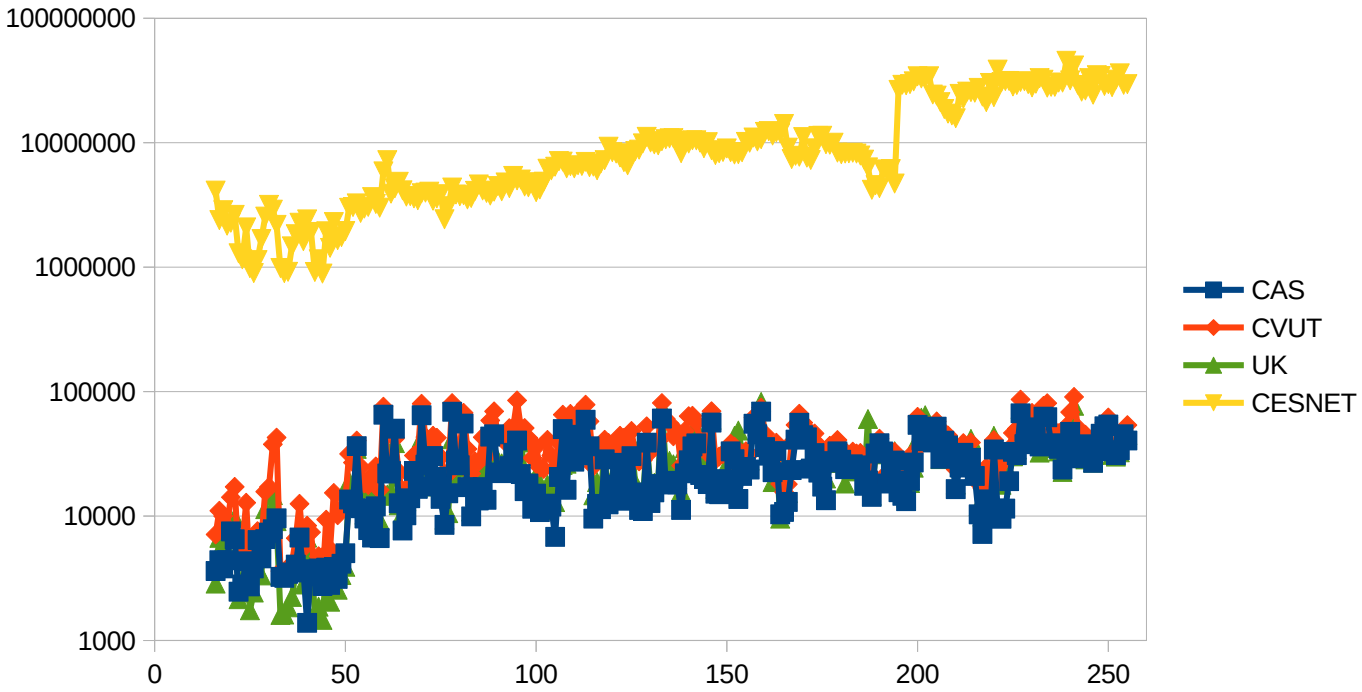
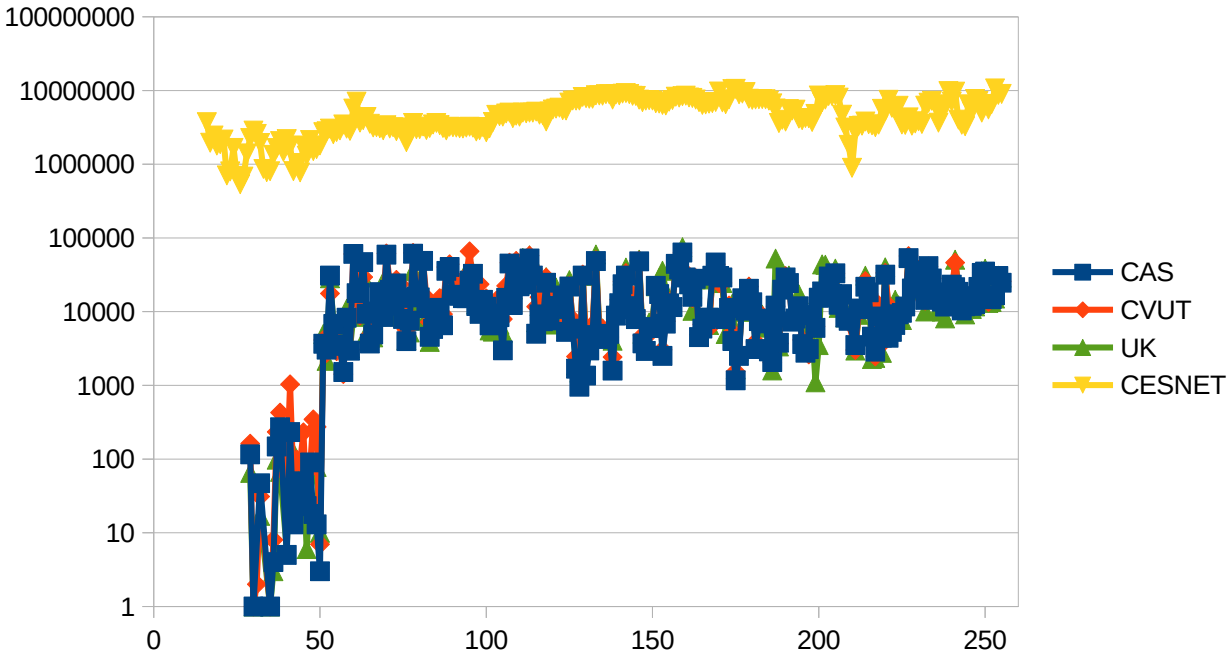
Bezpečnostní události v síti AVČR v roce 2025

Zdrojem informací je Warden – systém pro sdílení anomálií mezi bezpečnostními týmy. Jednotlivé události jsou zaznamenané ve formátu IDEA0 - Intrusion Detection Extensible Alert – https://idea.cesnet.cz/en/index. Data analyzujeme pomocí programu BaseX – což je „Open Source, lightweight, high-performance“ programové prostředí vytvořené na Universitě Konstanz (Kostnice), umožňující dotazy jazykem Xquery.
Archivujeme veškeré události od března 2021 a dále z nich vybíráme události s IP4 adresami v prostoru AVČR (CAS), Českého vysokého učení technického a Univerzity Karlovy.



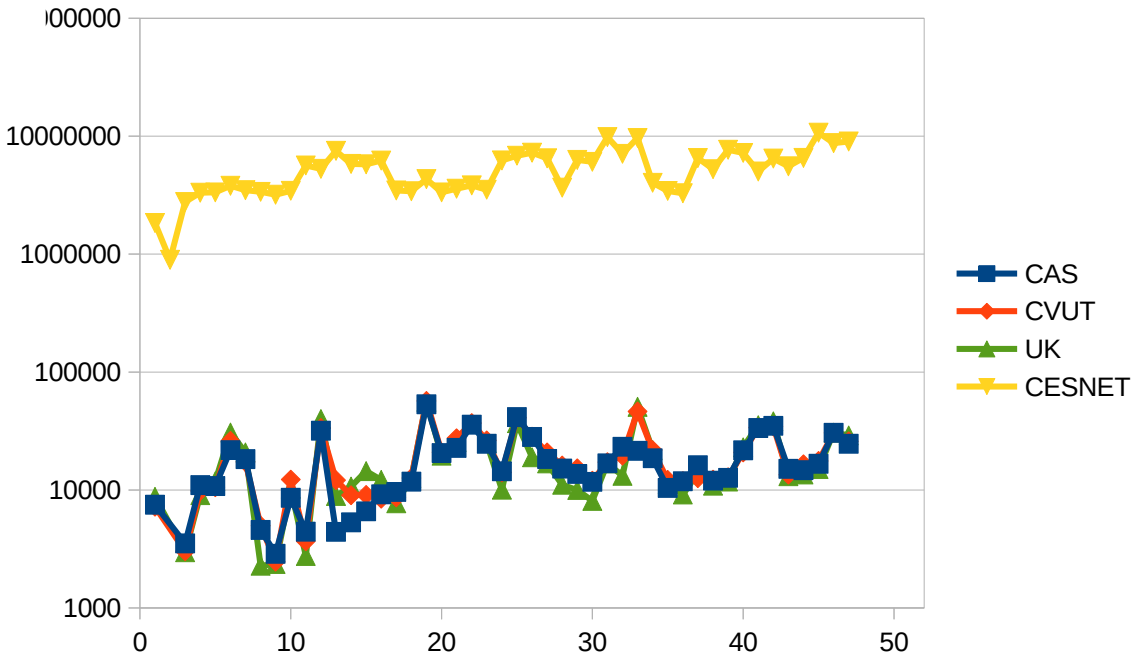
Týdenní souhrny počtu událostí (všech kromě testovacích) zaznamenaných v systému Warden od roku 2021 do současnosti. Je patrný řádový nárůst počtu na přelomu roku 2021 a 2022 (týden 53 od začátku 2021).



Týdenní souhrny počtu událostí Recon.Scanning zaznamenaných v systému Warden od roku 2021 do současnosti. Nárůst počtu na přelomu roku 2021 a 2022 (týden 53 od začátku 2021).

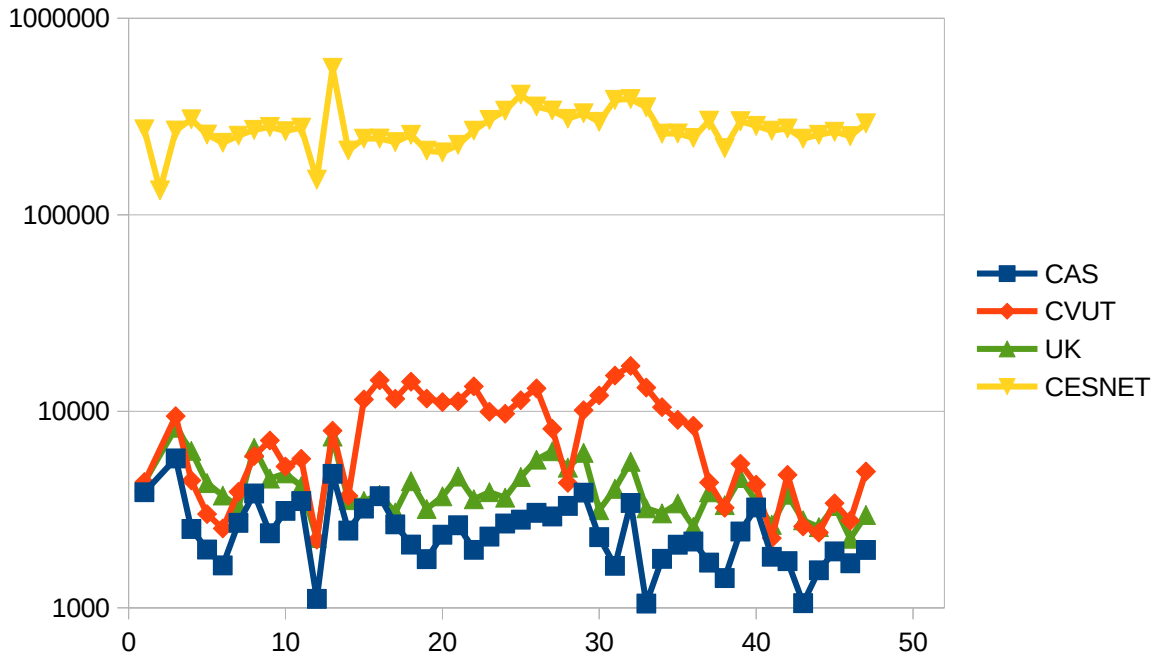
Řady týdenních souhrnů 2025 pro jednotlivé kategorie

Scanning, 2025



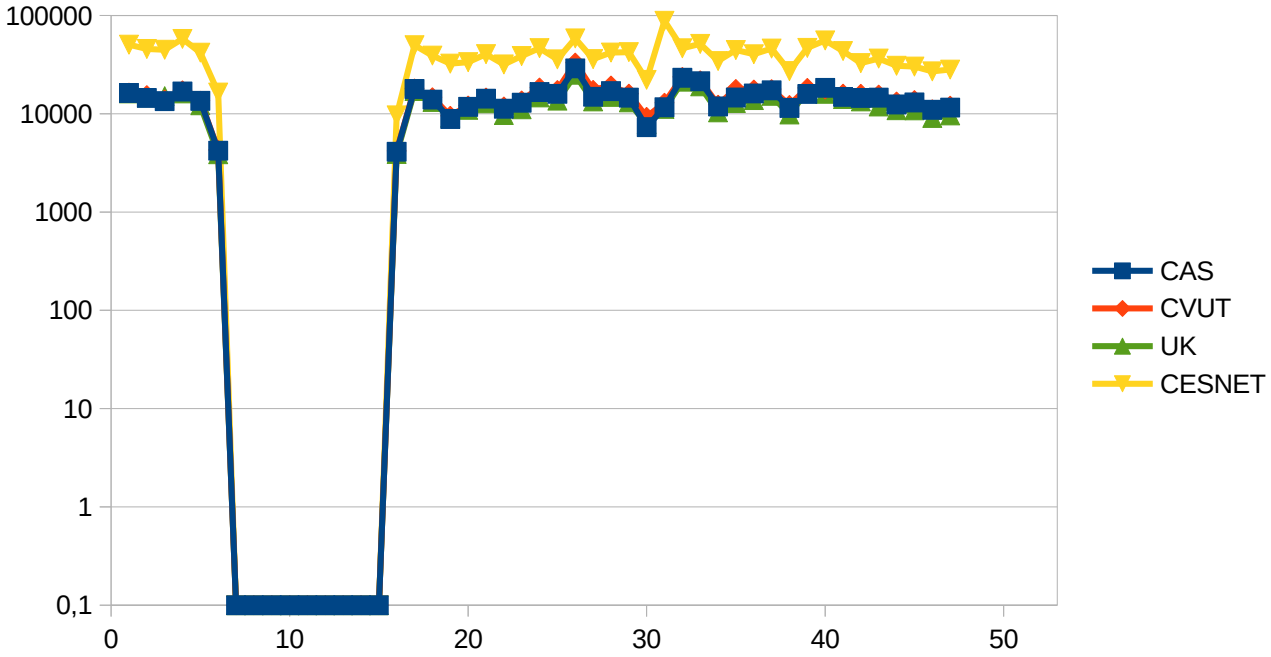
Pozorujeme těsnou korelaci mezi útoky zahrnujícími adresy AV, ČVUT a UK.

Attempt Login 2025



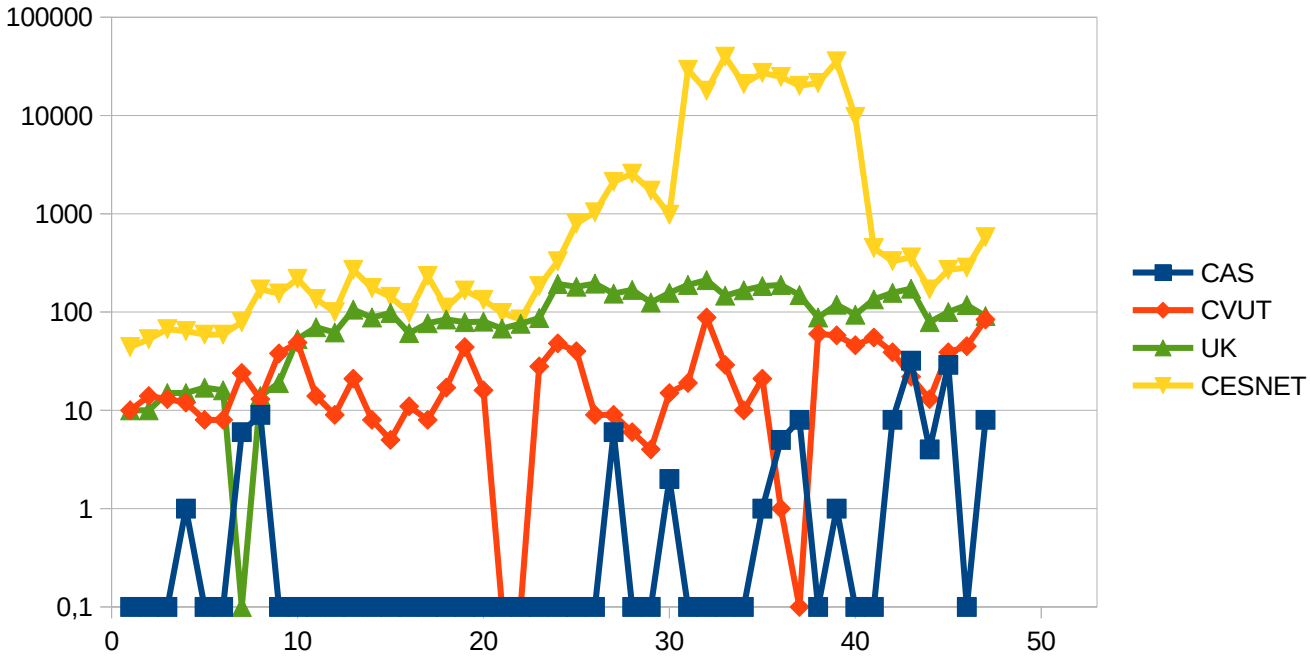
Pokusy o přihlášení jsou v akademických sítích stabilně zastoupené. Přechodně přibylo útoků na ČVUT.

Anomaly Traffic, 2025



Anomální provoz vykazuje občas výkyvy, které jsou zřejmě závislé na nasazení příslušných detektorů.

Botnet 2025



Výskyt botnetů se v posledním pololetí zvýšil.