Sentinel evolution

Rok 2020 a sběr dat na routerech Turris

Martin Prudek, Miroslav Hanák •
martin.prudek@nic.cz, miroslav.hanak@nic.cz •
11. 11. 2020

CZ.NIC | SPRÁVCE DOMÉNY CZ

Minipoty

- Minipot = minimální honeypot
- Honeypot – past na útočníka, sledování aktivity
- Minimální – připojení, přihlášení
- Odesílání dat do Sentinel infrastruktury
- Telnet – již od začátku
- HTTP, FTP, SMTP – od 1.8.2020

Minipoty

- Emulace nejpoužívanějších serverů
  - Splynutí z okolím – omezení identifikace
  - Žádný přístup k reálnemu systému
  - Nízká spotřeba systémových prostředků – CPU, RAM
- Hlavní princip interakce
  - Navázání spojení
  - Neúspěšná autentikace – sběr autentikačních dat
  - Ukončení spojení

Telnet minipot

- Ne klasický aplikační protokol
- Vzdálený přístup na CLI
- Autentikace není definována protokolem
- Dotaz na přihlášení a jméno, heslo = “uživatelská data“
- Sběr – uživatelské jméno, heslo
- Nejjednodušší minipot

HTTP minipot

- World Wide Web
- Bezestavový, request & response protokol
- Sběr – metoda, URL, User agent, uživatelské jméno, heslo
  - Basic autentikační schéma
- Složitější zpracování HTTP zprávy
  - Request line, headers, body
- Jednoduchá implementace protokolu

FTP minipot

- Přenos souborů
- Stavový, command & response protokol
- Sběr – uživatelské jméno, heslo
  - Parametry USER, PASS příkazů
- Jednoduché zpracování příkazů
- Stále poměrně jendoduchá implementace protokolu
  - Pouze control connection

SMTP minipot

- E-mail
- Stavový, command & response protokol
- LOGIN, PLAIN SASL autentikační mechanismy
- Sběr – uživatelské jméno, heslo
- Jednoduché zpracování příkazů
- Složitější protokol – session initialization, komplexnější autentikace
- Nejsložitější minipot

Minipoty – přehled nasbíraných dat

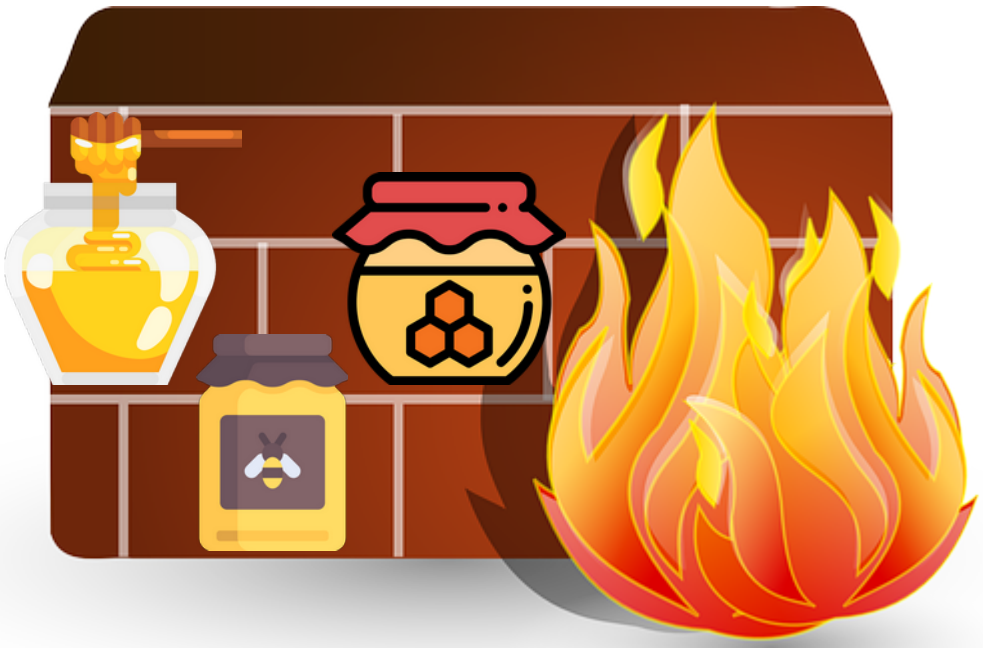
Počty a typy zachycených událostí

Událost	HTTP	FTP	SMTP	Telnet	Součet
Connect	5 181 313	2 970 934	401 530 346	20 404 313	430 086 906
Message	7 696 026	-	-	-	7 696 026
Login	-	2 702 801	399 069 128	2 065 538	403 837 467
Součet	12 877 339	5 673 835	800 599 474	22 469 851	841 620 399

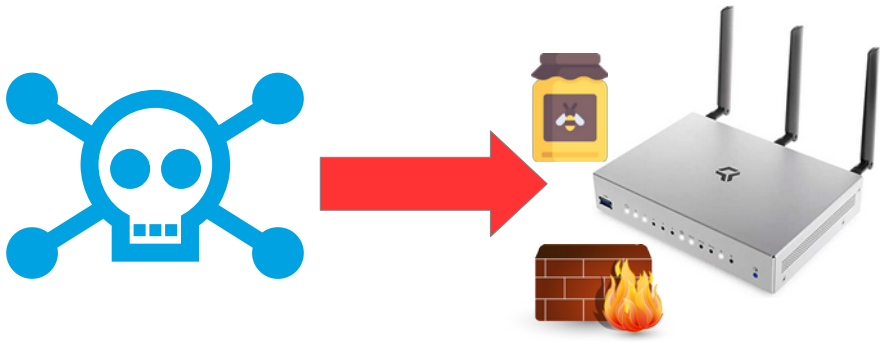
Počty unikátních IP adres

	HTTP	FTP	SMTP	Telnet	Součet	Globálně
Všechny události	239 619	15 599	10 453	793 182	1 058 853	959 984
Bez connect	216 521	7 813	1 810	28 503	319 974	248 026
Pokles počtu IP	10 %	50 %	83 %	96 %	70 %	74 %

Vliv nových minipotů na dynamický firewall

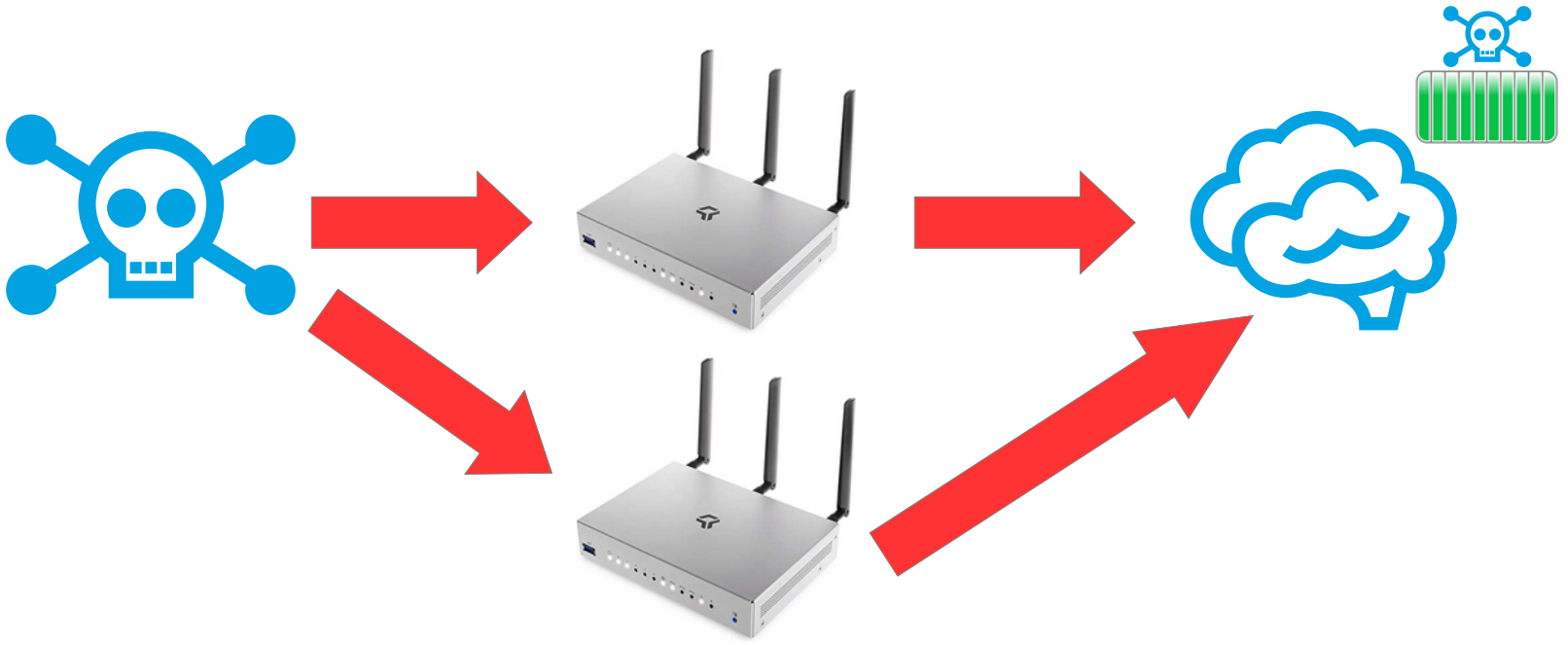


Turris:Sentinel dynamický firewall

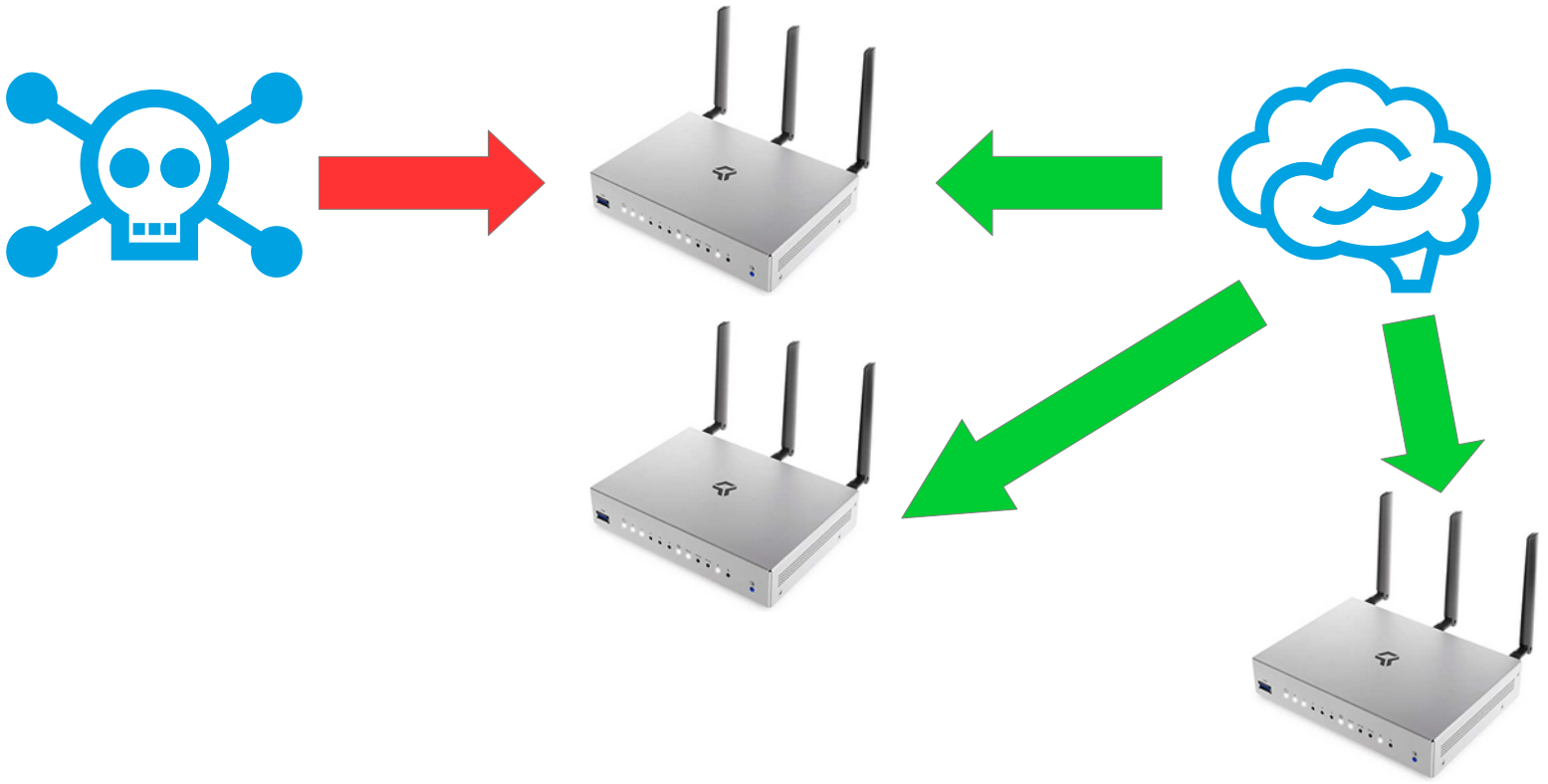


Turris:Sentinel dynamický firewall

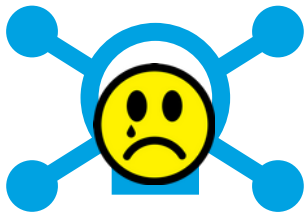
Turris:Sentinel dynamický firewall

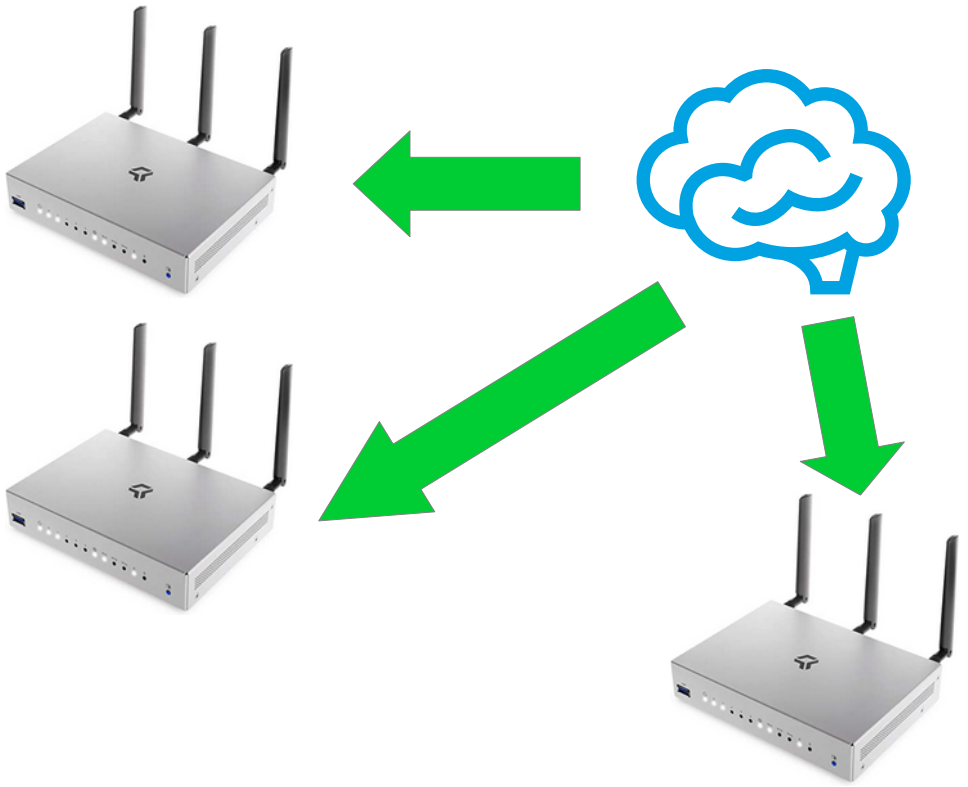


Turris:Sentinel dynamický firewall



Turris:Sentinel dynamický firewall

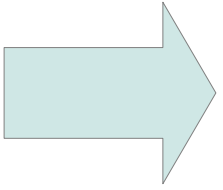


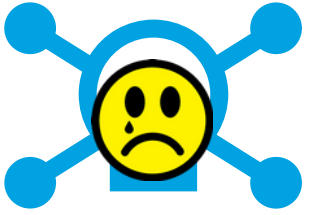


Turris:Sentinel dynamický firewall

- Maximálně 2 hlášení na každého

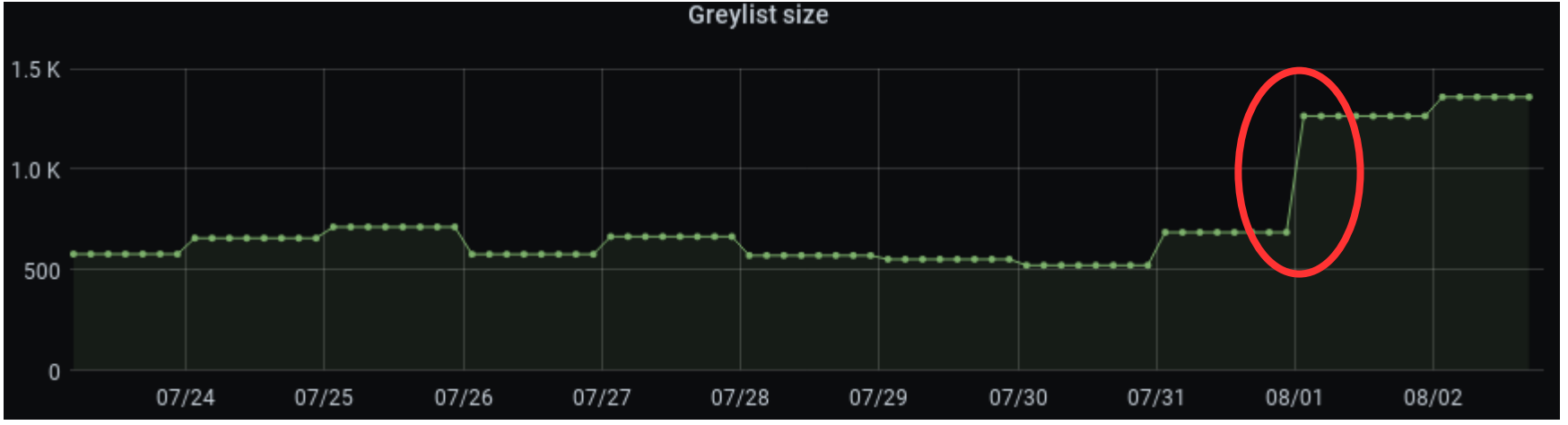
- Hlášení minimálně ze 2
- Nutné překročit práh skóre





Vývoj velikosti greylistu

- Po vydání nových minipotů

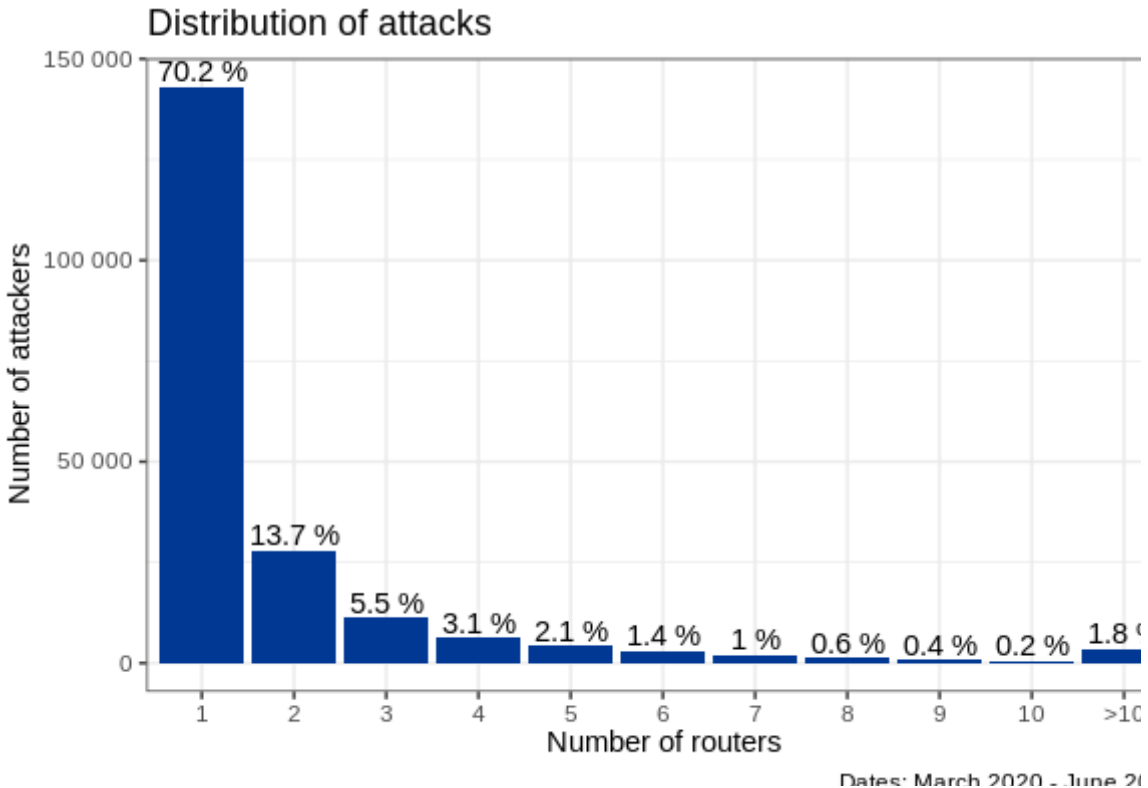


Vývoj velikosti greylistu

- Po vydání nových minipotů

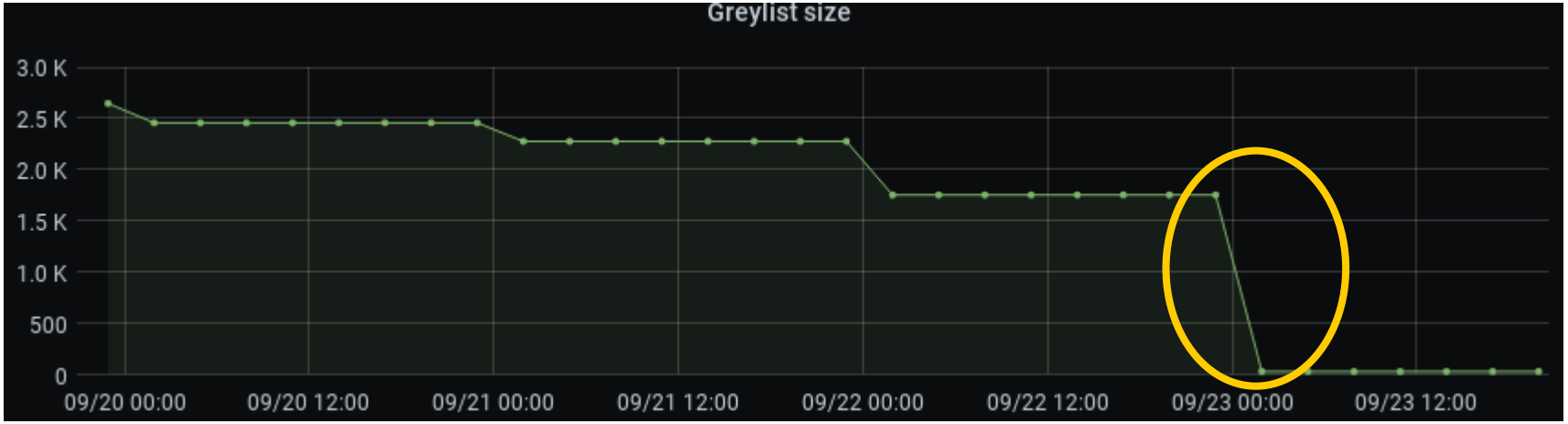
Vývoj velikosti greylistu

- >16% útočníku napadne alespoň 3 routery



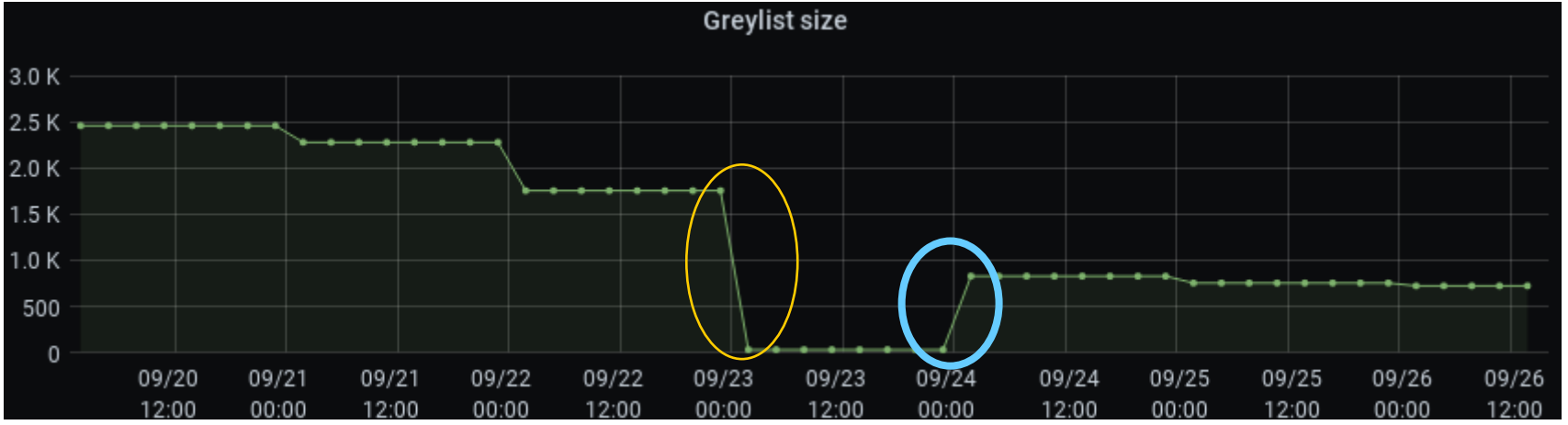
Vývoj velikosti greylistu

- Po vydání sentinelu do ostrého provozu
- Po zvýšení prahu pro umístění na greylistu



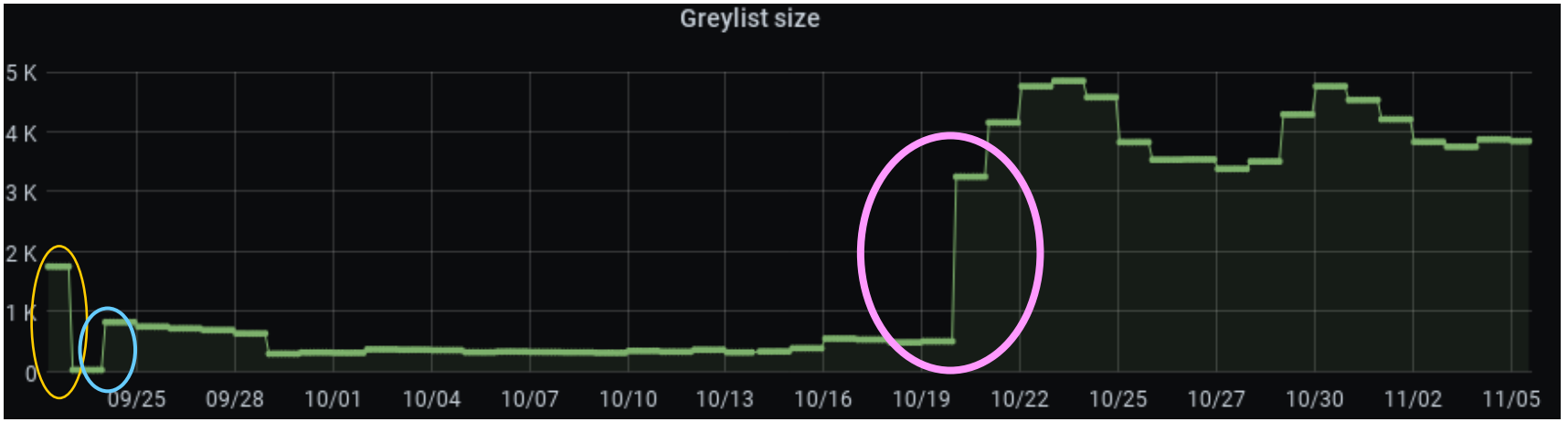
Vývoj velikosti greylistu

- Opětovné dočasné zvýšení prahu



Vývoj velikosti greylistu

- Po přepracovaní systému skórování



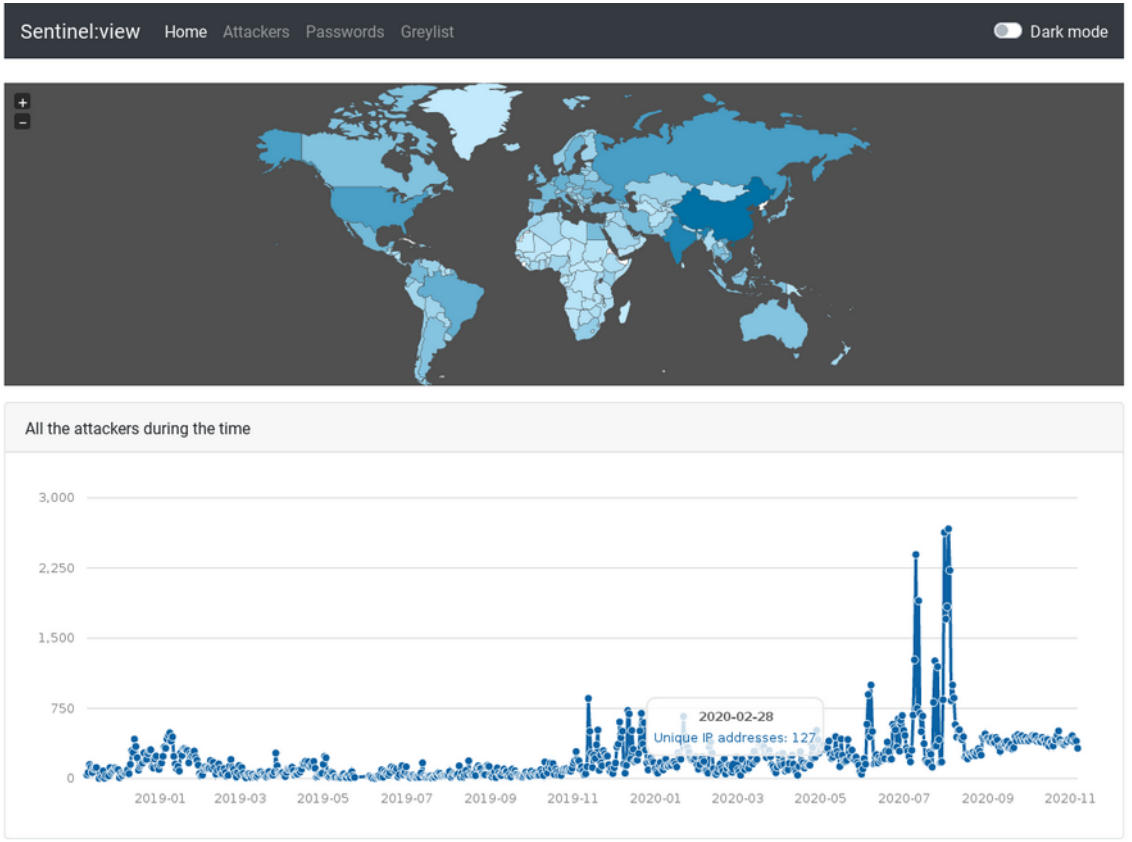
- ~7% ze všech průběžně hlášených adres

Další vylepšení Sentinelu za poslední rok

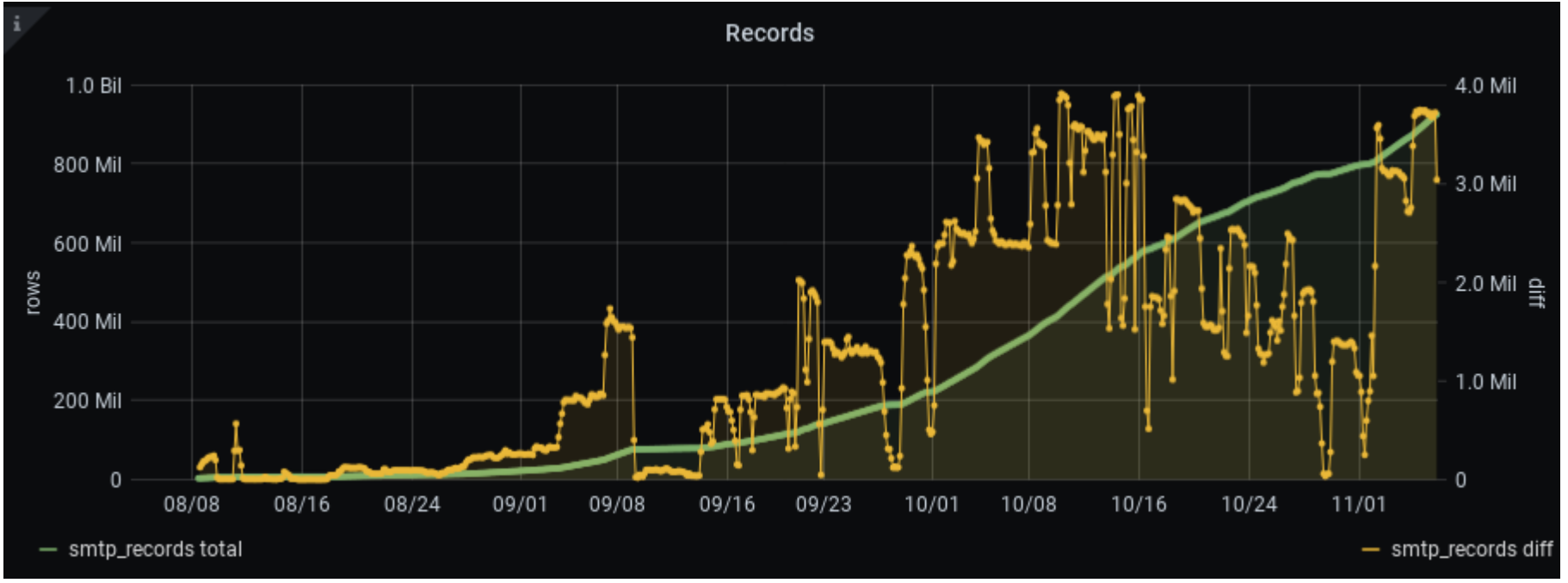
- Nový FW logs collector (používáme Netlink)
- Integrace Sentinel služeb na routeru
- Ladění certifikační autority
- Device token
- Safelist
- ReForis data collection tab

Výhled – view.sentinel.turris.cz

- Více statistik
- Prohlížení vlastních dat



Výhled


Records
1.0 Bil
800 Mil
600 Mil
400 Mil
200 Mil
0
rows
4.0 Mil
3.0 Mil
2.0 Mil
1.0 Mil
0
diff
08/08
08/16
08/24
09/01
09/08
09/16
09/23
10/01
10/08
10/16
10/24
11/01
smtp_records total
smtp_records diff

Děkuji za pozornost

Miroslav Hanák • miroslav.hanak@nic.cz

Martin Prudek • martin.prudek@nic.cz