µcollect

Monitoring sítě a detekce anomálií

Michal Vaner • michal.vaner@nic.cz • 30.11.2013

CZ.NIC | SPRÁVCE DOMÉNY CZ

Představení a motivace

- Sbírá a analyzuje síťový provoz
- Poběží na routeru Turris

- Existují řešení pro velké servery
- Mnohé sledují jen průtoky
- Jiné příliš zvědavé

Pluginový systém

- Jen .so knihovna s daným rozhraním
- Možnost načtení a vyhození za běhu
- Detekce chyb
  - Např. segmentation fault
  - Vyhození a nové načtení pluginu

Komunikace se serverem

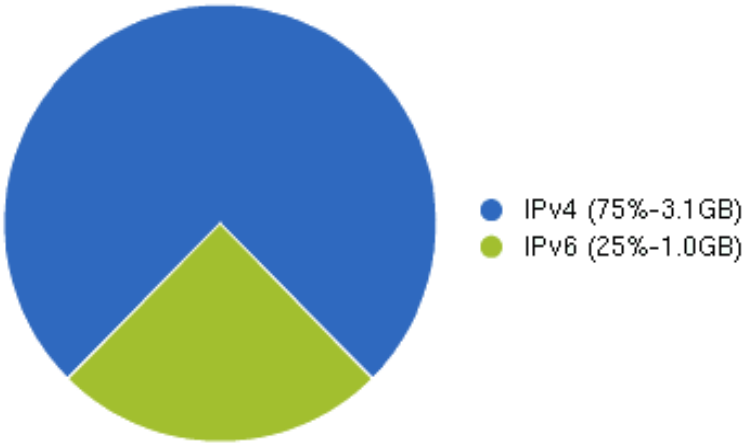
- Trvalé TCP spojení, obnovení když spadne
- Binární protokol
- Zabezpečení pomocí TLS
  - Certificate pinning
  - Challenge-response login
- Server žádá o data
- Naměřený provoz <50MiB/týden

Sběr dat

- PCAP na vnějším rozhraní
  - Nemění komunikaci
  - Nekouká na vnitřní síť
  - Nezpomaluje tok – při nestíhání vynechává
- Předkládá pakety pluginům
  - Žádný nekouká do aplikačních dat
  - Žádný nezkoumá „lokální“ konec

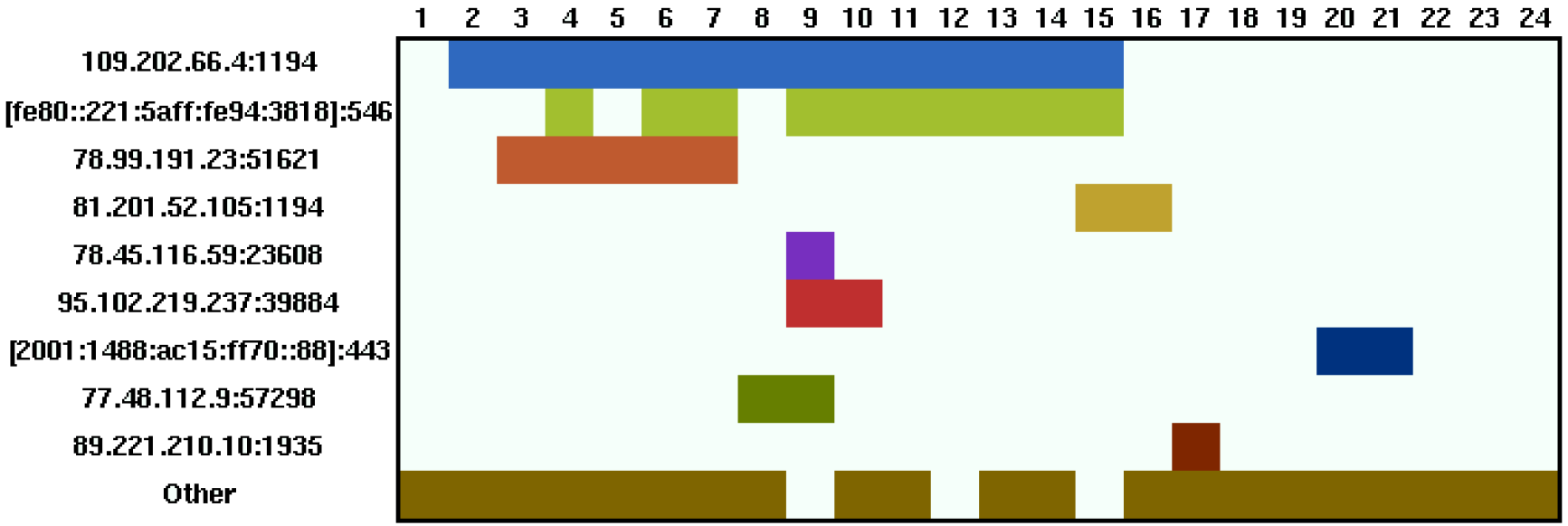
Plugin „Count“ (počet)

- Počítá pakety a jejich velikost
- Několik kategorií
  - Např. TCP/UDP
  - Nebo množství dat se serverem (50MB/Týden)
- Server sbírá a ukládá
  - Časem promaže
  - Nechá jen agregovaná data



Plugin „Buckets“ (kyblíčky)

- Hledá anomálie v provozu
- Těžké definovat, co je vlastně anomálie
- Jeden uživatel je vždy anomální



Plugin „Buckets“ – fungování

- Hashování několika funkcemi
- Odešlou se počty paketů v přihrádkách
- Server sečte klienty dohromady
- Najde lišící se přihrádky (statistika)
- Zeptá se klientů na klíče od anomálií

Plány do budoucna

- Ladění parametrů sběru
- Plugin histogram – top 10 IP adres
- Podpora dalších linkových vrstev
- Další pluginy v závislosti na výzkumu

Děkuji za pozornost

Michal Vaner • michal.vaner@nic.cz