Novinky v Turris Sentinel View

Od prvního vydání

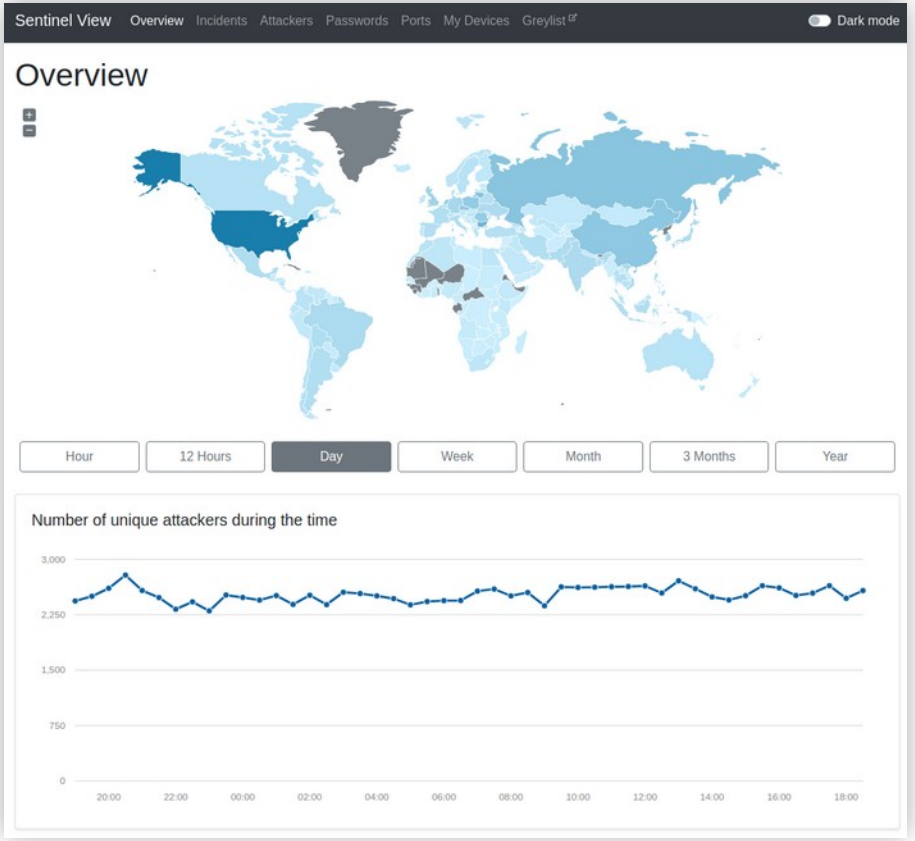
Filip Hron • filip.hron@nic.cz • 23.11.2022

TURRIS

Obsah

TURRIS

Nový vzhled

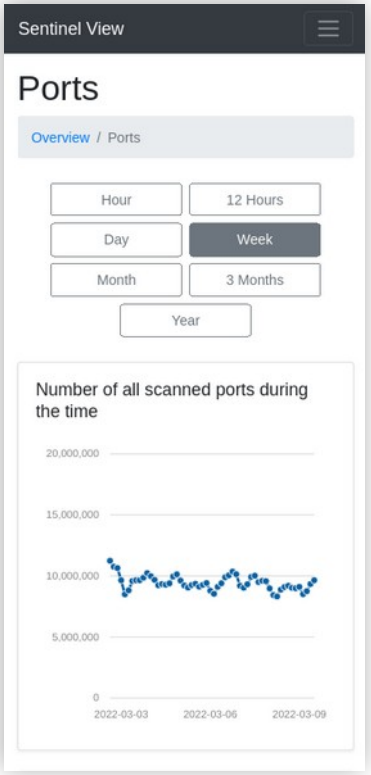


TURRIS

Filtrování v časových úsecích

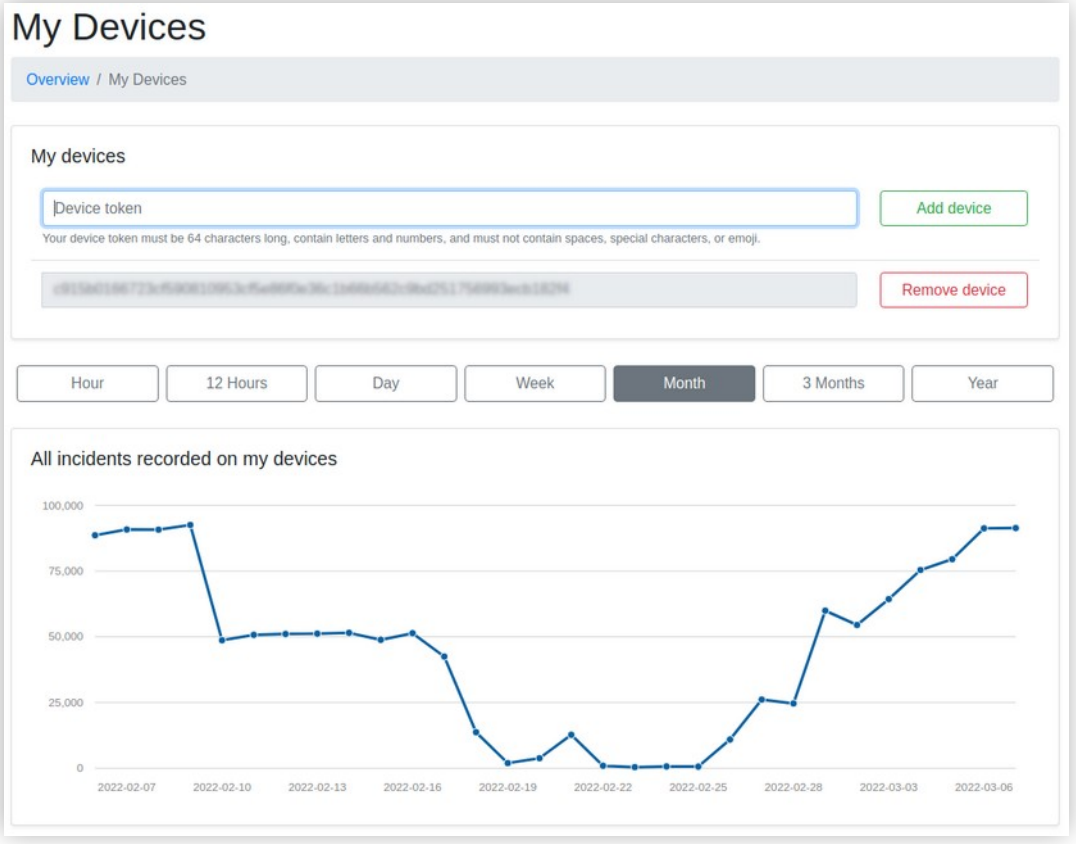
TURRIS

Responzivní vzhled



TURRIS

Moje zařízení



TURRIS

Backend

- Agregace dat podle zobrazení
- Cachování náhledů

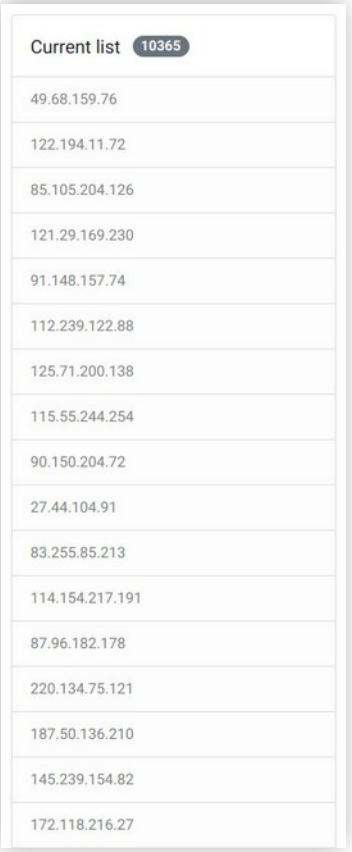
TURRIS

První verze Sentinel View, shrnutí

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

TURRIS

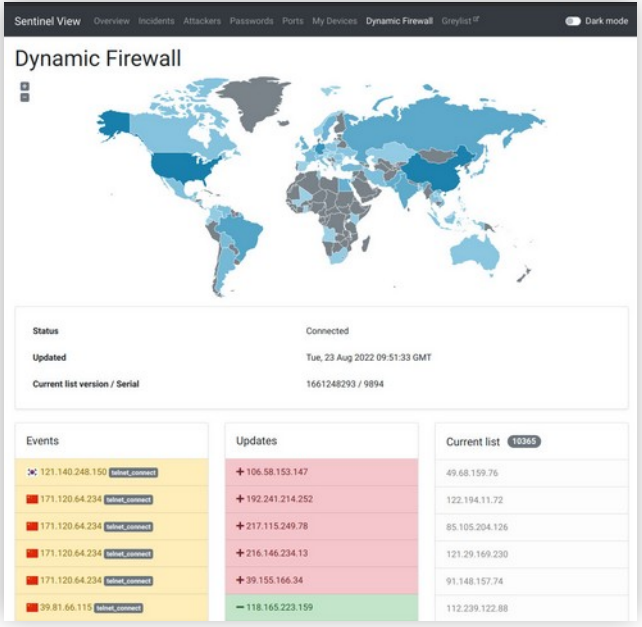
Události dynamického firewallu



TURRIS

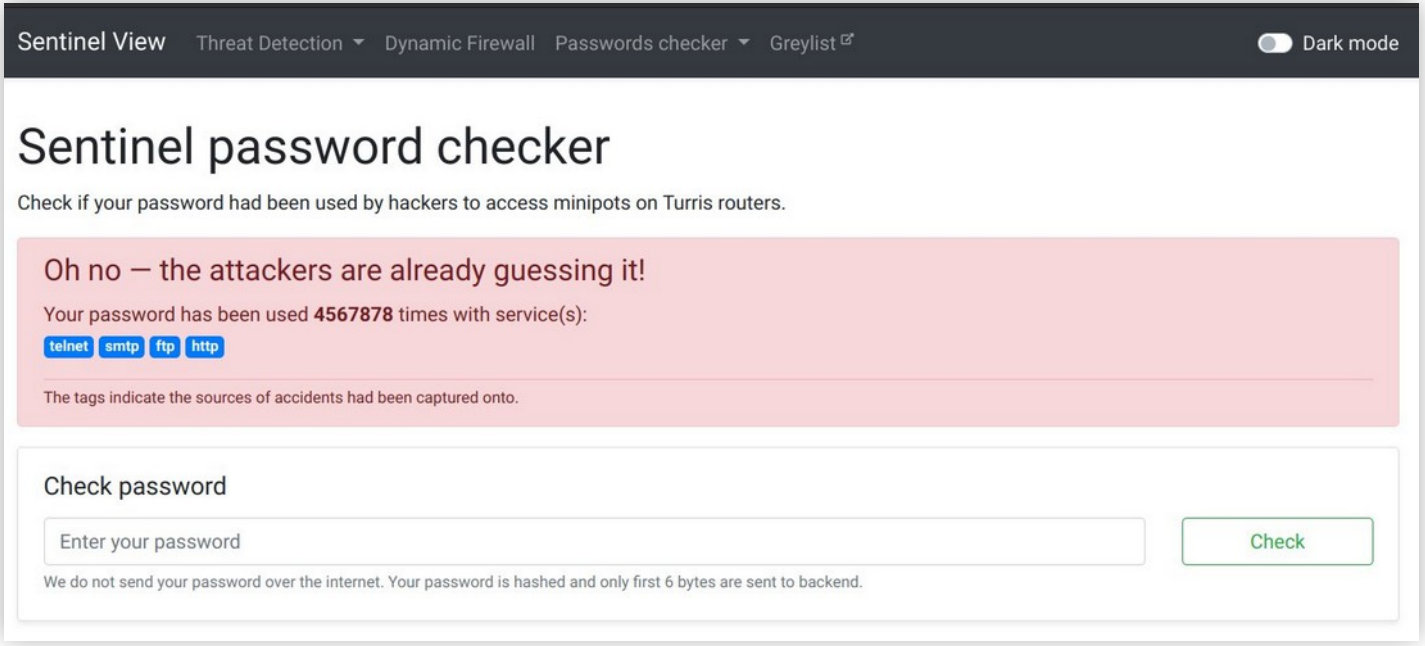
Verze 1.1.0, shrnutí

- Zobrazení událostí dynamického firewallu v reálném čase



TURRIS

Sentinel Password Checker (rozhraní)



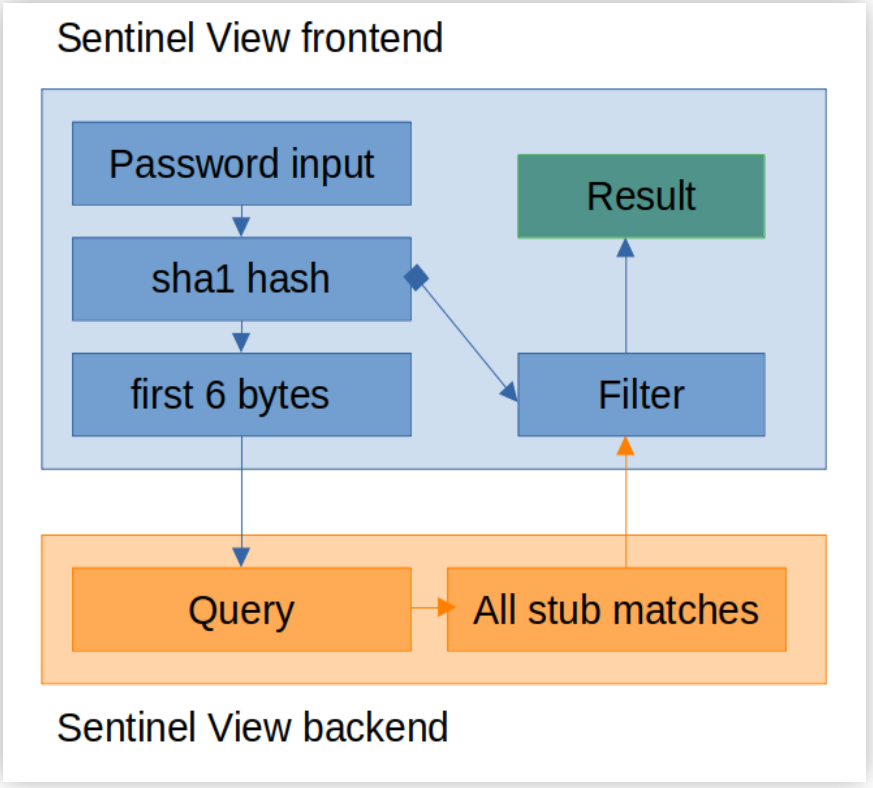
TURRIS

Zdroj dat

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

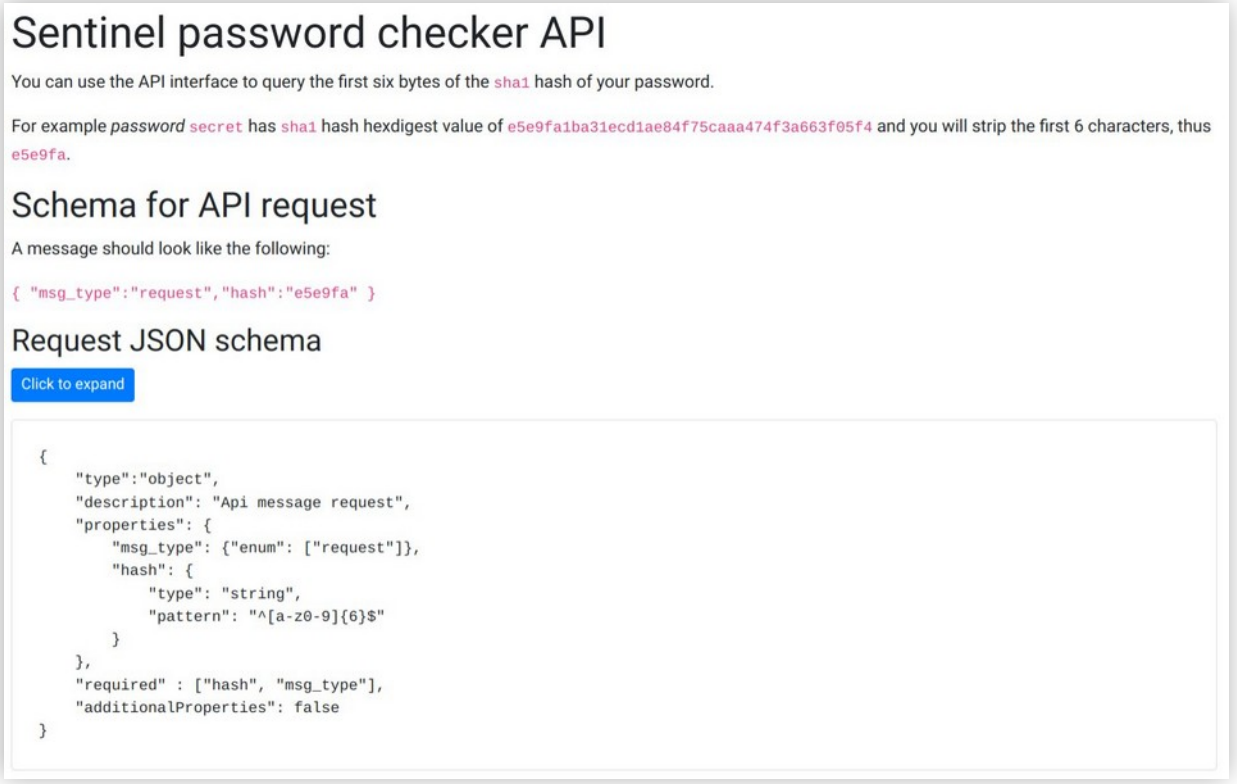
TURRIS

Dotazování



TURRIS

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
}
```

TURRIS

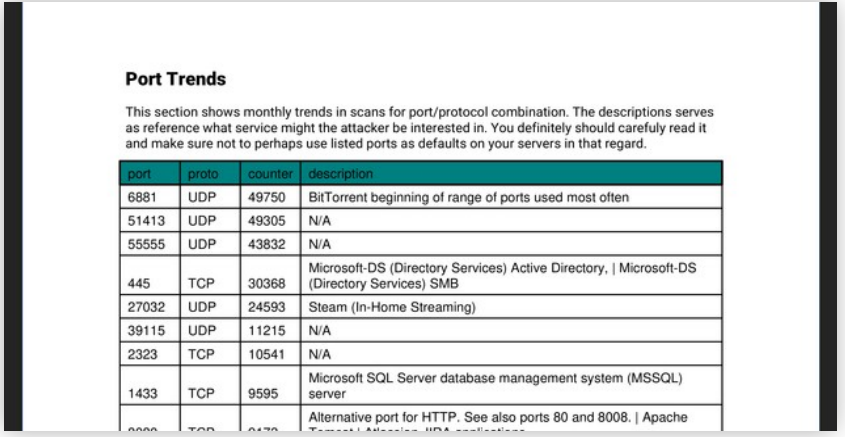
Sentinel Password Checker, shrnutí

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

TURRIS

Sentinel Reporter

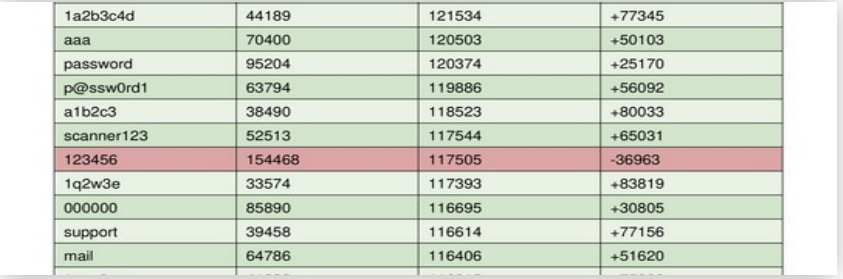
- Více výsledků (>15)
  - Složitější na výpočet
- PDF formát ke stažení
  - Další výstupy
- Komplexnější výsledky
  - Porovnání s předchozím měsícem
  - Popis dat
  - pro údaje za jeden měsíc
- Lepší dostupnost



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 carefuly 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
[illegible]	[illegible]	[illegible]	Alternative port for HTTP. See also ports 80 and 8008. | Apache [illegible]



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

TURRIS