

# Projekt PROKI po pěti letech

Pavel Bašta • [pavel.basta@nic.cz](mailto:pavel.basta@nic.cz) • 12. 11. 2020



# PROKI

## PREDIKCE A OCHRANA PŘED KYBERNETICKÝMI INCIDENTY



MINISTERSTVO VNITRA  
ČESKÉ REPUBLIKY

Projekt „**Predikce a ochrana před kybernetickými incidenty (PROKI)**“ (VI20152020026) je realizován v rámci Programu bezpečnostního výzkumu ČR na léta 2015 – 2020.



# PROKI (PRedikce a Ochrana před Kybernetickými Incidenty)

- Motivace
  - Dostat informace o kybernetických událostech a incidentech do koncových sítí
    - Velké množství různých zdrojů
    - Agregace dat dle sítí
  - Získat nástroj pro základní analytickou práci s incidenty
    - Incidenty v širším kontextu
    - Nalezení hlubších souvislostí a získání nových informací



# Používaný SW

- IntelMQ
  - Společně vyvíjený nástroj (Rakouskou, Portugalsko a Česká republika)
  - Řeší tři základní problémy
    - Formát (vnitřní struktura) předávaných dat
      - CSV, XML, JSON
    - Metoda doručení dat
      - E-mail, HTTP, vlastní API
    - Různost samotných informací (doména x IP)



# Používaný SW

- Intel MQ
  - Vyvinuté komponenty
    - Turris Greylist Parser
    - Generický CSV parser
    - SQL Bot
    - Abusis Expert
    - Custom filter
    - Envelope
    - TCP Output TCP Collector



# Používaný SW

- Redis
  - Dočasné úložiště dat pro IntelMQ
  - IntelMQ sem ukládá získaná data
  - Různé komponenty si pak data čtou a ukládají zpět na místo určené pro další komponentu v řetězci
- Logstash
  - Pracuje s daty, která jsou na výstupu IntelMQ komponenty předána do příslušné fronty úložiště Redis
  - Transformuje data před jejich uložením do databázového enginu Elasticsearch.
  - Sjednocení velikosti počátečních písmen, formátu data, formátu času



# Používaný SW

- Elasticsearch
  - Vyhledávací a databázový engine
  - Udržuje informace o incidentech pro další analýzy
- Kibana
  - Webová aplikace pro vizualizaci dat uložených v komponentě Elasticsearch
  - Vyhledávání, vizualizace, vytváření dashboardů



# Používaný SW

- PROKI API
  - Alternativa k rozesílání informací emaily
  - Zájemce si požádá o API klíč a zaregistruje rozsah IP adres, ze kterých bude k API přistupovat
  - Správce si tak může řídit frekvenci získávání informací nebo definovat požadavky na data za konkrétní období
- Build query
  - Nástroj pro porovnávání rozsáhlých CSV vůči datům v PROKI





# Výstupy projektu PROKI

- Informování o kybernetických bezpečnostních událostech a incidentech
- 43 zdrojů (honeypoty, blacklisty, nástroje monitorující zranitelnosti, sinkholing botnetů)
- Agregace dle sítí
- Na žádost komunity nyní zasíláno 2 x týdně
- Ostrý start 25.10.2017 (do té doby jen vybrané subjekty)



# Výstupy projektu PROKI

- Rok 2018
  - 31 324 zpráv do 862 sítí
- Rok 2019
  - 27477 zpráv do 623 sítí
- Rok 2020 (do srpna)
  - 22651 zpráv do 644 sítí



# Výstupy projektu PROKI

- Kritická infrastruktura
  - V PROKI se objevují i události přímo směřující na infrastrukturu institucí spadajících pod § 8 odst. 4 ZKB
  - Problém v reportování přímo dotčeným osobám (whois), nutnost předávat přes třetí stranu (ISP)
  - Ke konci roku 2017 přidána funkcionality, umožňující zasílat tyto informace přímo Národnímu úřadu pro kybernetickou a informační bezpečnost



# Výstupy projektu PROKI

- Reportování zranitelností
  - Zahrnuty na základě počátečních analýz
  - Důležitý preventivní prvek
  - Otevřené SMTP relay, otevřená nechráněná sdílení dat, otevřené nechráněné služby typu TFTP, Telnet, SNMP nebo otevřené DNS resolvery



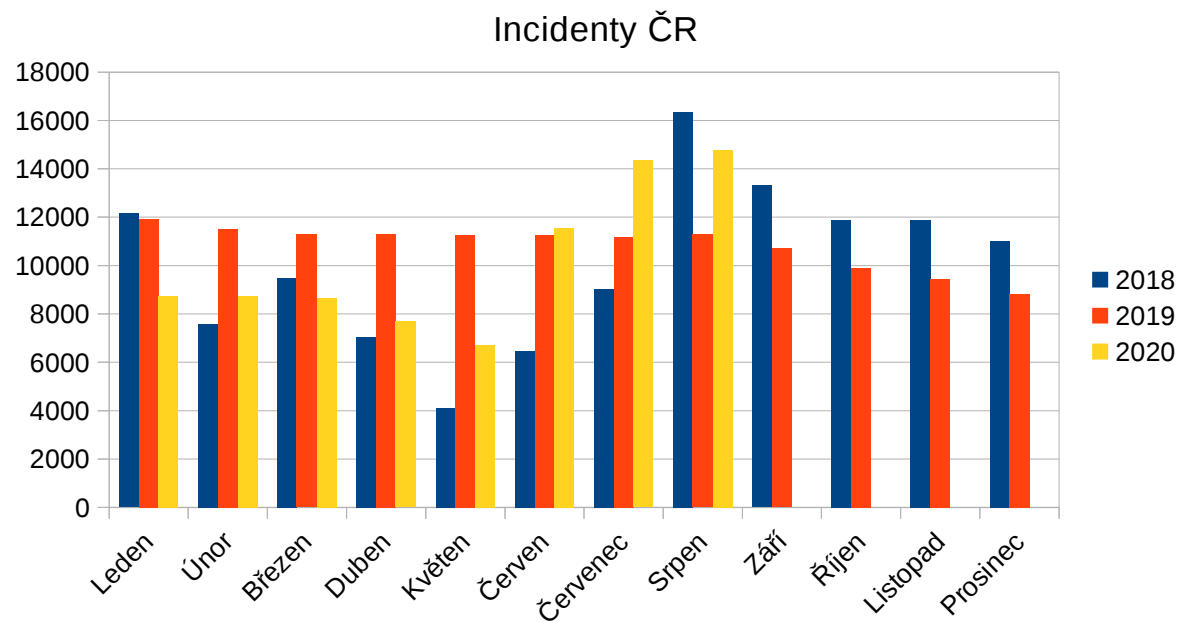
Table

JSON

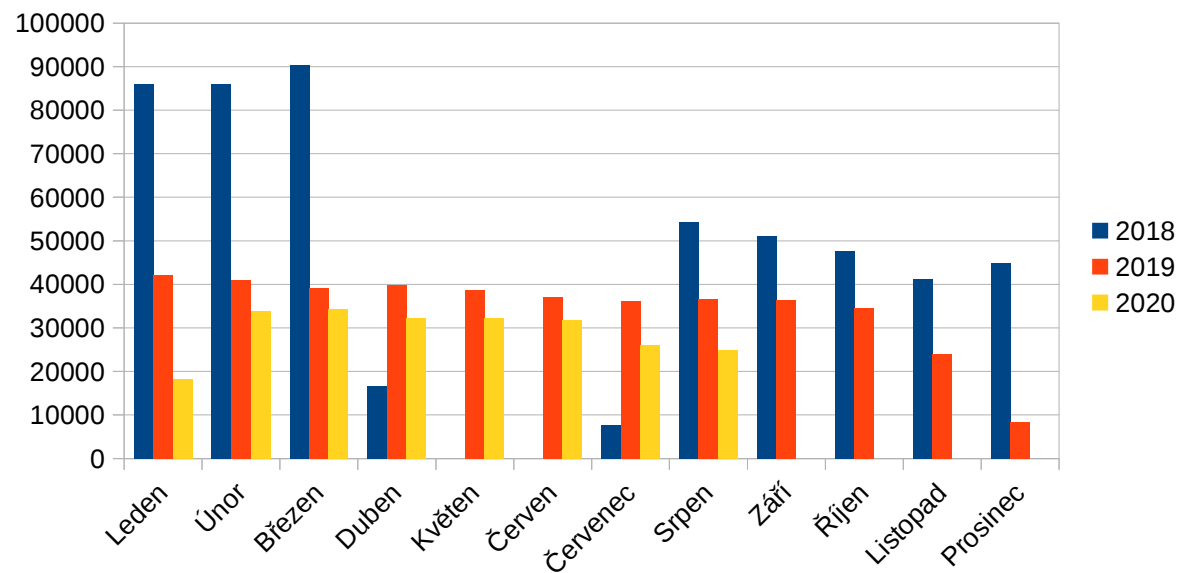
[View surrounding documents](#)[View single document](#)

|                             |                                 |
|-----------------------------|---------------------------------|
| @timestamp                  | February 8th 2020, 09:23:09.000 |
| t _id                       | 74nlI3ABPLNlXAWfkm06            |
| t _index                    | intelmq-2020.02                 |
| # _score                    | -                               |
| t _type                     | event                           |
| t classification.identifier | dns-open-resolver               |
| t classification.taxonomy   | vulnerable                      |
| t classification.type       | vulnerable service              |
| # extra.min_amplification   | 6.952                           |
| t extra.tag                 | openresolver                    |
| # feed.accuracy             | 50                              |
| t feed.name                 | dns-open-resolvers              |
| t protocol.application      | dns                             |
| t protocol.transport        | udp                             |

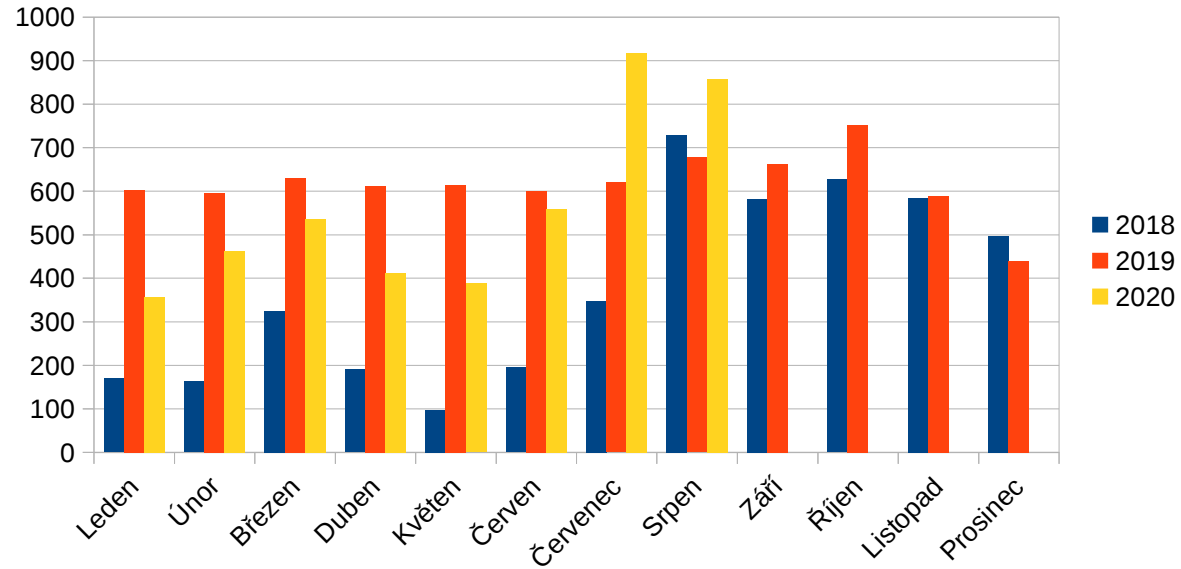




## Zranitelnosti ČR

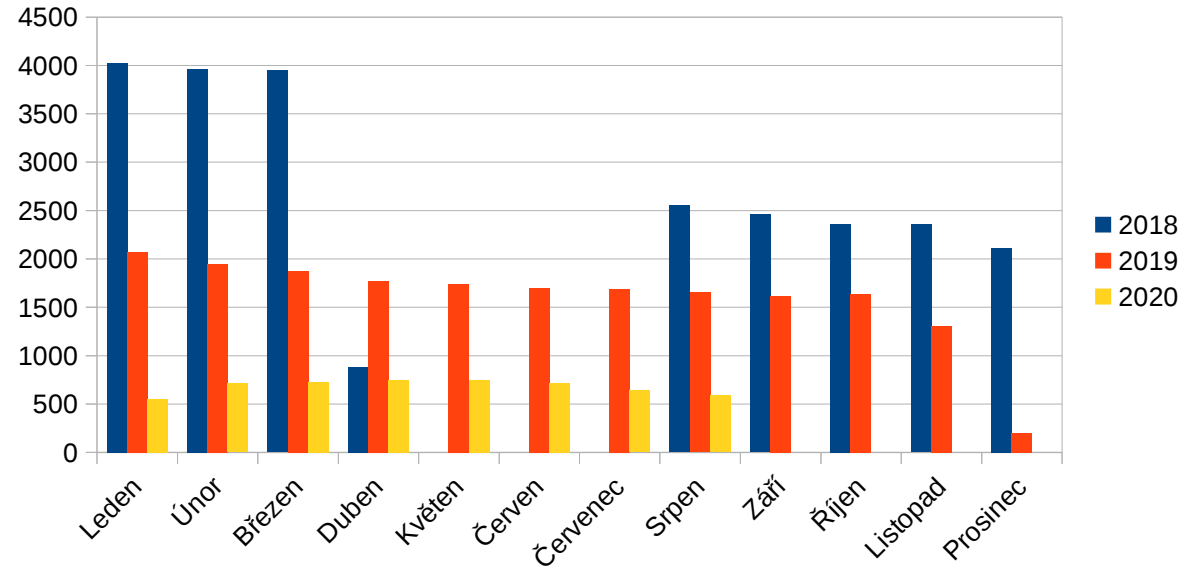


## Incidenty NUKIB





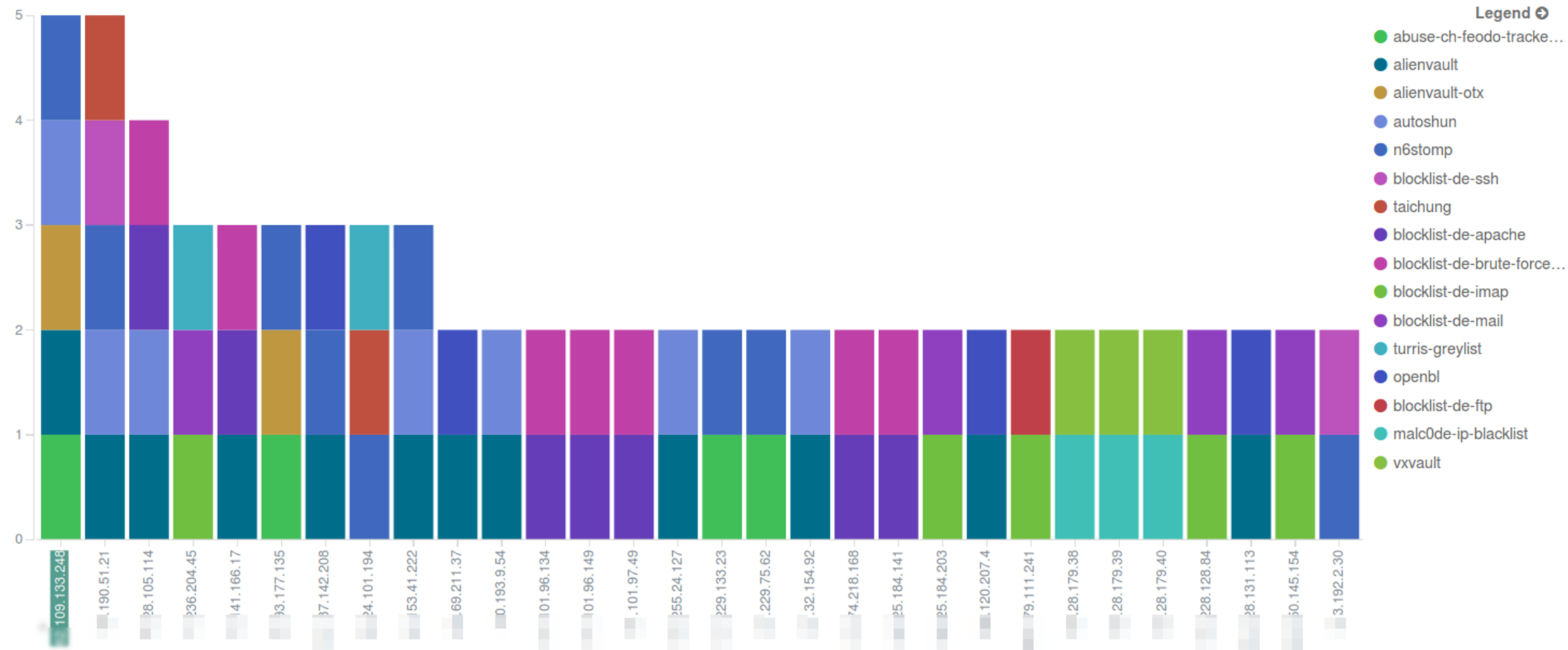
## Zranitelnosti NUKIB



# Výstupy projektu PROKI

- Analytické rozhraní PROKI
  - Vyhledávání, vizualizace a dashboard
  - Fulltext nebo konkrétní parametry (typ incidentu, zdrojová IP, zdroj informací a další)
  - Jednotlivé vizualizace mohou být na jednom dashboardu





source.ip: Descending

## .109.133.248 IP address information

### Geolocation

Country CZ

Autonomous System 

### Passive DNS replication

VirusTotal's passive DNS only stores address records. **The following domains resolved to the given IP address.**

2016-01-16 myqbee 

2016-01-10 mojeglou 

2016-01-06 hv2248. 

### Latest detected URLs

Latest URLs hosted in this IP address **detected by at least one URL scanner or malicious URL dataset.**

4/66 2016-02-07 17:51:47 http:// 09.133.248/

2/66 2016-02-05 13:16:57 https:// .109.133.248:444/

2/66 2016-02-04 11:48:31 https:// .109.133.248:444/dridex/220/c2-node/

2/66 2016-02-01 13:16:30 https:// .109.133.248:444/dridex/220/c2-node

2/66 2016-01-22 04:54:16 https:// .109.133.248/

2/66 2016-01-15 12:32:03 http:// 09.133.248:444/

### Latest undetected files that were downloaded from this IP address

Latest files that are **not detected by any antivirus solution and were downloaded by VirusTotal from the IP address provided.**

0/55 2015-12-21 14:21:35 4bfe514f9c9090f613ca7da05c40f4a747e1bcc8a22482f680ec3a097fb21cc3

| LEFT          | RTYPE | RIGHT    |
|---------------|-------|----------|
| aaw5zjuu.info | A     | 56.64.97 |
| acl4tsgf.info | A     | 56.64.97 |
| aebmayn.info  | A     | 56.64.97 |
| ahwqxmm.info  | A     | 56.64.97 |
| ajdxzru.info  | A     | 56.64.97 |
| akfbjke.info  | A     | 56.64.97 |
| anpvqug.info  | A     | 56.64.97 |
| antxxit.info  | A     | 56.64.97 |
| aplrcbp.info  | A     | 56.64.97 |
| apm3qjyp.info | A     | 56.64.97 |
| asbojayg.info | A     | 56.64.97 |
| ato2voqt.info | A     | 56.64.97 |
| ayfdzrc.info  | A     | 56.64.97 |
| azo1pinz.info | A     | 56.64.97 |
| badnnri.info  | A     | 56.64.97 |
| bavwehfm.info | A     | 56.64.97 |
| bicembyn.info | A     | 56.64.97 |
| bjewzvj.us    | A     | 56.64.97 |
| bjiwchl.us    | A     | 56.64.97 |
| bndosgs.us    | A     | 56.64.97 |
| bnizxyi.us    | A     | 56.64.97 |
| bnxextd.info  | A     | 56.64.97 |
| boaerbp.info  | A     | 56.64.97 |
| braftam.us    | A     | 56.64.97 |



# Výstupy projektu PROKI

- Využívání dalšími subjekty, reputační databáze
- Zaměření na zvlášt' zranitelná zařízení
  - 2019 – data z projektu Shodan
  - IP kamery, Routery, SCADA

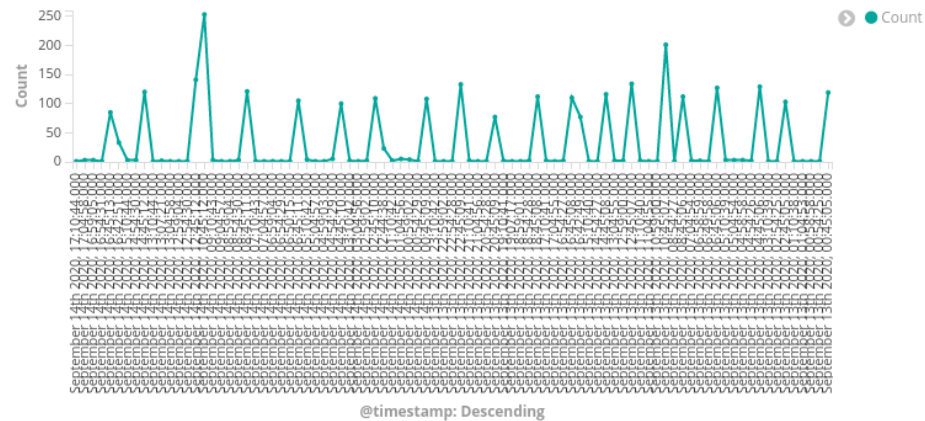


|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| @timestamp                    | 🔍📄🗂️🌟 September 2nd 2019, 01:08:59.000                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| t_id                          | 🔍📄🗂️🌟 b-QW72wB_HSDMyDs0iGg                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| t_index                       | 🔍📄🗂️🌟 intelmq-2019.09                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| #_score                       | 🔍📄🗂️🌟 -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| t_type                        | 🔍📄🗂️🌟 event                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| t_classification.identifier   | 🔍📄🗂️🌟 pop                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| t_classification.taxonomy     | 🔍📄🗂️🌟 intrusion attempts                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| t_classification.type         | 🔍📄🗂️🌟 brute-force                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| #destination.port             | 🔍📄🗂️🌟 110                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| #extra.source.local_port      | 🔍📄🗂️🌟 46,485                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| #feed.accuracy                | 🔍📄🗂️🌟 50                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| t_feed.name                   | 🔍📄🗂️🌟 spamhaus-cert                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| t_feed.url                    | 🔍📄🗂️🌟 https://portal.spamhaus.org/cert/api.php?cert=CSIRT.CZ&                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| t_protocol.application        | 🔍📄🗂️🌟 pop                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| t_protocol.transport          | 🔍📄🗂️🌟 tcp                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| t_raw                         | 🔍📄🗂️🌟 OyBCb3RzIHdpdGhv dXQgdGl tZSBmaWx0ZXIsIHB yZX BhcmV kIGZvc iBDU01SVC5DW iBvbiBV VEM gPSBTdw4gU2VwICA xIDI zOjAw0jA0ID IwMTkK0yBDb3B5cm lnaHQgwqkgM jAx0SBUaGU gU3BhbWhhdXMgUHJvamVjdCBMdGQuIEFsbCB yaWdodHMgc mVzZXJ2ZW QuCjsgTm8gc mUtZG lzdH JpYnV0aW9 uIG9yIHB1Ymx pYyBhY2N1c3M gYWxs b3d1ZCB3aXR ob3V0IFNwYW loYXVzIH B1cm1pc3Npb24uCjsgRml1bGRzIG Rlc2NyaXB0aw9u0go7CjsgMSAtIEluZmVjdGVk IE1QCjsgMiAtIEFTT go7IDMgL SBDb3VudHJ5IE NvZGUK0yA0IC0gTG FzdHNlZW4gVG1tZXN0YW1wIChpb1BVVE MpCjsgNSAtIEJvdCB0YW1lCjsgICBDb21tYW5kICYgQ29udHJvbCAoQyZDKSBpbmZvc m1hdGlvbiwgawYgYXZhaWxhYmx10go7IDYgLSBDJkMgRG9tYWluCjsgNyAtIFJlbW90ZSBJU CAoAY29ubmVjdGluZyB0bykK0yA4IC0gUmVtb3RlIFBvcnQgKG Nvb m5lY3RpbmcgdG8pCjsg0SA tIE xvY2FsIFBvcnQK0yAXMC AtIFByb3RvY29sCjsgICBBZGRpdGlvbmFsIGZpZWxkc yBtYXkgYm UgYWRkZWQgaW4gdGhlIGZ1dHVyZSB3aXR ob3V0IG5vdG1jZQ o7CjsgaXAsIGFzb iwgY291bnRyeSwgbGF zdHNlZW4sIGJvdG5hbWUsIGRvbWFpbiwgcmVtb3RlX21wLCByZW1vdGVfcG9ydCwgbG9jYWxf cG9ydCwgchJvdG9jb2wKOwo40S4yMDMuMTM3LjMxLEFTMjU1MTIsQ1osMTU2NZzM3NDY1Nixwb3AsLSwtLDExMCw0NjQ4NSx0Y3A= |
| t_source.abuse_contact        | 🔍📄🗂️🌟 abuse@ [redacted]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| t_source.asn                  | 🔍📄🗂️🌟 25512                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| t_source.geolocation.cc       | 🔍📄🗂️🌟 CZ                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| t_source.geolocation.city     | 🔍📄🗂️🌟 uvaly                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| #source.geolocation.latitude  | 🔍📄🗂️🌟 48.733                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| #source.geolocation.longitude | 🔍📄🗂️🌟 16.683                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 🖥 source.ip                   | 🔍📄🗂️🌟 [redacted].137.31                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| t_source.network              | 🔍📄🗂️🌟 [redacted].128.0/17                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 🕒 time.observation            | 🔍📄🗂️🌟 September 2nd 2019, 01:08:59.000                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 🕒 time.source                 | 🔍📄🗂️🌟 September 1st 2019, 23:50:56.000                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

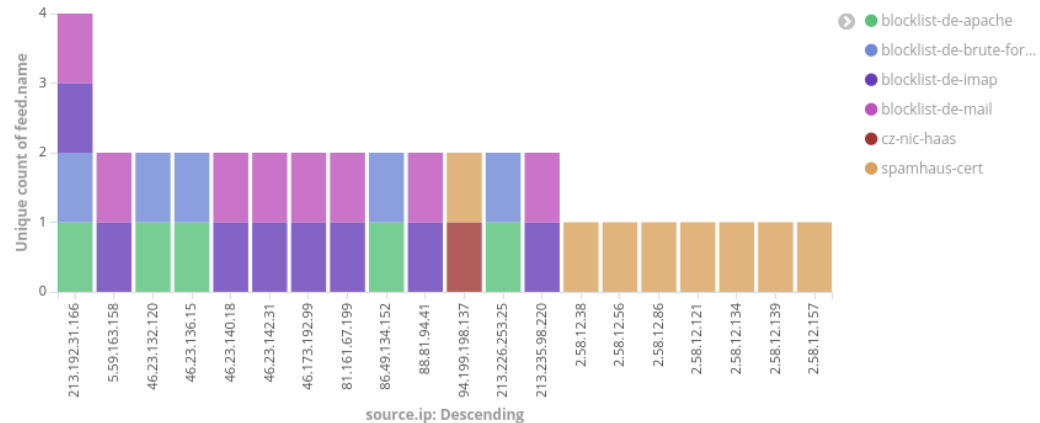
|                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| @timestamp                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| t._id                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| t._index                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| #._score                            | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| t._type                             | event                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| t.classification.taxonomy           | malicious code                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| t.classification.type               | botnet drone                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| t.destination.abuse_contact         | acct-arin@fsi.io                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| t.destination.asn                   | 393667                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| t.destination.geolocation.cc        | US                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| # destination.geolocation.latitude  | 37.751                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| # destination.geolocation.longitude | -97.822                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| destination.ip                      | .252                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| t.destination.network               | .0/24                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| # destination.port                  | 80                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| # extra.source.local_port           | 1,946                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| # feed.accuracy                     | 50                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| t.feed.name                         | spamhaus-cert                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| t.feed.url                          | https://portal.spamhaus.org/cert/api.php?cert=CSIRT.CZ&                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| t.malware.name                      | conficker                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| t.protocol.transport                | tcp                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| t.raw                               | OyBcb3RzIHdpdGhvdmVudHJlbnV0aW9uIG9yIHB1YmxyYWhvbiBVVEMgPSBUAHUGT2N0IDMxIDE3OjAwOjAzIDIwMTkKQ0YBD3B5cm1naHQgwkgMcjAxOSBUAGUgu3BhbwhhdXMGuHJVamVjdCBMdGQuIEFsbcByawddodHMgcmlldGVzdCjsgTM8gcmUtZGlzdHJpYnV0aW9uIG9yIHB1YmxyYWhvbiBVVEMgPScjsgNSATIEJvdCB0YW1lcjsgICBDb21tYW5kICYqQ29udHJvbCAoQyZDKSBpbmZvcmlhdGlvbiwgagWgyXZhaWxhYmxlOgo7IDYGLSBDJKMGrg9tyWLcjsNgNyAtIFJlbW90ZSBJUCAoY29ubmVjdGluZyB0bykkOYA4IC0gUmVtb3RlIFBvcnkKgGNvbm5lY3RpbnmcgdG8pcjsgOSAteXvy2FsiFBvcnkQKOyaAxcMAatIFBYyb3RvY29scjsgICBBZGRpdG1vbmfSIgZpZWxzcyBTXXkygmUgyWRkwQag4gd6hlIGZldHVyzSB3axRob3V0IG5vdGllajZzo7cjsgaXAxiGFzbwiwy291bnRyeSwgbGFzdHNlZW4sIGJvdG5hbWUsIGRvbwFpbicwcmVtb3RIeX2lwLCByZW1vdGVfcG9ydCwgbG9jYXxfcg9ydCwgcHJvdG9jb2wkOwoSMC4xNXzuYmJI0LjiYMCMxBUZUMTAzMAsQiosMTU3MjUnZjY0Mixxb25maWNrZXIsLDENWC4YNduQMtuqmjuYLdgwLEDESNDYSdGnw |
| t.source.abuse_contact              | abuse[REDACTED]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| t.source.asn                        | 5610                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| t.source.geolocation.cc             | CZ                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| t.source.geolocation.city           | dolni bojanovice                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| # source.geolocation.latitude       | 48.85                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| # source.geolocation.longitude      | 17.017                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| source.ip                           | [REDACTED].4.220                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| t.source.network                    | [REDACTED]/13                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| @time.observation                   | October 31st 2019, 18:09:00.000                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| @time.source                        | October 31st 2019, 16:44:02.000                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |



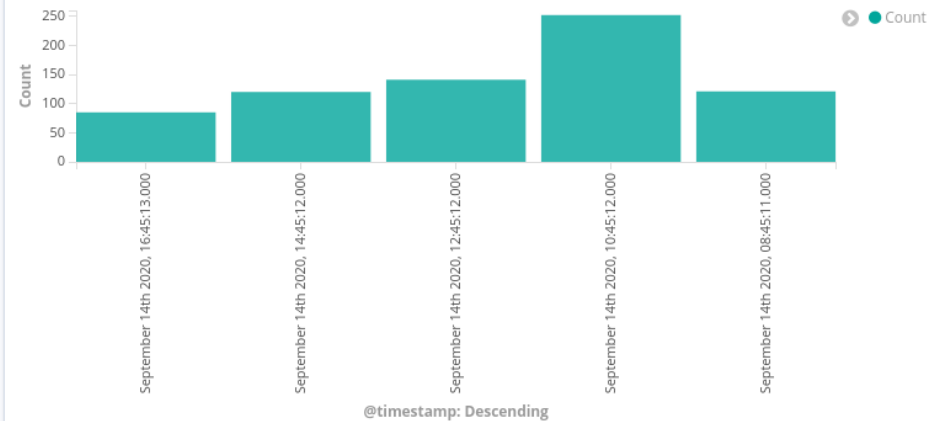
pocyt incidentu cz



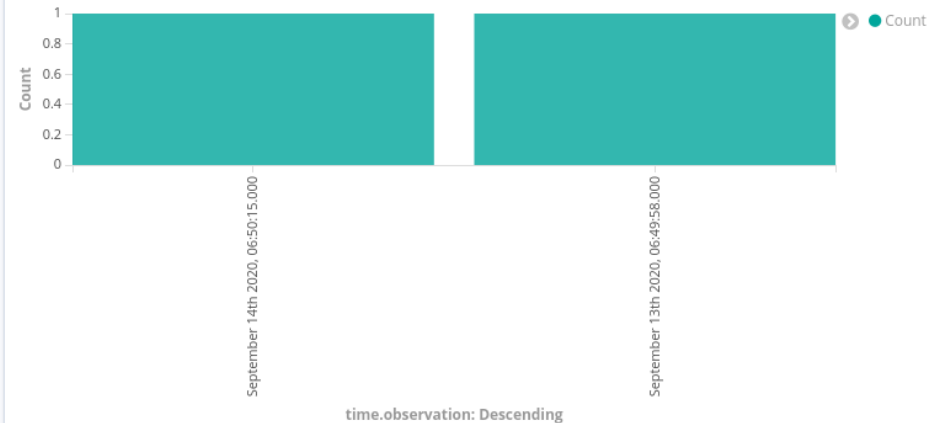
IP+pocet+feed+cz



CZ\_IP\_malware



CZ\_IP\_phishing



# Co se povedlo a co méně?

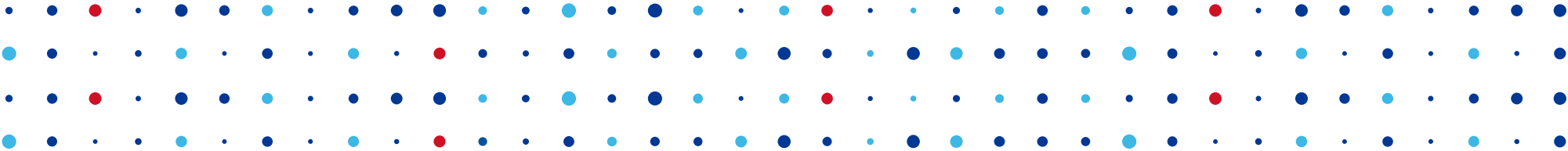
- Co se povedlo
  - Doručení informace o bezpečnostní události či incidentu do koncové sítě (API+mail)
    - Zpětná vazba na základě osobních kontaktů
  - Sdílení informací s dalšími subjekty (Komerční firmy, NÚKIB...)
  - Vyhledávání zvlášt' zranitelných zařízení
- Co se povedlo méně
  - Na výsledky analytických výstupů nedostáváme obvykle žádnou reakci, kompromitovaný stroj je opraven, ale ani přes žádost nedostaneme data k další analýze



# Další vývoj

- Pravidelné revize zdrojů dat
- Využití výstupů projektu v dalších projektech sdružení
- Změnit způsob ukládání dat (lepší zobrazení historických stavů IP adresy)
- Automatizovat porovnávání dat z projektu Shodan vůči datům z dalších zdrojů
- Změnit postup zpracování dat (nevytvářet duplicitní data k odeslání a uložení do databáze)





# Děkuji za pozornost

Pavel Bašta • [pavel.basta@nic.cz](mailto:pavel.basta@nic.cz)