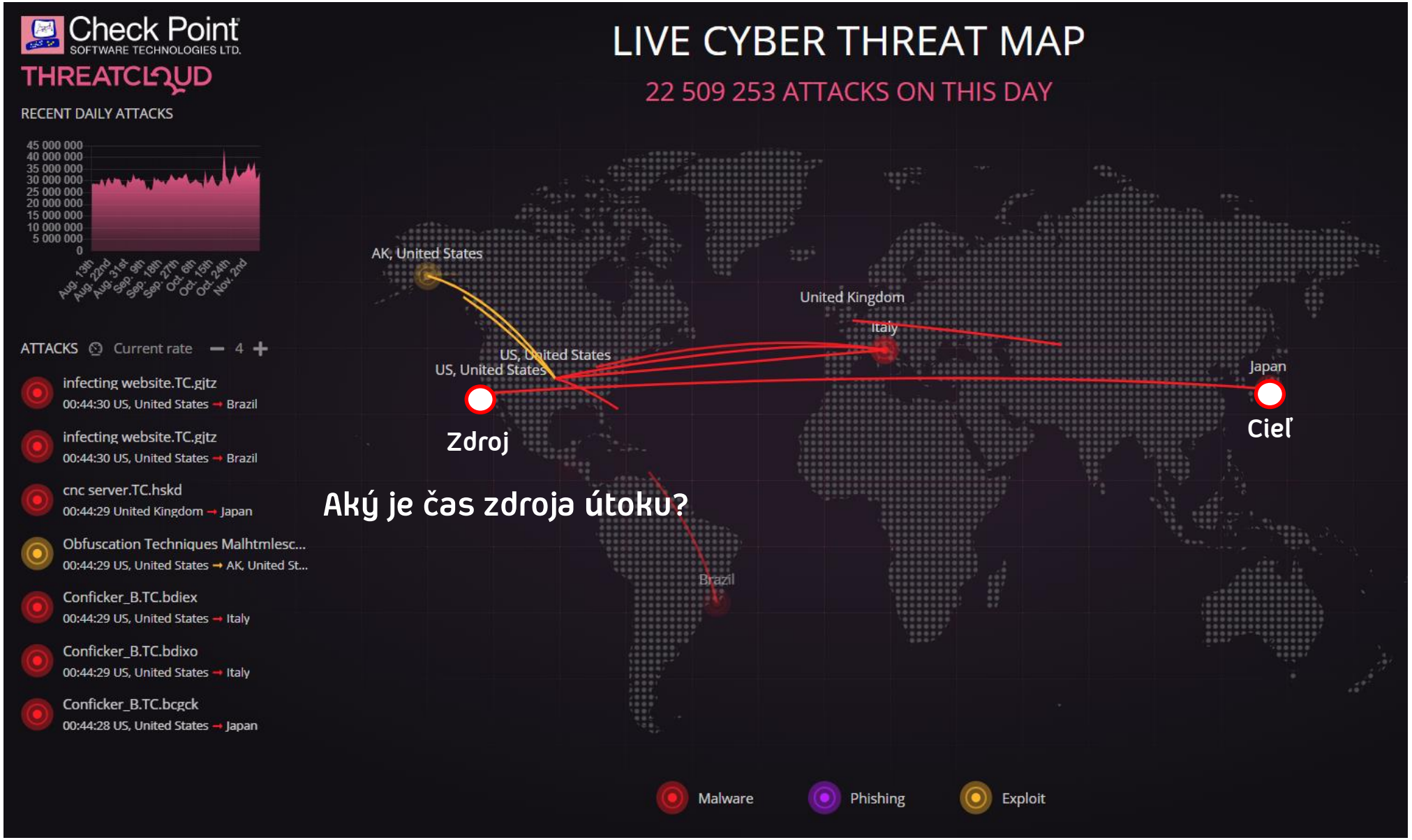


Bodová predikcia (1 krok, 30 minút)

Anomália?

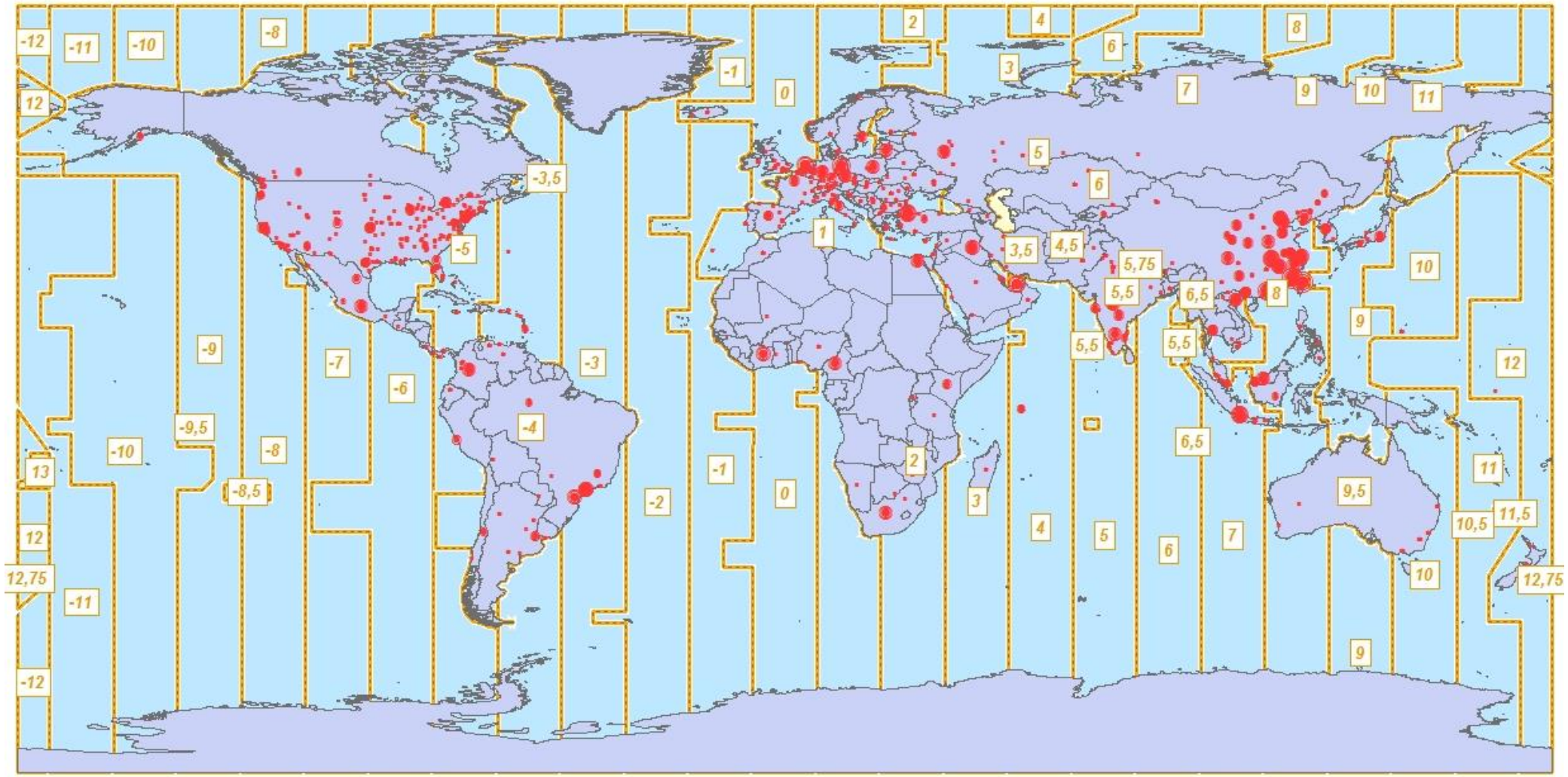


Časopriestorový apekt – časové zóny (I.)

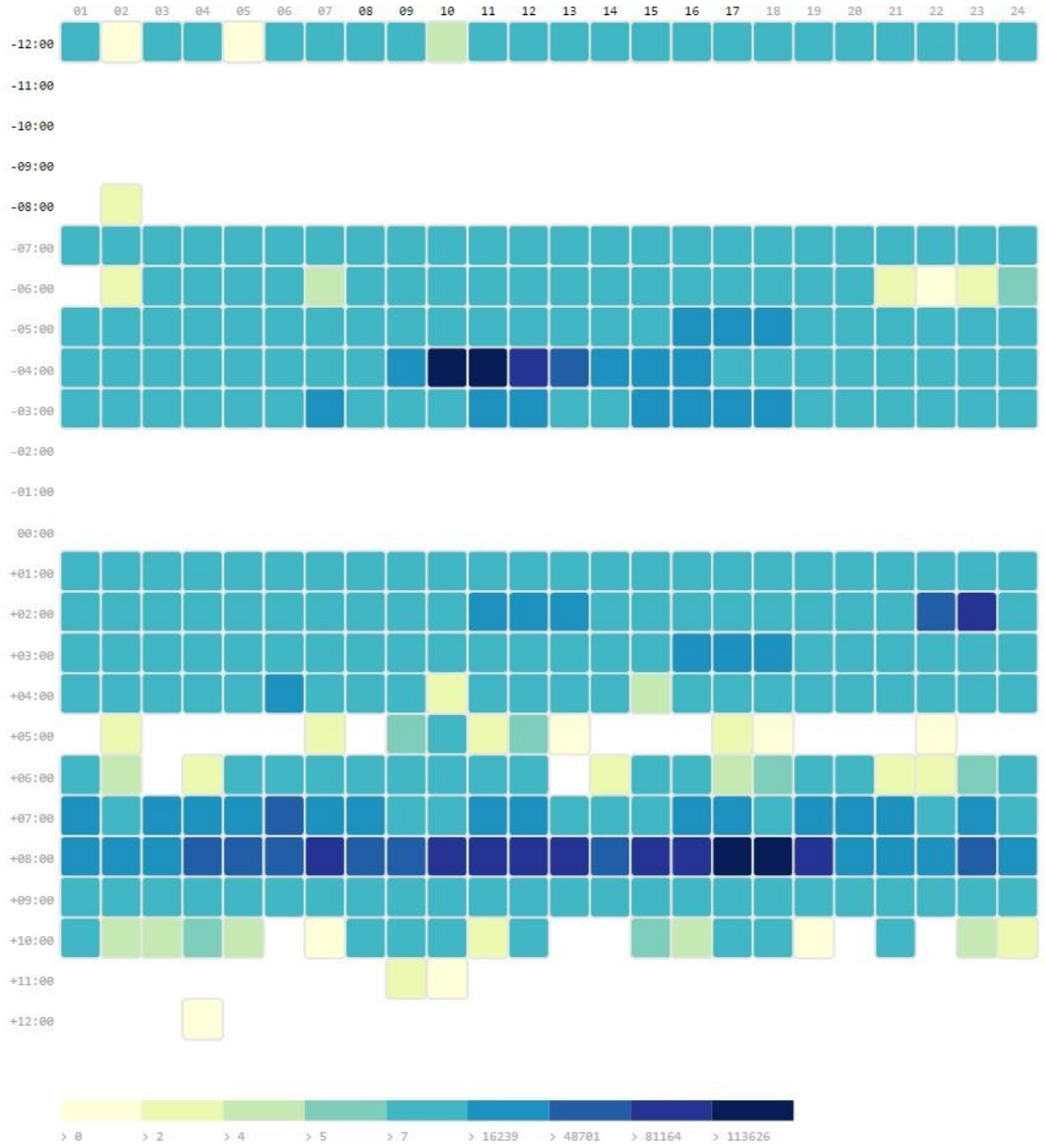


Zdroj: https://threatmap.checkpoint.com/

Časopriestorový apekt – časové zóny (II.)



Časopriestorový apekt – časové zóny (III.)



Ďakujem za pozornosť


Jesenná 5, Košice


ics.science.upjs.sk


csl.science.upjs.sk


ui@upjs.sk