Praktické výsledky a využití projektu PROKI v CSIRT.CZ

Pavel Bašta • pavel.basta@nic.cz • 16. 9. 2020

CZ.NIC | SPRÁVCE DOMÉNY CZ

CSIRT.CZ

- Národní CSIRT České republiky
- Provozován sdružením CZ.NIC od 1.1 2011
- Řešení incidentů
  - Nejen subjekty dle zákona, ale v těchto případech i ostatní
    - bezpečnostní incident přetrvává (nebyl odstraněn v přijatelném časovém intervalu)
    - na hlášení bezpečnostního incidentu nikdo nereaguje (je jedno jestli se jedná o kontakt v ČR nebo mimo ČR)
    - na hlášení bezpečnostního incidentu jste obdrželi zamítavou odpověď (adresát se odmítá problémem zabývat, danou situaci za problém nepovažuje a podobně)
    - nedokážete dohledat, kdo je za síť/IP adresu (obecně zdroj útoku) zodpovědný nebo se kontaktní informace ukážou jako neaktuální
    - jste přesvědčeni o tom, že problém by se mohl týkat více sítí, které by bylo záhodno zkontaktovat a vyrozumět

Další činnost CSIRT.CZ

- Vzdělávání
  - Školení, prezentace na konferencích, Postřehy z bezpečnosti, Aktuálně z bezpečnosti, publikování v časopisech, komentování v médiích
- Podpora komunity
  - Pracovní skupina CSIRT.CZ, školení pro začínající CSIRTy, školení ENISA, podpora zájemců o členství v mezinárodních organizacích TF-CSRT a FIRST
- Prevence
  - Malicious Domain Manager, Skener webu, Penetrační testování, Zátěžové testy, Honeypoty, jednorázové akce, PROKI

Druhy incidentů (otevřené a zavřené)

	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	sum
Sensor Network*				491	3924	2121	2380	3771	9944	13858	18435	14911	11570	81405
Phishing	65	220	209	144	159	175	368	367	363	409	518	483	574	4054
Spam	47	28	103	26	43	73	159	108	289	121	144	128	164	1433
Malware	53	134	121	10	20	45	117	240	104	99	135	85	84	1247
Other	1	5	13	62	14	75	102	264	182	200	58	85	76	1137
Probe		3	14	25	12	26	86	42	13	26	171	141	45	604
Trojan	66	6	26	5	5	12	56	90	79	94				439
DOS	2	4	2	2	68	72	32	37	12	14	7	16	13	281
Botnet		3	46	5	8	15		4	71	29	20	4	1	206
Virus		84	99											183
Portscan	10	4	1	6	1	3	2	5	6	13	16	3	19	89
Pharming							18	3	2	3	10	9	2	47
Outside_remit													2	2
sum	244	491	634	285	330	496	940	1160	1121	1008	1079	954	980	9722

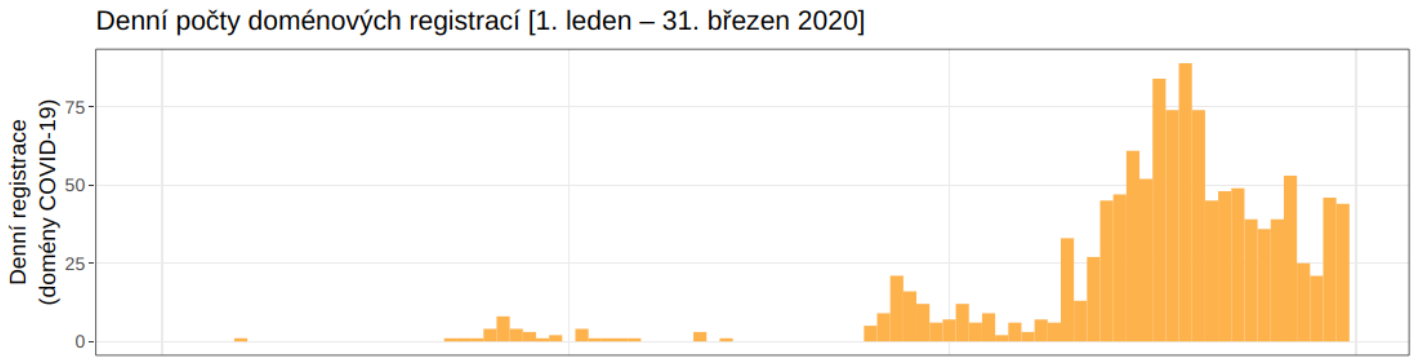
*** Sensor Network není započten do celkového počtu**

Proč je důležité míti komunitu?

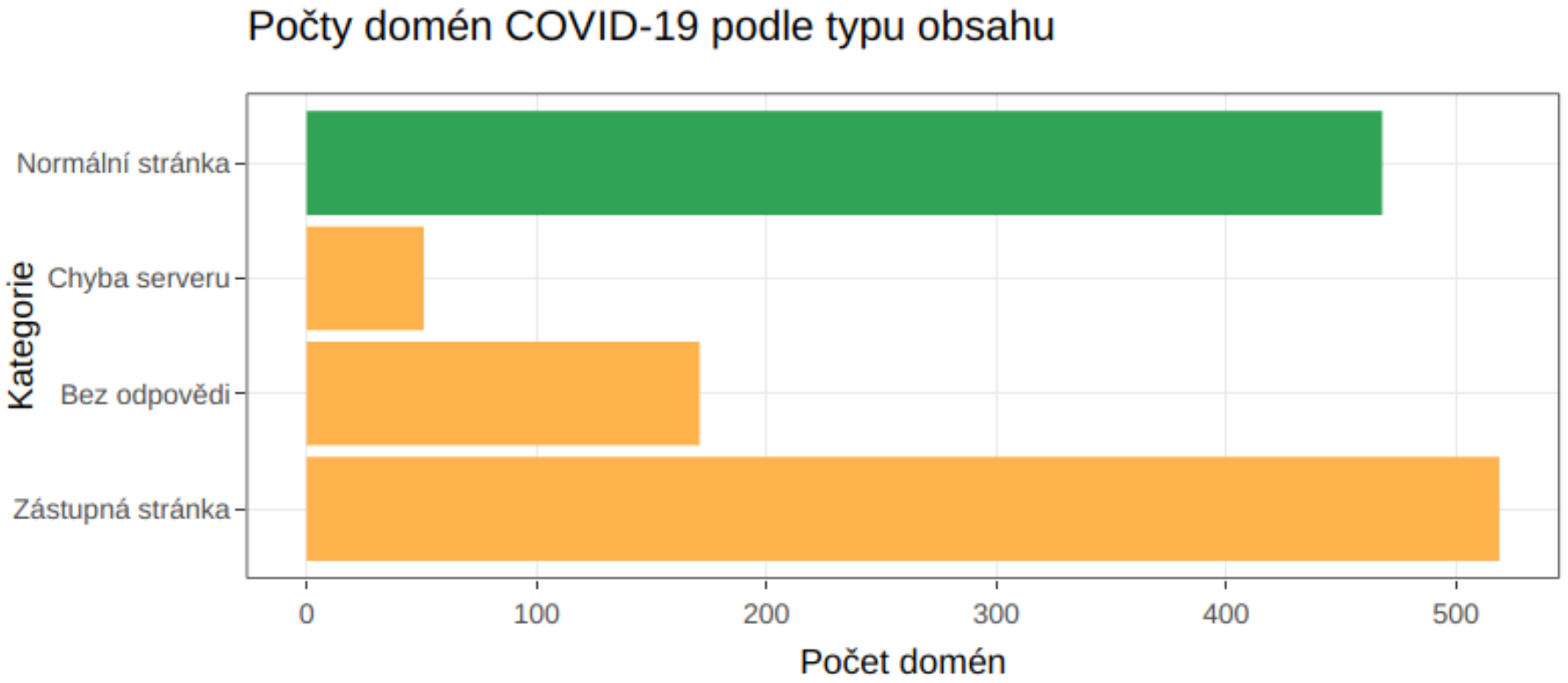
- Spolupráce s NCOZ a projektem FENIX
  - Rozsáhlé skenování ve stejné době jako útoky na nemocnice
  - Zaznamenána i komunikace opačným směrem (skenující IP použita i jako C&C server)
  - Společně s NCOZ jsme požádali o pomoc členy projektu FENIX
  - Hledali se stroje komunikující s danou IP, zároveň sítě zablokovali další pokusy o skenování
  - Analýza technických detailů útoku a hledání dalších zainteresovaných IP adres

Analýza domén .CZ

- Domény registrované po 1.lednu
- Domény obsahující: corona, korona, virus, rousk, respirator, epidem, dezinfekc, karanten, covid, pandem, ffp2, ffp3
- První doména 23. ledna 2020 „koronavirus.cz“



Zdroj: https://adam.pages.nic.cz/reports/adam/covid19-cz/



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 množšví 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 Elastisearch
  - 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

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 funkcionalita, umožňující zasílat tyto informace přímo Národnímu úřadu pro kybernetickou a informační bezpečnost

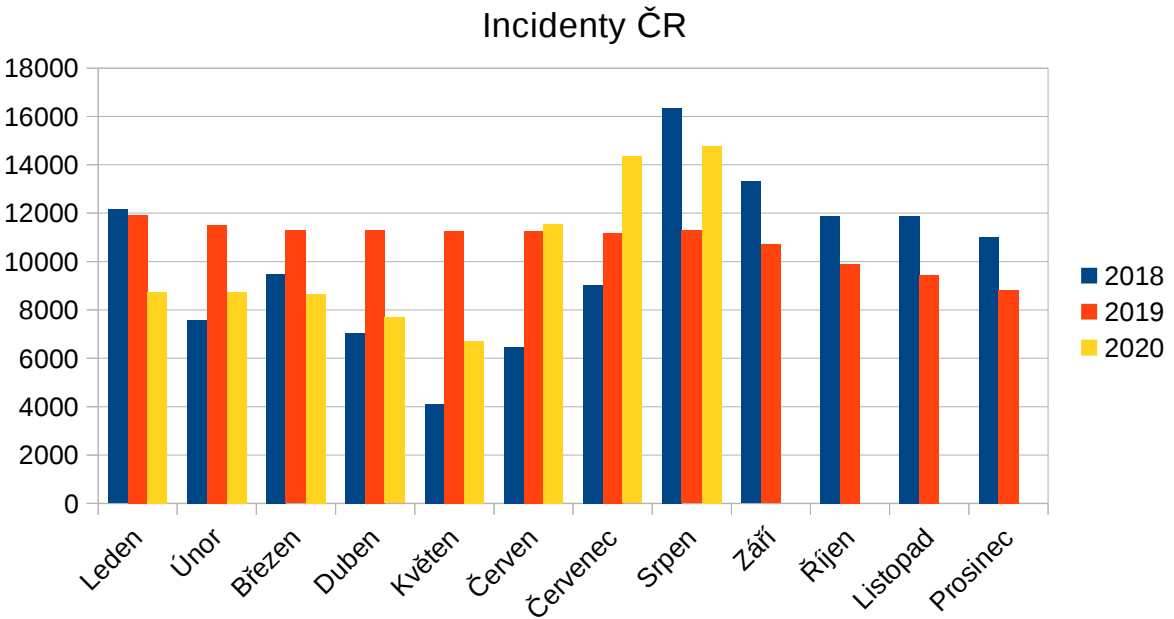
Výstupy projektu PROKI

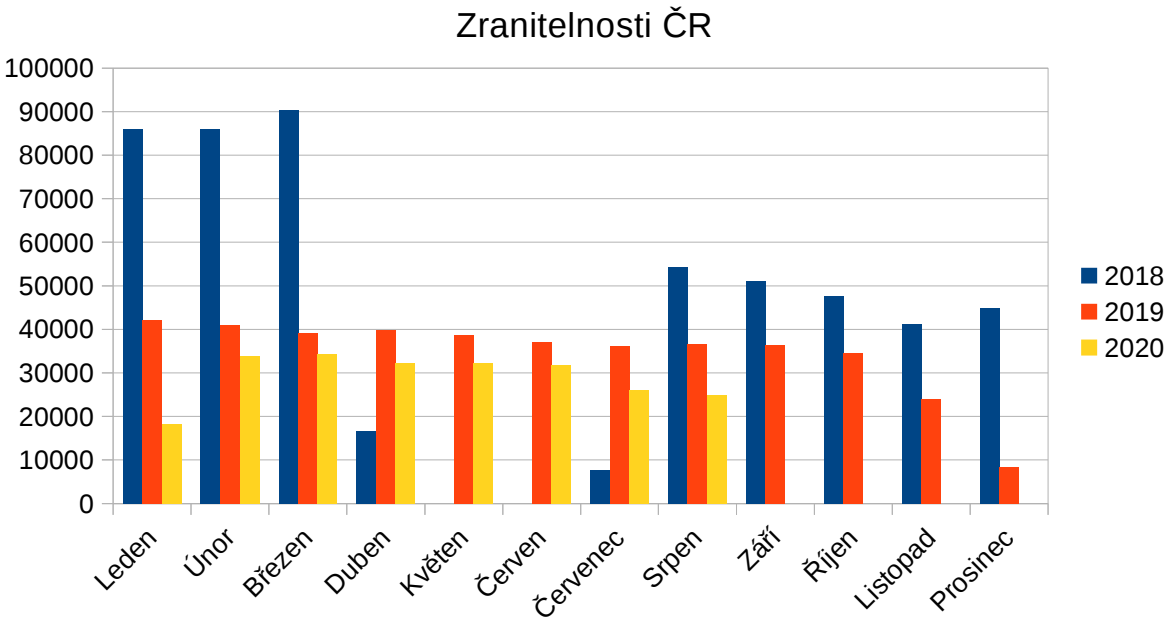
- Reportování zranitelností
  - Zahrnuty na základě počátečních analýz
  - Důležitý preventivní prvek
  - Otevřené SMTP relay, otevřená nechráněná sdílení dat, otevřené nechráněné služby typu TFTP, Telnet, SNMP nebo otevřené DNS resolvery

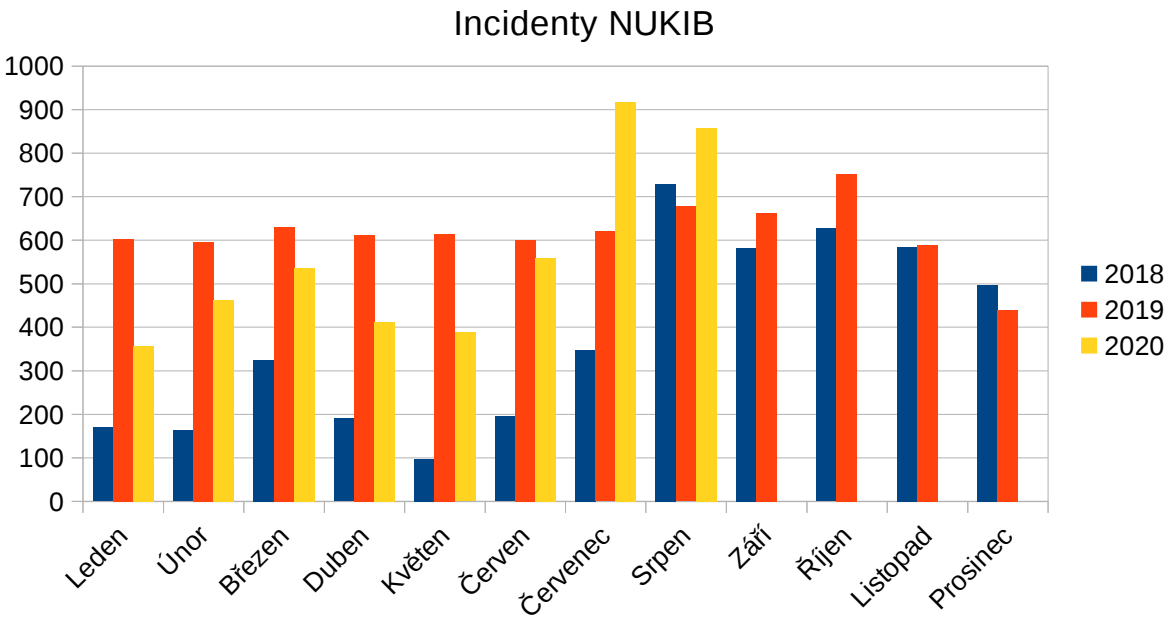
Table | JSON

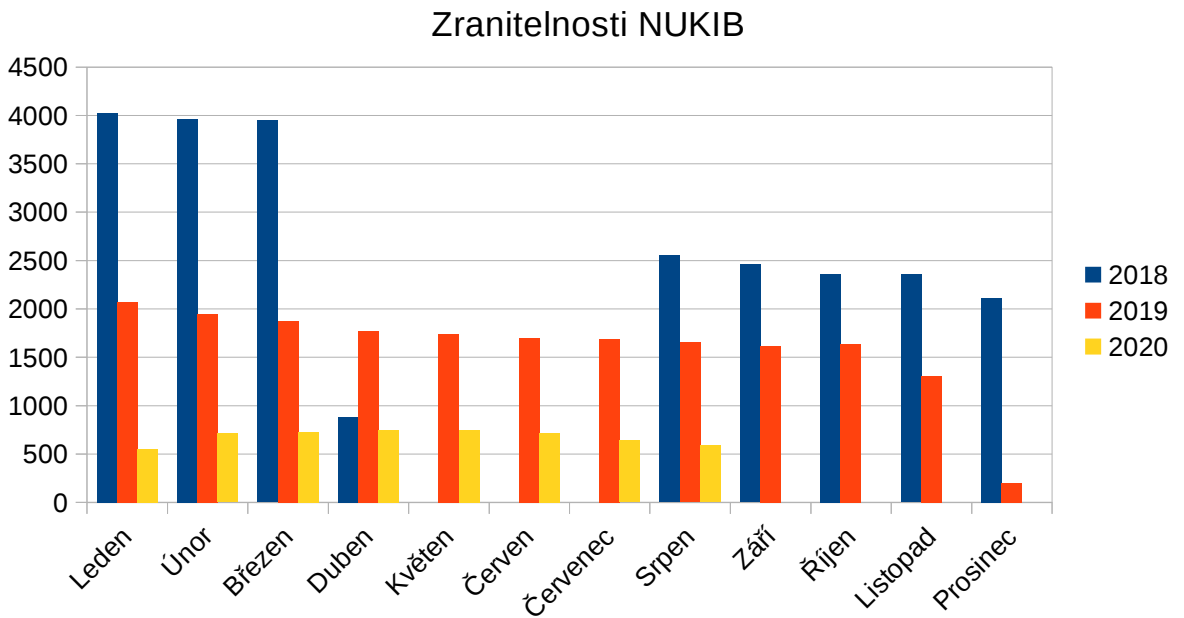
View surrounding documents | View single document

🕒	@timestamp	February 8th 2020, 09:23:09.000
t	_id	74nlI3ABPLNlXAWfkmO6
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


Incidenty ČR
18000
16000
14000
12000
10000
8000
6000
4000
2000
0
Leden
Únor
Březen
Duben
Květen
Červen
Červenec
Srpen
Září
Říjen
Listopad
Prosinec
2018
2019
2020

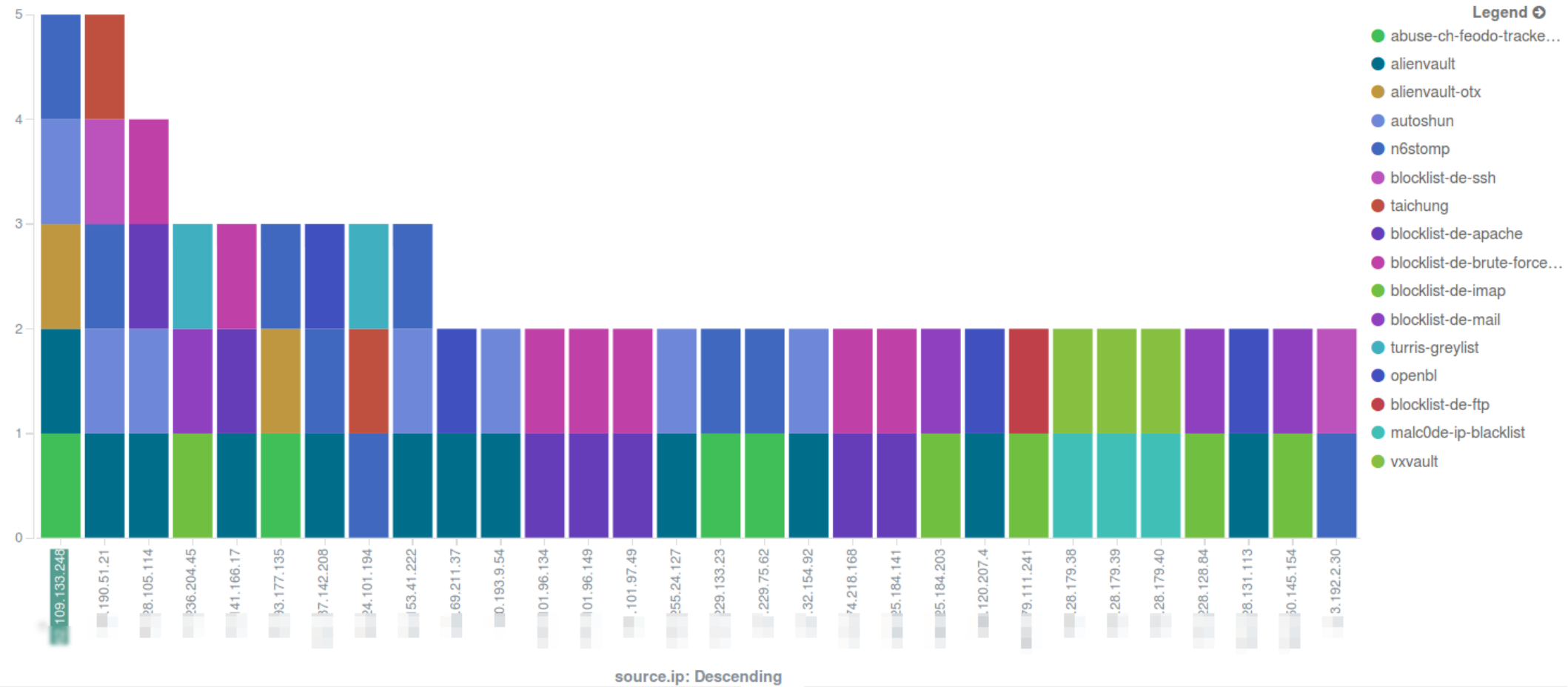

Zranitelnosti ČR
100000
90000
80000
70000
60000
50000
40000
30000
20000
10000
0
Leden
Únor
Březen
Duben
Květen
Červen
Červenec
Srpen
Září
Říjen
Listopad
Prosinec
2018
2019
2020


Incidenty NUKIB
1000
900
800
700
600
500
400
300
200
100
0
Leden
Únor
Březen
Duben
Květen
Červen
Červenec
Srpen
Září
Říjen
Listopad
Prosinec
2018
2019
2020



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



virustotal

.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	mojeglo
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 zvlášť zranitelná zařízení
  - 2019 – data z projektu Shodan
  - IP kamery, Routery, SCADA

Table | JSON

View surrounding documents | View single document

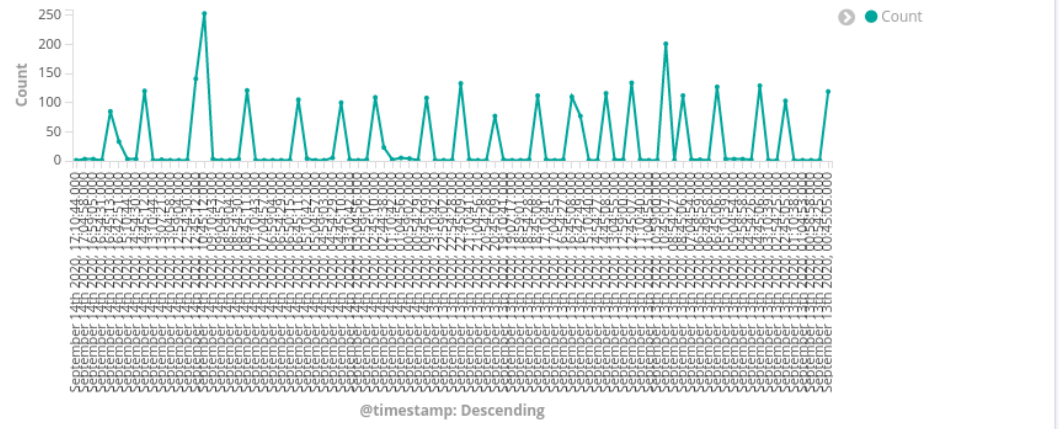
@timestamp	September 2nd 2019, 01:08:59.000
_id	b-QW72wB_HSdMyDs0iGg
_index	intelmq-2019.09
_score	-
_type	event
classification.identifier	pop
classification.taxonomy	intrusion attempts
classification.type	brute-force
destination.port	110
extra.source.local_port	46,485
feed.accuracy	50
feed.name	spamhaus-cert
feed.url	https://portal.spamhaus.org/cert/api.php?cert=CSIRT.CZ&
protocol.application	pop
protocol.transport	tcp
raw	OyBCb3RzIHdpdGhvdXQgdGltZSBmaWx0ZXIsIHByZXBhcmVkIGZvciBDU0lSVC5DWiBvbiBVVEMgPSBTdW4gU2VwICAxIDIzOjAwOjA0IDIwMTkKOyBDb3B5cmlnaHQgwqkgMjAxOSBUaGUgU3BhbWhhdXMgUHJvamVjdCBMdGQuIEFsbCByaWdodHMgcmVzZXJ2ZWQuCjsgTm8gcmUtZGlzdHJpYnV0aW9uIG9yIHB1YmxpYyBhY2Nlc3MgYWxsb3dlZCB3aXRob3V0IFNwYW1oYXVzIHBlcm1pc3Npb24uCjsgRmllbGRzIGRlc2NyaXB0aW9uOgo7CjsgMSAtIEluZmVjdGVkIElQCjsgMiAtIEFTTgo7IDMgLSBDb3VudHJ5IENvZGUKOyA0IC0gTGFzdHNlZW4gVGltZXN0YW1wIChpbiBVVEMpCjsgNSAtIEJvdCBOYW1lCjsgICBDb21tYW5kICYgQ29udHJvbCAoQyZDKSBpbmZvcm1hdGlvbiwgaWYgYXZhaWxhYmxlOgo7IDYgLSBDJkMgRG9tYWluCjsgNyAtIFJlbW90ZSBJUCAoY29ubmVjdGluZyB0bykKOyA4IC0gUmVtb3RlIFBvcnQgKGNvbm5lY3RpbmcgdG8pCjsgOSAtIExvY2FsIFBvcnQKOyAxMCAtIFByb3RvY29sCjsgICBBZGRpdGlvbmFsIGZpZWxkcyBtYXkgbWUgYWRkZWQgaW4gdGhlIGZ1dHVyZSB3aXRob3V0IG5vdGljZQo7CjsgaXAsIGFzbiwgY291bnRyeSwgbGFzdHNlZW4sIGJvdG5hbWUsIGRvbWFpbiwgcmVtb3RlX2lwLCByZW1vdGVfcG9ydCwgbG9jYWxfcG9ydCwgcHJvdG9jb2wKOwo4OS4yMDMuMTM3LjMxLEFTMjU1MTIsQ1osMTU2NzM3NDY1Nixwb3AsLSwtLDExMCw0NjQ4NSx0Y3A=
source.abuse_contact	abuse@c[illegible]
source.asn	25512
source.geolocation.cc	CZ
source.geolocation.city	uvaly
source.geolocation.latitude	48.733
source.geolocation.longitude	16.683
source.ip	[illegible].137.31
source.network	[illegible].128.0/17
time.observation	September 2nd 2019, 01:08:59.000
time.source	September 1st 2019, 23:50:56.000

Table | JSON

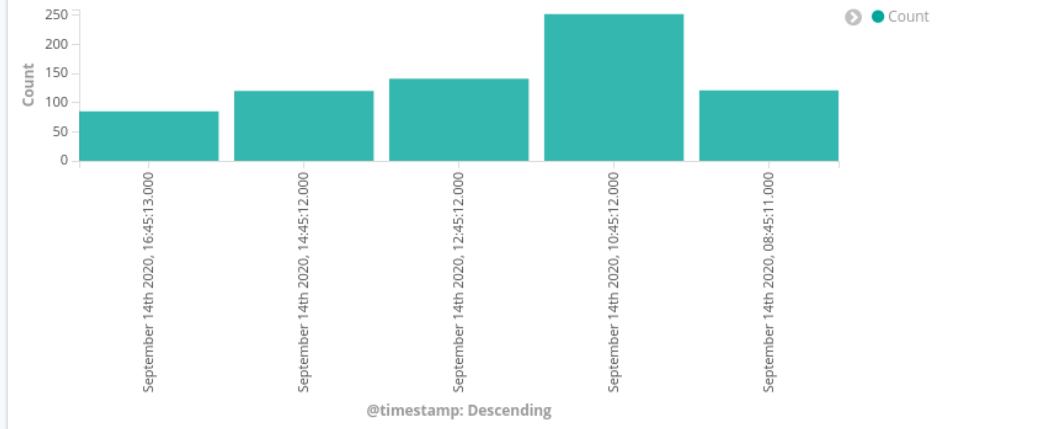
View surrounding documents | View single document

@timestamp	October 31st 2019, 18:09:00.000
t	_id	bebKIm4BCaCSVoENyBqU
t	_index	intelmq-2019.10
#	_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	[redacted].252
t	destination.network	[redacted].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	OyBCb3RzIHdpdGhvdXQgdGltZSBmaWx0ZXIsIHByZXBhcmVkIGZvciBDU0lSVC5DWiBvbiBVVEMgPSBUaHUgT2N0IDMxIDE3OjAwOjAzIDIwMTkKOyBDb3B5cmlnaHQgwqkgMjAxOSBUaGUgU3BhbWhhdXMgUHJvamVjdCBMdGQuIEFsbCBy aWdodHMgcmVzZXJ2ZWQuCjsgTm8gcmUtZGlzdHJpYnV0aW9uIG9yIHB1YmxpYyBhY2Nlc3MgYWxsb3dlZCB3aXRob3V0IFNwYW1oYXVzIHBiciBVVEMpCjsgNSAtIEJvdCBOYW1lCjsgICBDb21tYW5kICYgQ29udHJvbCAoQyZDKSBpbmZvcm1hdGlvbiggaWYgYXZhaWxhYmxlOgo7IDYg LSBDJkMgRG9tYWluCjsgNyAtIFJlbW90ZSBJUCAoY29ubmVjdGluZyB0bykKOyA4IC0gUmVtb3RlIFBvcnQgKGNvbm5lY3RpbmcgG8pCjsgOSAtIExvY2FsIFBvcnQKOyAxMCAtIFByb3RvY29sCjsgICBBBZGRpdGlvbmFsIGZpZWxkcyBt YXkgYmUgYWRkZWQgaW4gdGhlIGZ1dHVyZSB3aXRob3V0IG5vdGljZQo7CjsgaXAsIGFzbiwgY291bnRyeSwgbGFzdHNlZW4sIGJvdG5hbWUsIGRvbWFpbiwgcmVtb3RlX2lwLCByZW1vdGVfcG9ydCwgb3jYWxfcG9ydCwgcHJvdG9jb2wK Owo5MC4xNzYuMjI0LjIyMCxBUzU2MTAsQ1osMTU3MjUzNjY0Mixjb25maWNrZXIsLDEwNC4yNDQuMTQuMjUyLDgwLDE5NDYsdGNw
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]0/13
time.observation	October 31st 2019, 18:09:00.000
time.source	October 31st 2019, 16:44:02.000

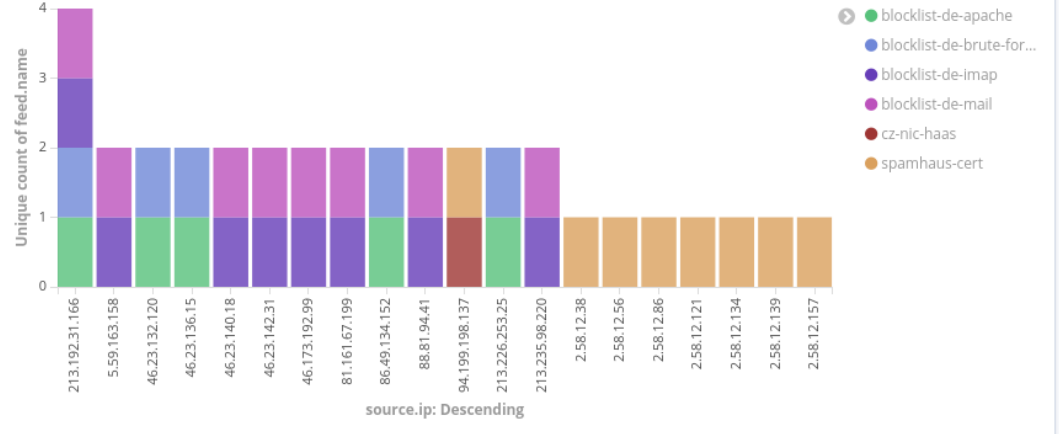
pocty incidentu cz



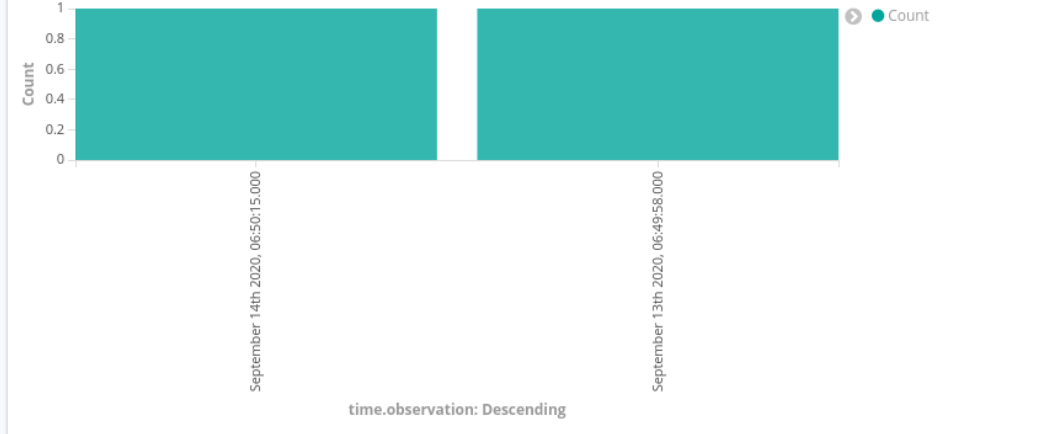
CZ_IP_malware



IP+pocet+feed+cz



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 zvlášť 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