

# Novinky v Turris Sentinel View

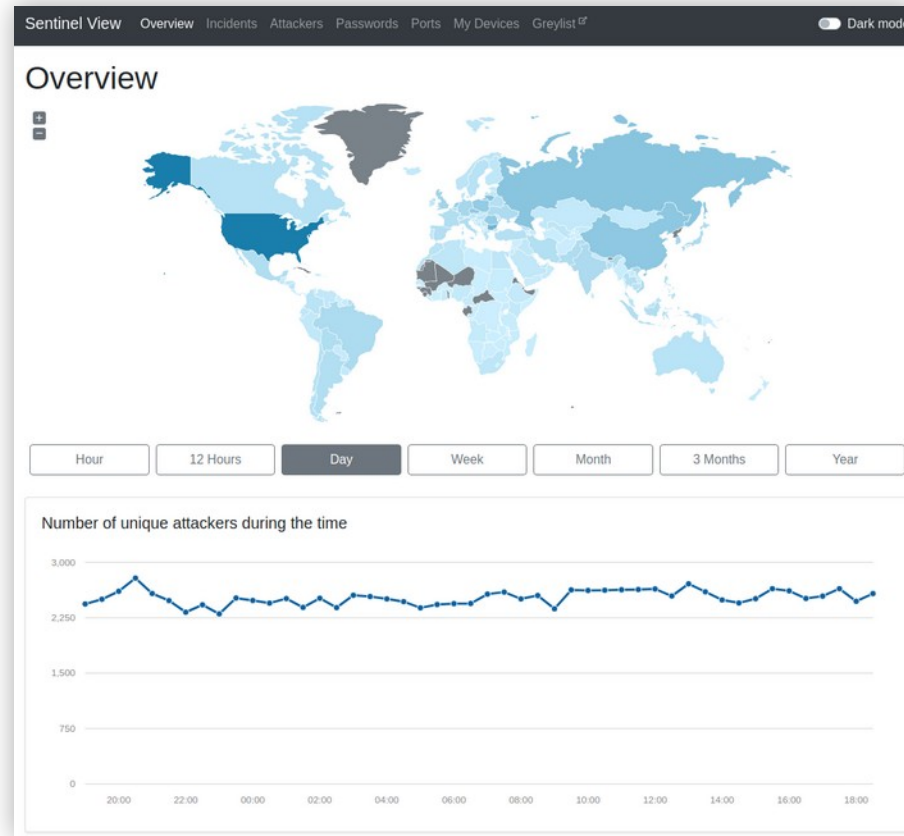
Od prvního vydání

Filip Hron • [filip.hron@nic.cz](mailto:filip.hron@nic.cz) • 23.11.2022

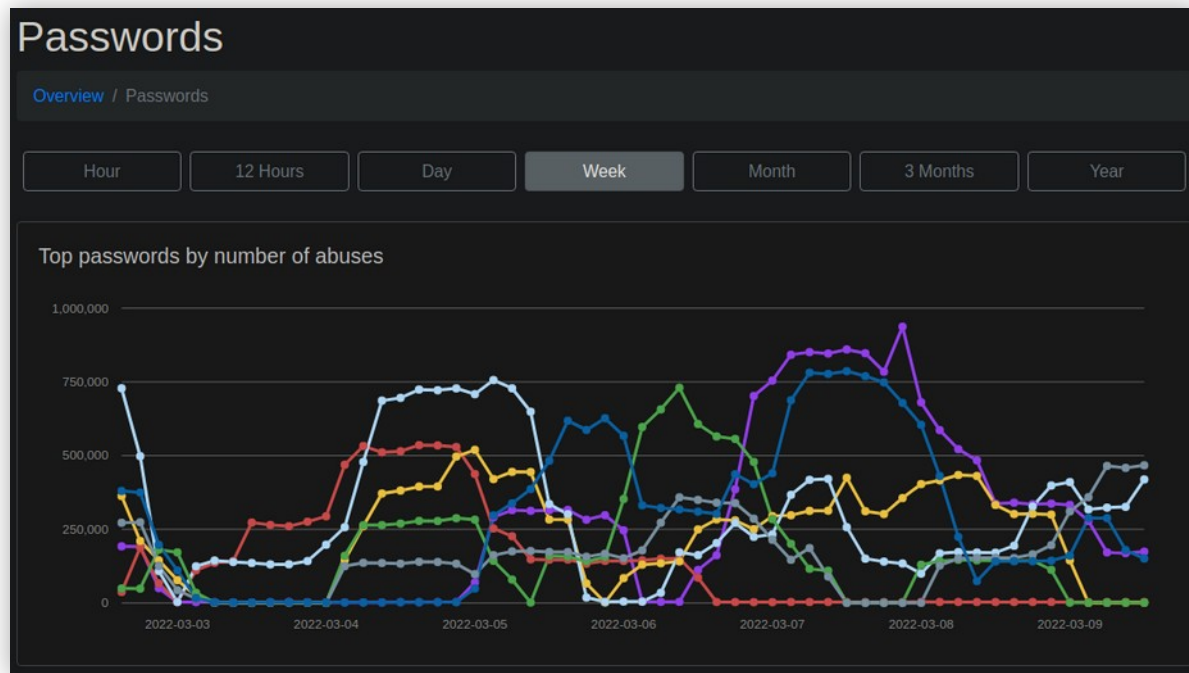
# Obsah

- První vydání Sentinel View, verze 1.0.0
- Verze 1.1.0
- Verze 1.2.0
- Sentinel Reporter

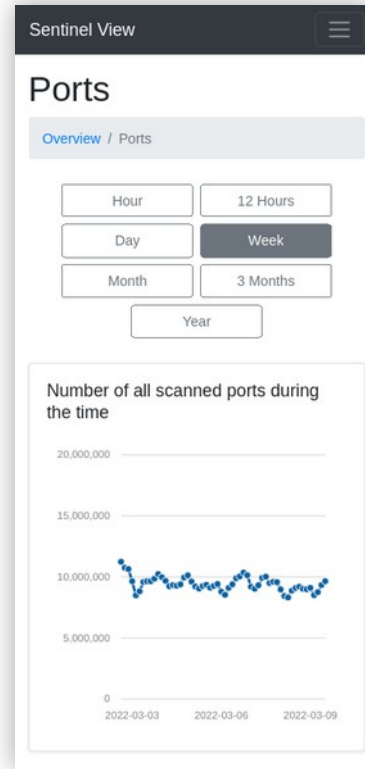
# Nový vzhled



# Filtrování v časových úsecích



# Responzivní vzhled





# Backend

- Agregace dat podle zobrazení
- Cachování náhledů

# První verze Sentinel View, shrnutí

- Nový vzhled
- Filtrování podle časových úseků
- Moje zařízení
- Vylepšený backend



# Události dynamického firewallu

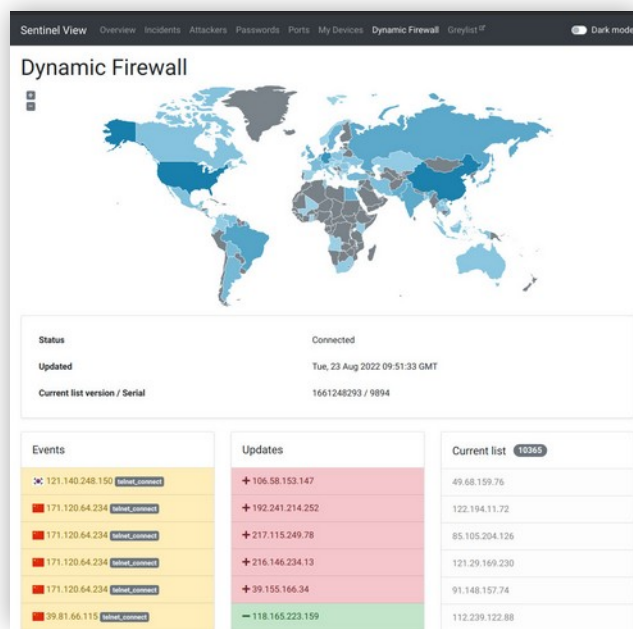
Events	
110.182.182.148	telnet_connect
81.215.14.117	telnet_connect
110.85.98.144	telnet_connect
167.71.210.106	telnet_connect
120.223.242.153	http_connect
132.247.105.174	telnet_connect
45.184.71.13	telnet_connect
80.82.77.139	smtp_connect
45.184.71.13	telnet_connect
117.203.50.136	telnet_connect
122.116.39.21	telnet_connect
119.163.42.219	smtp_connect
125.84.236.107	http_message
125.84.236.107	http_connect
46.1.33.193	telnet_connect
128.14.141.34	http_message
128.14.141.34	http_connect

Updates	
- 39.40.220.137	
+ 112.196.49.77	
- 94.64.108.231	
+ 119.180.112.234	
+ 182.126.88.81	
- 39.71.101.189	
+ 111.70.5.6	
- 196.221.204.80	
- 61.219.153.246	
+ 222.93.28.73	
+ 142.165.239.35	
+ 175.107.1.49	
- 115.50.2.122	
+ 61.241.170.171	
+ 120.231.221.234	
- 222.165.140.170	
+ 182.155.33.199	

Current list <span>10365</span>	
49.68.159.76	
122.194.11.72	
85.105.204.126	
121.29.169.230	
91.148.157.74	
112.239.122.88	
125.71.200.138	
115.55.244.254	
90.150.204.72	
27.44.104.91	
83.255.85.213	
114.154.217.191	
87.96.182.178	
220.134.75.121	
187.50.136.210	
145.239.154.82	
172.118.216.27	

# Verze 1.1.0, shrnutí

- Zobrazení událostí dynamického firewallu v reálném čase



# Sentinel Password Checker (rozhraní)

Sentinel View Threat Detection ▾ Dynamic Firewall Passwords checker ▾ Greylist [↗](#) Dark mode

## Sentinel password checker

Check if your password had been used by hackers to access minipots on Turrís routers.

**Oh no – the attackers are already guessing it!**

Your password has been used **4567878** times with service(s):

[telnet](#) [smtp](#) [ftp](#) [http](#)

The tags indicate the sources of accidents had been captured onto.

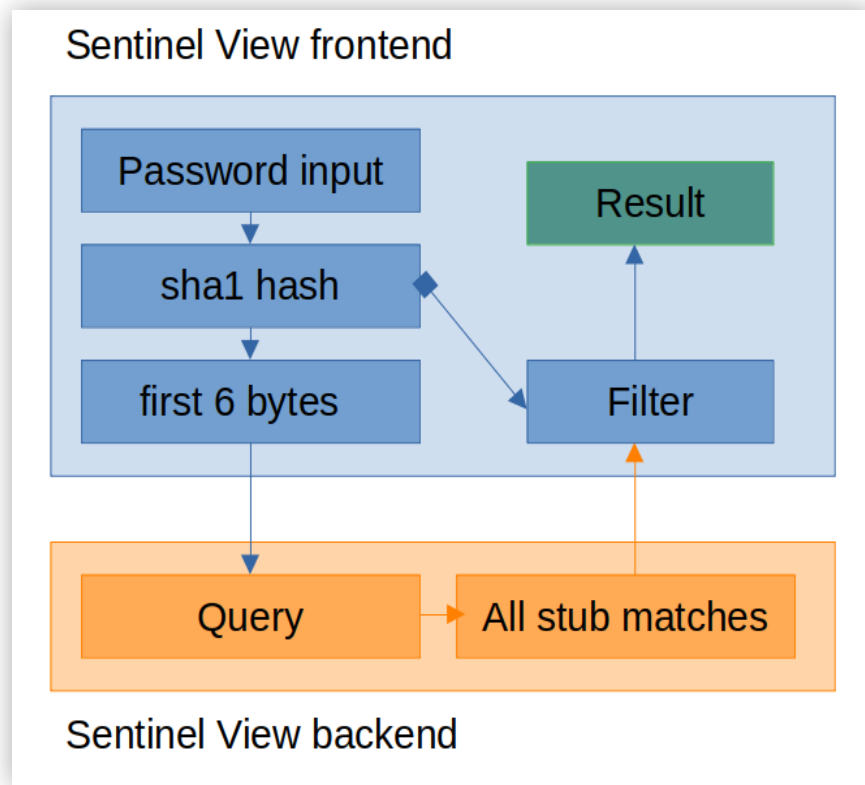
### Check password

We do not send your password over the internet. Your password is hashed and only first 6 bytes are sent to backend.

# Zdroj dat

- Odbočeno z ukládání ostrých dat z routeru
- Sha1
- počítadlo
- Služba minipotu (zdroj)

# Dotazování



# API

## Sentinel password checker API

You can use the API interface to query the first six bytes of the `sha1` hash of your password.

For example `password secret` has `sha1` hash hexdigest value of `e5e9fa1ba31ecd1ae84f75caaa474f3a663f05f4` and you will strip the first 6 characters, thus `e5e9fa`.

### Schema for API request

A message should look like the following:

```
{ "msg_type": "request", "hash": "e5e9fa" }
```

### Request JSON schema

[Click to expand](#)

```
{
  "type": "object",
  "description": "Api message request",
  "properties": {
    "msg_type": { "enum": ["request"] },
    "hash": {
      "type": "string",
      "pattern": "^[a-z0-9]{6}$"
    }
  },
  "required": ["hash", "msg_type"],
  "additionalProperties": false
}
```

# Sentinel Password Checker, shrnutí

- Rozhraní
- Zdroje dat
- Dotazování
- API
- Podle služby Have I Been Pwned

# Sentinel Reporter

- Více výsledků (>15)
  - Složitější na výpočet
- PDF formát ke stažení
  - Další výstupy
- Komplexnější výsledky
  - Porovnání s předchozím měsícem
  - Popis dat
  - pro údaje za jeden měsíc
- Lepší dostupnost

**Port Trends**

This section shows monthly trends in scans for port/protocol combination. The descriptions serves as reference what service might the attacker be interested in. You definitely should carefully read it and make sure not to perhaps use listed ports as defaults on your servers in that regard.

port	proto	counter	description
6881	UDP	49750	BitTorrent beginning of range of ports used most often
51413	UDP	49305	N/A
55555	UDP	43832	N/A
445	TCP	30368	Microsoft-DS (Directory Services) Active Directory,   Microsoft-DS (Directory Services) SMB
27032	UDP	24593	Steam (In-Home Streaming)
39115	UDP	11215	N/A
2323	TCP	10541	N/A
1433	TCP	9595	Microsoft SQL Server database management system (MSSQL) server
8080	TCP	8130	Alternative port for HTTP. See also ports 80 and 8008.   Apache Tomcat, Atlassian JIRA application

1a2b3c4d	44189	121534	+77345
aaa	70400	120503	+50103
password	95204	120374	+25170
p@ssw0rd1	63794	119886	+56092
a1b2c3	38490	118523	+80033
scanner123	52513	117544	+65031
123456	154468	117505	-36963
1q2w3e	33574	117393	+83819
000000	85890	116695	+30805
support	39458	116614	+77156
mail	64786	116406	+51620



# Díky za pozornost

Filip Hron • [filip.hron@nic.cz](mailto:filip.hron@nic.cz)

Více na <https://blog.nic.cz/author/fhron/>