

# CZ.NIC and CSIRT.CZ

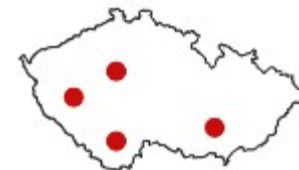
## CZ.NIC

- National Domain Name Registry
- 
- As a national registry and not-for-profit organization, CZ.NIC invests its money back into the internet community and develops projects that aim to improve security throughout the internet.



## CSIRT.CZ

- Operated by CZ.NIC association by 2011
- CSIRT.CZ historically started in 2008 at academic association called CESNET as a research grant
- Basic rights of CSIRT.CZ are established by the Act on Cyber Security no. 181/2014 (ACS), section 17
- Most of it's rights and duties are defined in public contract with National Information and Cyber Security Authority (NÚKIB) previously in agenda of National Security Office



## CSIRT.CZ

### Activities according to the Act on Cyber Security

- Ensures the sharing of information on the national and international level in the field of cyber security
- Receives notification about contact details from entities which are given by law:
  - Electronic communication service providers, Entity operating an electronic communication network (unless they are critical infrastructure)
    - e.g. ISP, Universities
  - A public authority or legal or natural person administering an important network
    - e.g. Providers of IS
  - Digital service provider
    - e.g. Web Browser Provider, Cloud Service or Online Market Place Provider

## CSIRT.CZ

- Receives cybersecurity incidents reports from stated entities, keeps a record of these incidents and stores and protects them
- Evaluates these incidents
- Provide methodical support, help and cooperation when a cyber security incident occurs
- Acts as a point of contact
- Carries out vulnerability analyses in the cyber security field
- Transfers to the NÚKIB data on cyber security incidents reported by stated entities, without disclosing the reportee

## Reporting to CSIRT.CZ

### CSIRT.CZ operates as the last resort team

Reports we mostly deal with:

- Lasting incidents
- Incidents who nobody reacts to
- Constituent of the incident refused to respond or deal with the incident
- If the incident could affect a wide range of objects



## CSIRT.CZ

- Addressing security incidents and its coordination
- Education and tutoring
- Proactive services in the area of security
- Support cooperation within national and international community



## Incident Handling

### Tools we use

- OTRS (typical ticket system)
- Supportive sources:
  - Passive DNS (AUT)
  - , shodan, virustotal, PROKI, Honeypots, Turris
- whois, wget...





## OTRS

## Important features

- Automatic text analysis
  - Identification of the type of the incident
  - IP address
  - NETNAME
  - Abuse contact
- Tools for mass distribution of information (954 reports recieved = 13 540 alerts sent)



## Communication of the incident via OTRS

- According to the information found, the incident is being send to abuse contact of the IP adress connected to the incident (whois)
- If escalation needed recepients are expanded – domain holder – contacts from the website
- The announcer is always informed of the result



# Incident handling statistics

**TLP: CLEAR**

Reference period: April 1, 2008 – March 28, 2023

Number of incidents by type (open and closed cases)

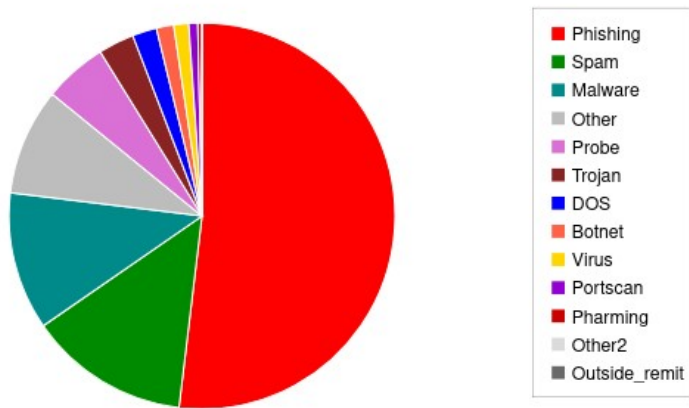
	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	sum
Sensor Network*				491	3924	2121	2380	3771	9944	13858	18435	14911	16217	10284	8815	1320	106471
Phishing	65	220	209	144	159	175	368	367	363	409	518	483	738	1277	1485	610	7590
Spam	47	28	103	26	43	73	159	108	289	121	144	128	216	163	220	101	1969
Malware	53	134	121	10	20	45	117	240	104	99	135	85	109	141	224	51	1688
Other	1	5	13	62	14	75	102	264	182	200	58	85	86	58	63	41	1309
Probe		3	14	25	12	26	86	42	13	26	171	141	68	67	69	12	775
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	16	11		3	298
Botnet		3	46	5	8	15		4	71	29	20	4	2	1	4		212
Virus		84	99														183
Portscan	10	4	1	6	1	3	2	5	6	13	16	3	29	7	2	1	109
Pharming							18	3	2	3	10	9	3			1	49
Other2																1	1
Outside_remit																1	1
sum	244	491	634	285	330	496	940	1160	1121	1008	1079	954	1267	1725	2067	822	14623

\* Sensor Network is not counted to the overall sum

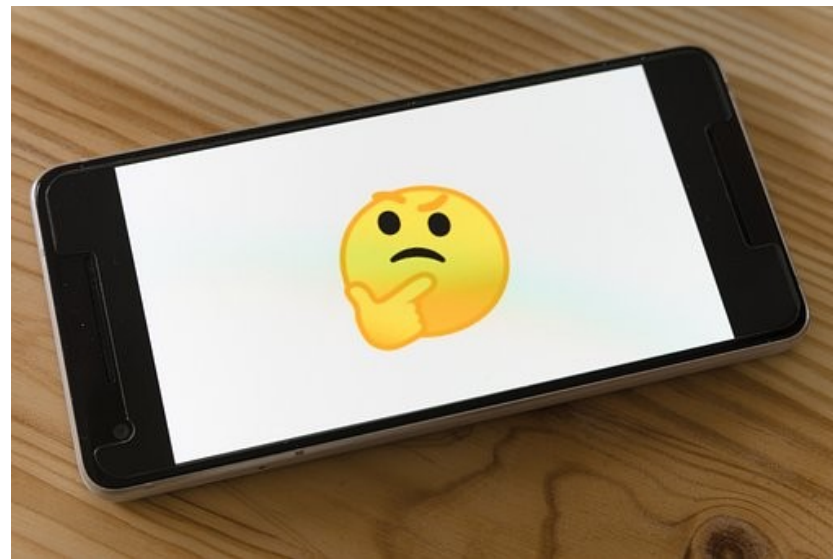
More information about the types of the incidents can be found [here](#).

## Incident Statistics

Total number of incidents during the reporting period (open and closed cases)



- Enormous increase of Phishing incidents after the pandemic started



## Precaution against Incidents

- PROKI
- Honeypots
- Web Scanner
- Stress (D)DoS Tests
- Pentests



## PROKI

- Helps to automatically process information about security incidents and report them to relevant constituents
- The National Security Team receives information from various sources about IP addresses on blacklists, IP addresses that spread malware, IP addresses connecting to C&C servers and it is necessary to distribute them effectively.
- Target groups:
  - ISPs
  - Czech organizations that are members of the RIPE NCC (LIR - Local Internet Registry)

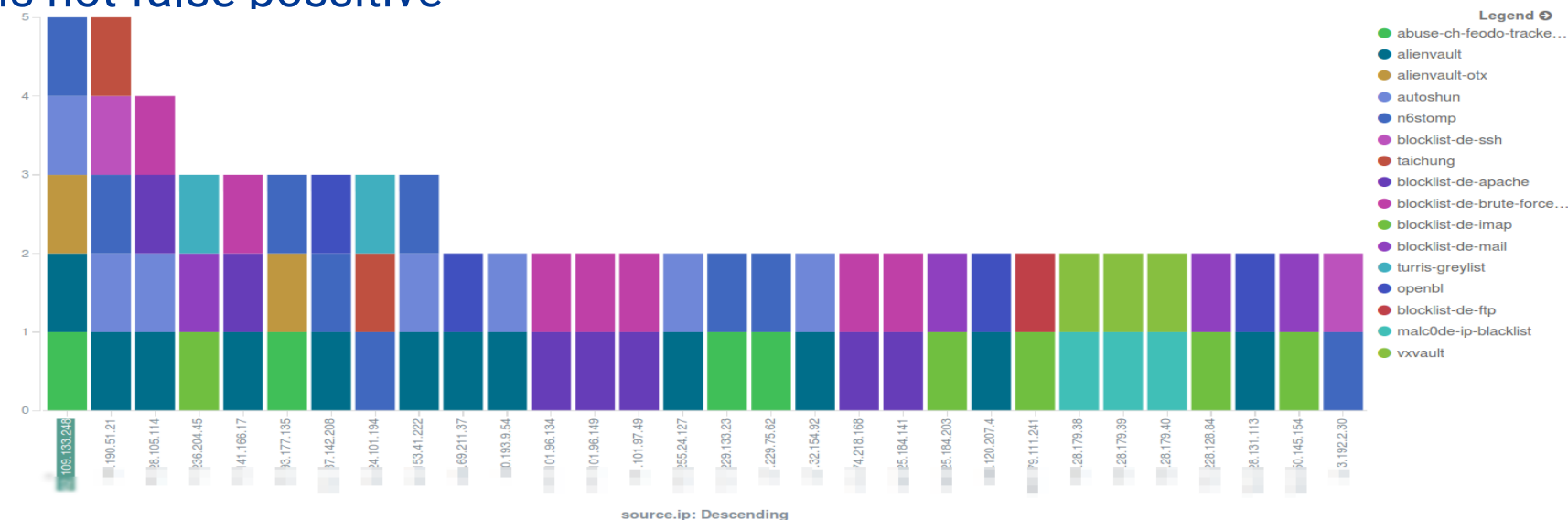
## PROKI

- Security events from more than 28 sources
  - All formes – public, private and our own - Turris HaaS and Sentinel
    - IntelMQ, Public blacklists of IP with detected harmful activity, other soruces provided by community,
      - <https://csirt.cz/cs/zdroje-dat/>
- On average 115 000 events from Czech Networks daily
- From 2021 enriched of data from Shodan for CZ
  - This is being used to compare known infected IP adresse's with specific devices
    -
- 2022 - 4 940 898 registered events of 47 720 unique IP adresses it generated 28 563 reports to 706 unique abuse contacts

## PROKI

Better understanding of already known incidents – Identification of yet unrevealed problems

Identification of problematic IP addresses – the more IPs the more we are sure it is not false positive





## Content of the Report from PROKI

- time\_detected – the time when the incident was detected by the source system
- ip - the IP address displaying the behavior described
- class – an incident class
  - i.e. Malicious Code, Intrusion Attempts, Information Gather
- type - an incident type (one class may contain several types)
  - i.e. botnet drone, scanner, malware
- time\_delivered - the time when the incident was recorded by the PROKI system
- country\_code – country code
- asn - autonomous system number
- description - an additional description of the incident, if available
- malware - malware family or name, if available
  - i.e. Trojan.Backdoor, Office.Word.Downloader
- feed\_name - source feed name; their list is stated bellow
- feed\_url – source feed URL
- the original record from the source feed

## Turris

- Some of investments went also into the project Turris which started as a research project and currently has the third version of the original Turris Omnia model, named Turris MOX



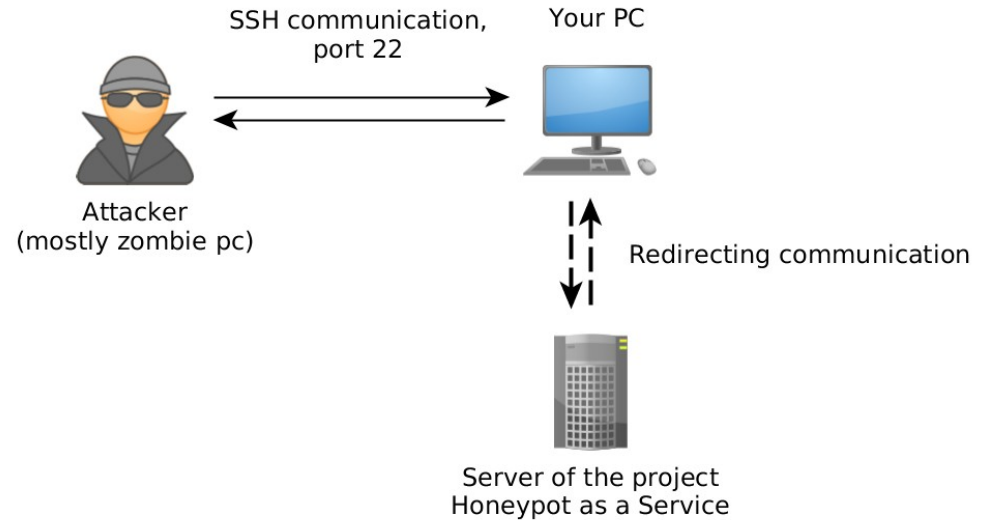
## TURRIS



- Programmable OS router with the main focus on security of home networks and small offices
- If the user gives us a permission we use the data (root account for every user and OS)
- The name of the Turris project is based on a Latin word for **tower**, representing an alert tower often used to warn of approaching danger
- Uniquely, the **first version** of Turris Omnia **remains up to date**, despite being **9 years old**

# Turris HaaS

- Honeypot as a service
- Within this project, there are more than 4,000 routers with honeypots across Czechia
- Once it is discovered that a specific attack has occurred on any of the routers, alerts are sent to our team. They analyze the attack and, if necessary, send a security update to all the routers



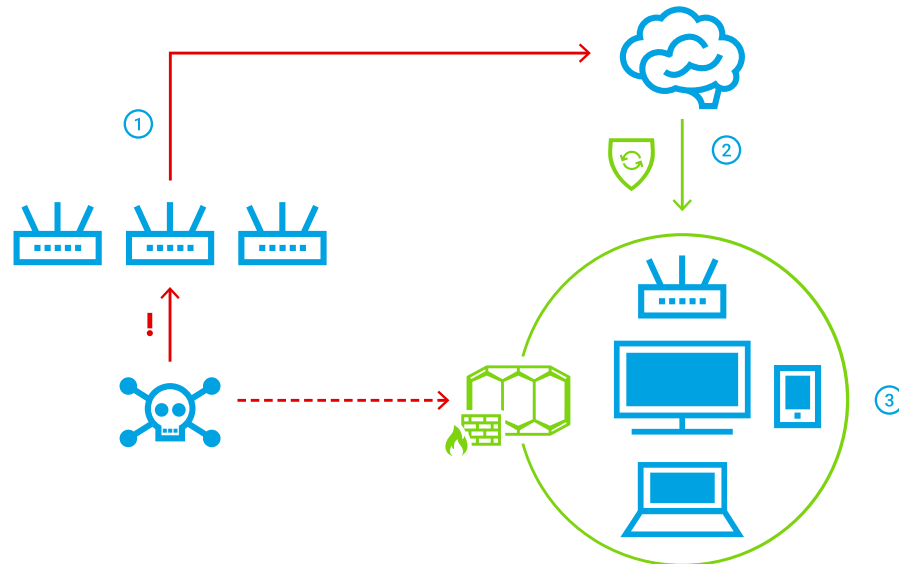
## HaaS

In one year 250 102 unique combinations of login details were captured and 1230 malware samples analyzed

- Most common login combinations:
- 1. root root 4988327x
- 2. pi raspberry 1256419x (implicit password Raspbian)
- 3. pi raspberryraspberryy993311 1016219x (search for Backdoor SH.PIMINE.AA malware infected devices)
- 4. admin 816406x
- 5. root admin 410065x
- 6. ubnt ubnt 391758x

## Turris Sentinel

- Threat detection and cyberattack prevention system
- Part of Turris OS
- Data collection
  - Minipots
  - Firewall logs
    - OPTIONAL
- HaaS as an external resource








## Turris Sentinel

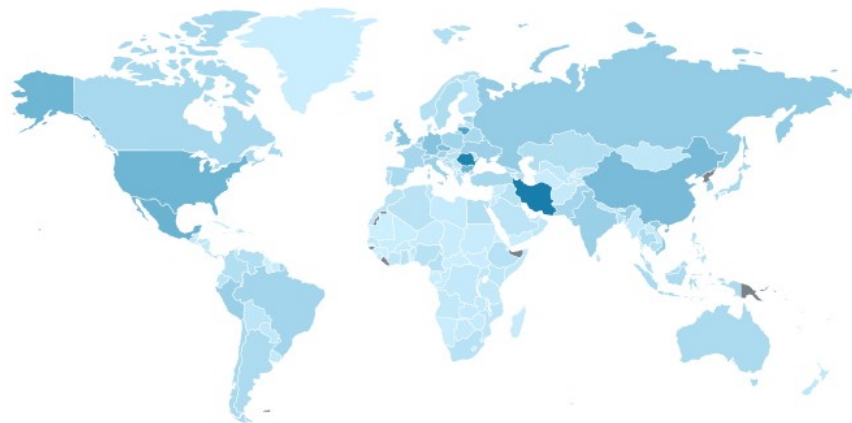
- Data processing
  - Real-time stream of events
  - Data pipelines
  - Malicious IP addresses detection
  - IP address score
  - Score threshold

[www.view.sentinel.turris.cz](http://www.view.sentinel.turris.cz)

### Top countries by recorded incidents

1.		IR	1072165
2.		RO	924537
3.		US	57531
4.		MX	30884
5.		CN	24366
6.		KW	22554
7.		HK	21062
8.		CZ	18503
9.		IT	13291
10.		VN	7765
11.		RU	6372
12.		PE	5661
13.		GB	4988
14.		CL	3890
15.		UA	3881

## Overview



Hour

12 Hours

Day

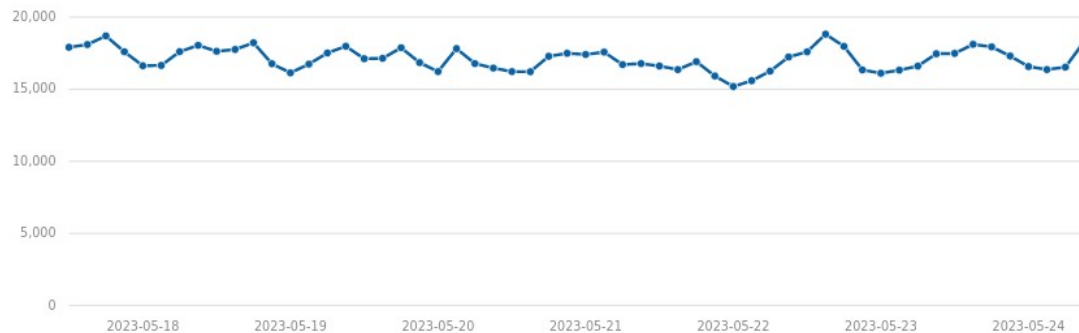
Week

Month

3 Months

Year

Number of unique attackers during the time





Most abused passwords

1.	123456	17234615
2.	1234	16566947
3.	123456789	16125017
4.	12345	12756812
5.	1QAZ2wxx	2510207
6.	P@ssw0rd	1239915
7.	password	814462
8.	12345678	722862
9.	123	676016
10.	abc123	442035
11.	P@\$Sw0rd123	439636
12.	123123	437381
13.	1qaz@WSX	428484
14.	1	423737
15.	Aa123456	417752

Password Details

Threat Detection / Passwords / Password Details

123456

Hour

12 Hours

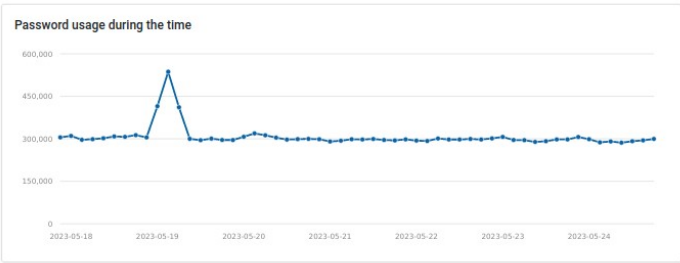
Day

Week

Month

3 Months

Year



Password's top usernames

1.	admin	56880
2.	root	42316
3.	test	20028
4.	webmaster	14543
5.	postmaster	13685
6.	user	11899
7.	sales	11751
8.	info	11227
9.	guest	10713
10.	backup	10359
11.	mail	10107
12.	admin1	9581
13.	contact	9476
14.	test1	8857
15.	scan	8249
16.	support	8188
17.	fax	8065
18.	administrator	7837
--		----

# Sentinel Password Checker

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

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

Your password has been used **509 701 785** times with service(s):

**telnet** **smtp** **ftp** **http**

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

## Check password



Check

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

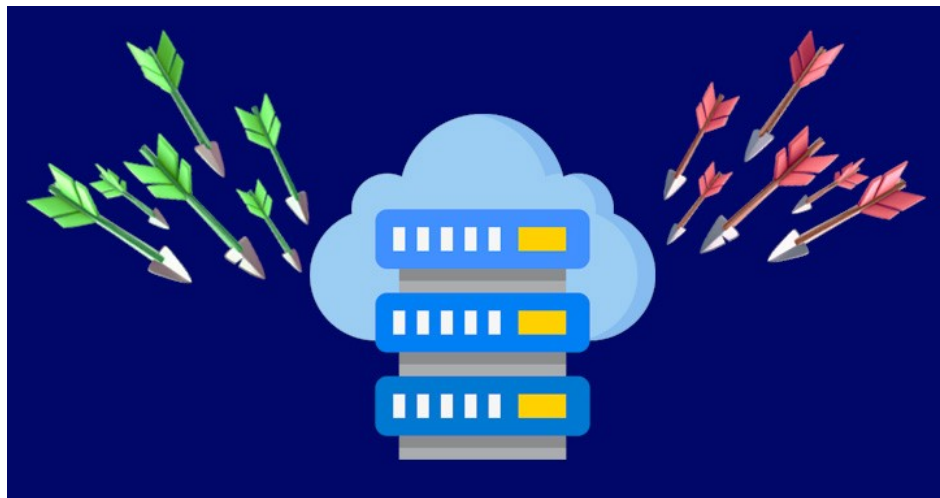
## Other services provided by CSIRT.CZ

### Web Scanner

- Helps mainly to public institutions and non profit organizations
- Vulnerability scanner with automatic tools followed by the manual test
- Detailed report for the website operator
- In 2022 we tested 26 domains based on 18 orders
- 9 of these tests were done to important information systems (according to The Act on Cybersecurity)
- 11 websites as part of penetration testing

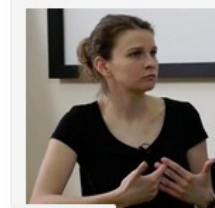
## Stress (D)DoS Tests

- Ordered DDoS
- Different types of attacks (SYN flood, UDP flood, ICMP flood, slowloris)
- Price 0,50 EUR



## Education and Awareness Raising

- Conferences and Working Groups (organization and active participation)
- Trainings e.g. Security and privacy on the Internet
- Specialized tailored-made trainings for Teachers, Police Officers, Students, State Office for Nuclear Safety, Czech National Bank...)
- Awareness raising throughout wide range of publication activities (web portals, our own websites, printed magazines...)
- Cooperation on educational series for National TV
- Translation and publication of materials (OWASP TOP10, Master your Space)



Privacy policy



Kafemlejnek.TV

20 - Cyber Security Incident Response Team

SOUNDCLOUD



Share



1.4K

### Postřehy z bezpečnosti: BlackLotus je UEFI bootkit obcházející Secure Boot



V dnešním ohlédnutí za uplynulým týdnem se podíváme na výsledky analýzy malwaru BlackLotus, zranitelnosti IP telefonů a platformy Booking.com, na nesmrtelný Internet Explorer a...

CSIRT.CZ | 6. 3. 2023 | 19 Doba čtení: 4 minuty



What happens to one of us should only happen to one of use.

Thank you for your attention.