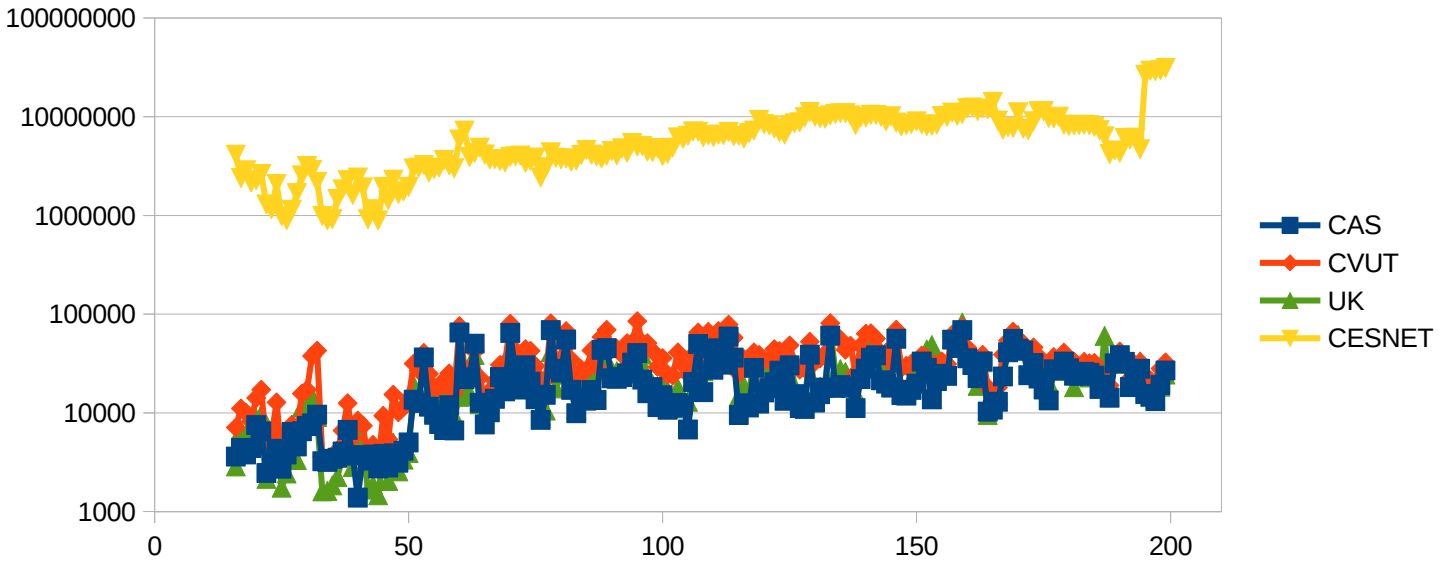
Bezpečnostní události v síti AVČR v letech 2021-2024

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.

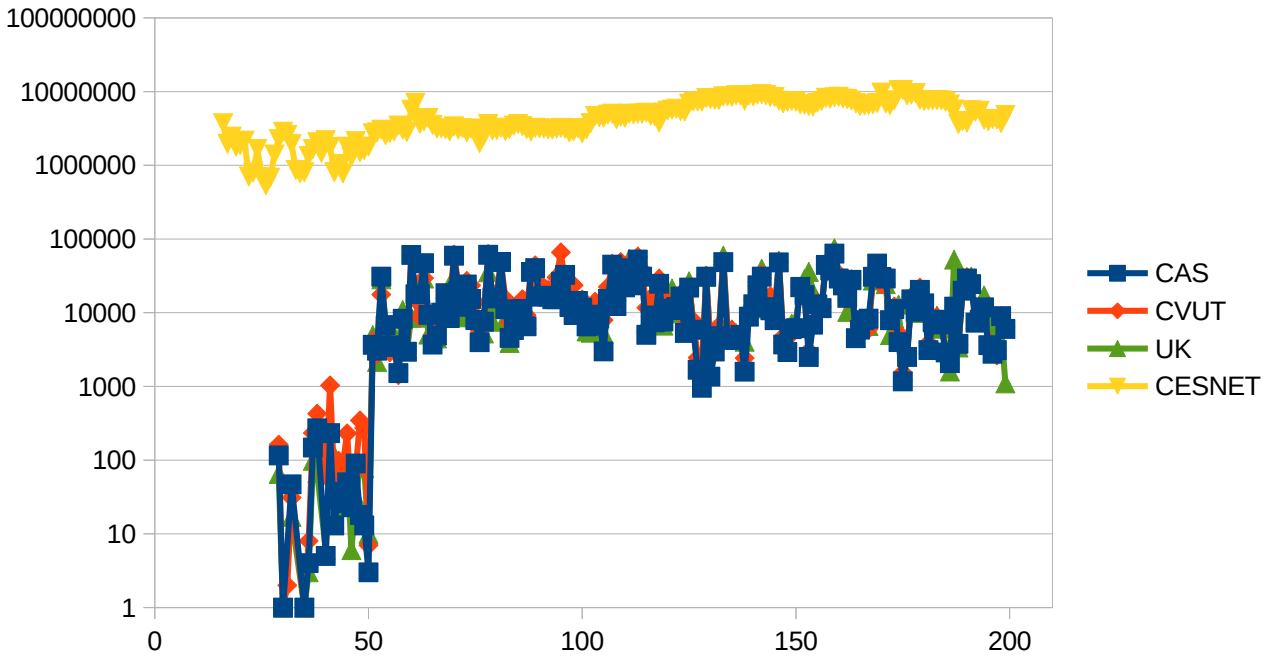


Týdenní souhrny počtu událostí (všech kromě testovacích) zaznamenaných v systému Warden od roku 2021 do současnosti. Je patrný řádový nárůst počtu na přelomu roku 2021 a 2022 (týden 53 od začátku 2021).

Události jsou ve formátu IDEA kategorizovány podle typu, souhrn kategorií (ne testovacích) za posledních 5 týdnů je v následující tabulce. Převládající kategorie UserCompromise se v tomto množství objevila teprve nedávno a nemusí se ani týkat adres v síti CESNET.

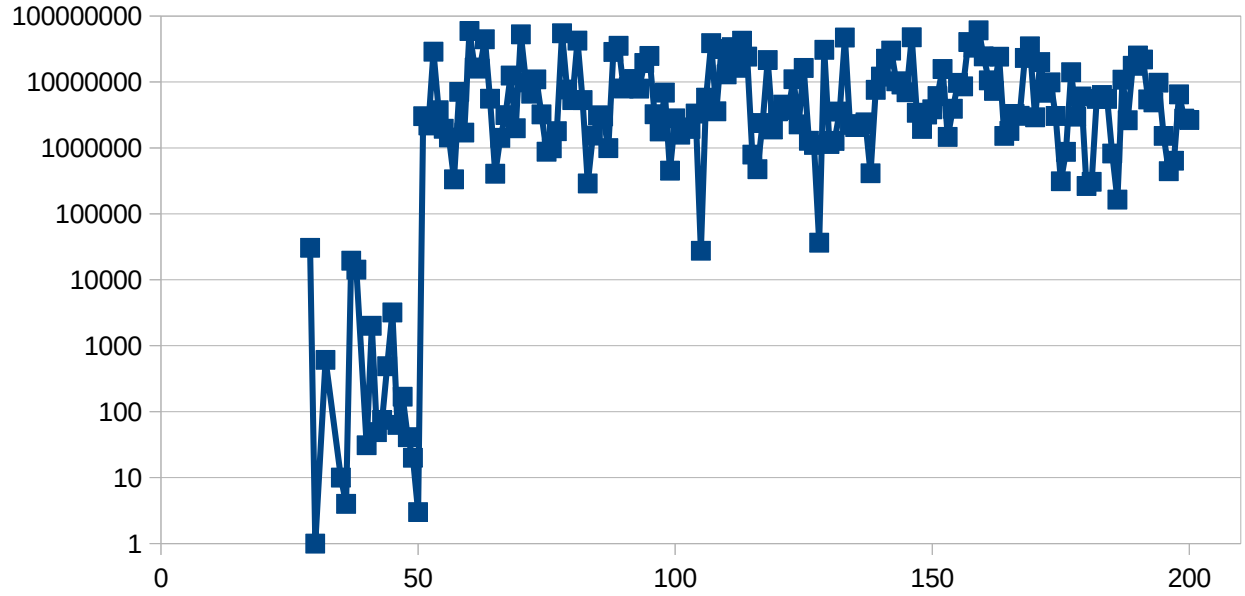
Intrusion.UserCompromise	120205367
Recon.Scanning	21380024
Attempt.Login	2138715
Availability.DoS	519298
Malware	509928
Anomaly.Traffic	194492
Vulnerable.Config	182727

Kategorie Recon.Scanning



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).

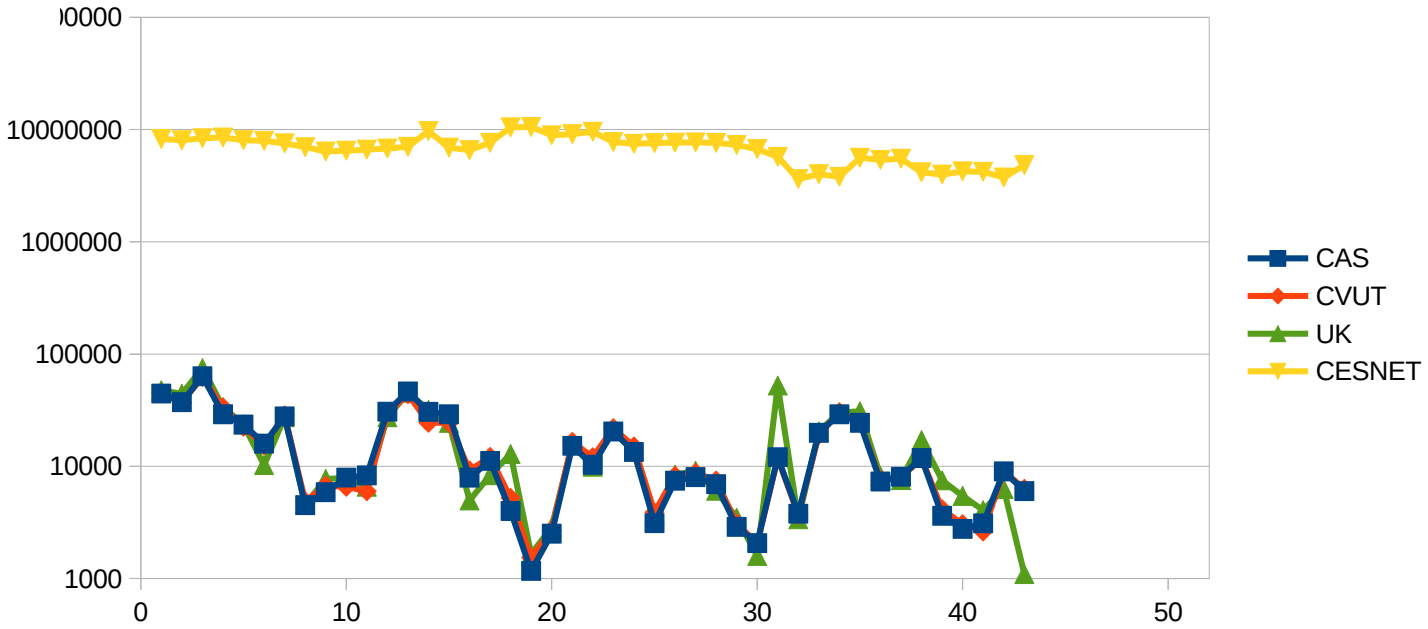
Scanning, Target v CAS, počet IP, 2021-4



Týdenní souhrny počtu napadených IP adres v událostech týkajících se adresového prostoru AVČR. Na přelomu roku 2021 a 2022 (týden 53) začaly chodit hromadné útoky na cca 1000 adres současně. Zdrojové IP adresy těchto útoků odkazovaly k poskytovatelům služeb zpočátku převážně z Ruska ale i např. Holandska, v současnosti vede Bulharsko. Intenzita a charakter útoků se od roku 2022 nemění.

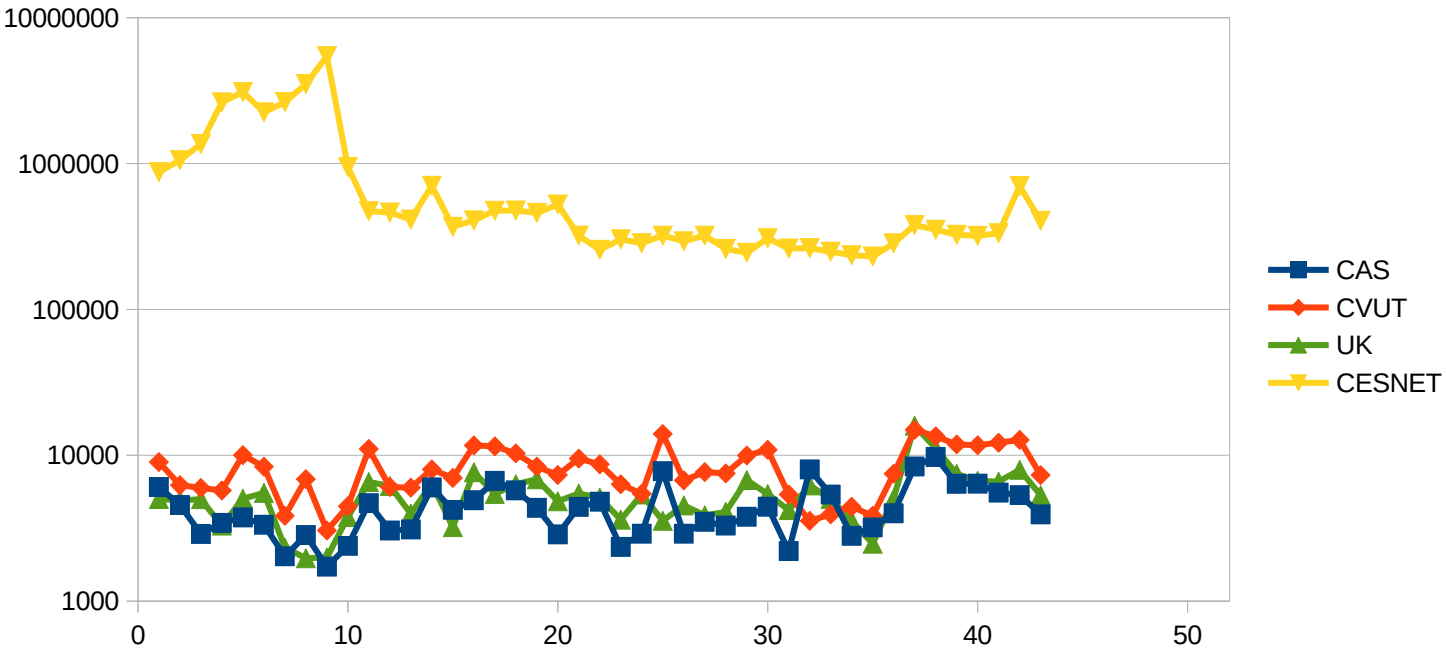
Řady týdenních souhrnů 2024 pro jednotlivé kategorie

Scanning, 2024



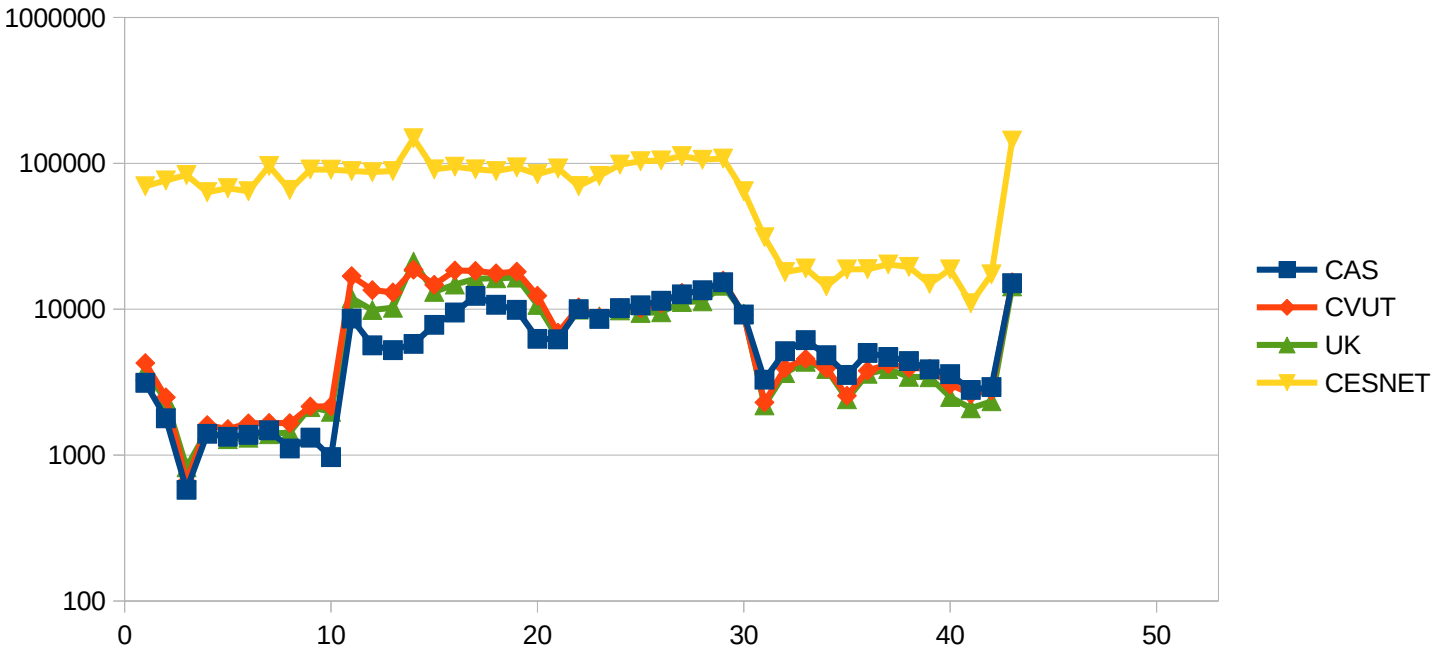
Pozorujeme těsnou korelaci mezi útoky zahrnujícími adresy AV, ČVUT a UK.

Attempt Login 2024



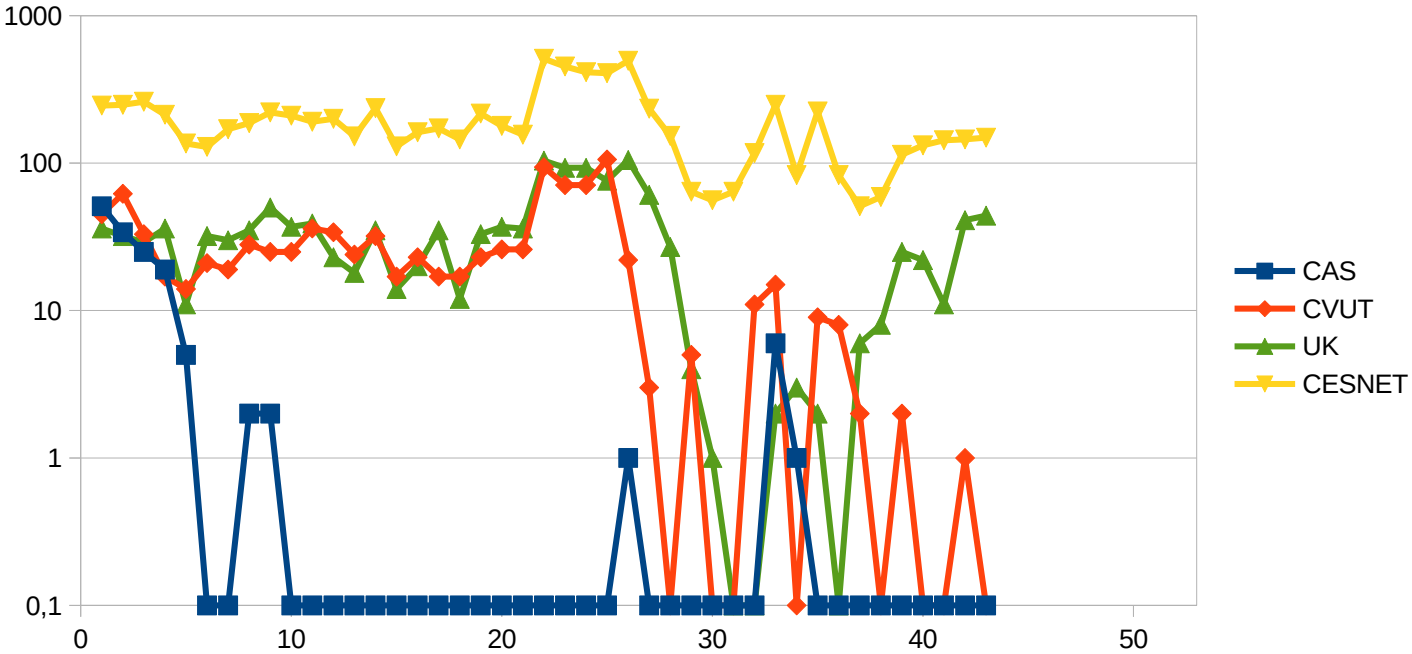
Pokusy o přihlášení jsou v akademických sítích stabilně zastoupené. Nejvýraznější jev byl nárůst v celé síti začátkem roku.

Anomaly Traffic, 2024



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

Botnet 2024



V počtu zachycených botnetů se situace v akademické síti letos výrazně zlepšila.