CZ.NIC and CSIRT.CZ
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
CSIJT.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 administrating 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
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
• 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...
Important features

- Authomatic text analysis
  - Identification of the type of the incident
  - IP address
  - NETNAME
  - Abuse contact

- Tools for mass distribution of information (954 reports received = 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

**Reference period:** April 1, 2008 — March 28, 2023

### Number of incidents by type (open and closed cases)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishing</td>
<td>65</td>
<td>220</td>
<td>209</td>
<td>144</td>
<td>159</td>
<td>175</td>
<td>368</td>
<td>367</td>
<td>363</td>
<td>409</td>
<td>518</td>
<td>483</td>
<td>738</td>
<td>1277</td>
<td>1485</td>
<td>610</td>
<td>7590</td>
</tr>
<tr>
<td>Spam</td>
<td>47</td>
<td>28</td>
<td>103</td>
<td>26</td>
<td>43</td>
<td>73</td>
<td>159</td>
<td>108</td>
<td>299</td>
<td>121</td>
<td>144</td>
<td>128</td>
<td>216</td>
<td>163</td>
<td>220</td>
<td>101</td>
<td>1969</td>
</tr>
<tr>
<td>Malware</td>
<td>53</td>
<td>134</td>
<td>121</td>
<td>10</td>
<td>20</td>
<td>45</td>
<td>117</td>
<td>240</td>
<td>104</td>
<td>99</td>
<td>135</td>
<td>85</td>
<td>109</td>
<td>141</td>
<td>224</td>
<td>51</td>
<td>1688</td>
</tr>
<tr>
<td>Other</td>
<td>1</td>
<td>5</td>
<td>13</td>
<td>62</td>
<td>14</td>
<td>75</td>
<td>102</td>
<td>264</td>
<td>182</td>
<td>200</td>
<td>58</td>
<td>86</td>
<td>86</td>
<td>58</td>
<td>63</td>
<td>41</td>
<td>1309</td>
</tr>
<tr>
<td>Probe</td>
<td>3</td>
<td>14</td>
<td>25</td>
<td>12</td>
<td>26</td>
<td>86</td>
<td>42</td>
<td>13</td>
<td>26</td>
<td>171</td>
<td>141</td>
<td>68</td>
<td>67</td>
<td>69</td>
<td>12</td>
<td>775</td>
<td></td>
</tr>
<tr>
<td>Trojan</td>
<td>66</td>
<td>6</td>
<td>26</td>
<td>5</td>
<td>5</td>
<td>12</td>
<td>56</td>
<td>90</td>
<td>79</td>
<td>94</td>
<td>439</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DOS</td>
<td>2</td>
<td>4</td>
<td>2</td>
<td>68</td>
<td>72</td>
<td>32</td>
<td>37</td>
<td>12</td>
<td>14</td>
<td>7</td>
<td>16</td>
<td>16</td>
<td>11</td>
<td>3</td>
<td>298</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Botnet</td>
<td>3</td>
<td>46</td>
<td>5</td>
<td>8</td>
<td>15</td>
<td>4</td>
<td>71</td>
<td>29</td>
<td>20</td>
<td>4</td>
<td>2</td>
<td>1</td>
<td>4</td>
<td>212</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Virus</td>
<td>84</td>
<td>99</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>183</td>
</tr>
<tr>
<td>Portscan</td>
<td>10</td>
<td>4</td>
<td>1</td>
<td>6</td>
<td>1</td>
<td>3</td>
<td>2</td>
<td>5</td>
<td>6</td>
<td>13</td>
<td>16</td>
<td>3</td>
<td>29</td>
<td>7</td>
<td>2</td>
<td>1</td>
<td>109</td>
</tr>
<tr>
<td>Pharming</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>18</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>10</td>
<td>9</td>
<td>3</td>
<td></td>
<td></td>
<td>49</td>
</tr>
<tr>
<td>Other2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Outside_remit</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>sum</td>
<td>244</td>
<td>491</td>
<td>634</td>
<td>285</td>
<td>330</td>
<td>196</td>
<td>940</td>
<td>1160</td>
<td>1121</td>
<td>1008</td>
<td>1079</td>
<td>954</td>
<td>1267</td>
<td>1725</td>
<td>2067</td>
<td>822</td>
<td>14623</td>
</tr>
</tbody>
</table>

* Sensor Network is not counted to the overall sum

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

- 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 forms – public, private and our own - Turris HaaS and Sentinel
    - IntelMQ, Public blacklists of IP with detected harmful activity, other sources 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 addresses with specific devices

- 2022 - 4 940 898 registered events of 47 720 unique IP addresses it generated
  28 563 reports to 706 unique abuse contacts
PROKI

Better understanding of already known incidents – Identification of yet unreviewed 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
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
- 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
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 raspberryraspberry993311 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

Top countries by recorded incidents

<table>
<thead>
<tr>
<th>Rank</th>
<th>Country</th>
<th>Incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IR</td>
<td>1072155</td>
</tr>
<tr>
<td>2</td>
<td>RO</td>
<td>924537</td>
</tr>
<tr>
<td>3</td>
<td>US</td>
<td>57531</td>
</tr>
<tr>
<td>4</td>
<td>MX</td>
<td>30884</td>
</tr>
<tr>
<td>5</td>
<td>CN</td>
<td>24366</td>
</tr>
<tr>
<td>6</td>
<td>KW</td>
<td>22554</td>
</tr>
<tr>
<td>7</td>
<td>HK</td>
<td>21062</td>
</tr>
<tr>
<td>8</td>
<td>CZ</td>
<td>18503</td>
</tr>
<tr>
<td>9</td>
<td>IT</td>
<td>13291</td>
</tr>
<tr>
<td>10</td>
<td>VN</td>
<td>7765</td>
</tr>
<tr>
<td>11</td>
<td>RU</td>
<td>6372</td>
</tr>
<tr>
<td>12</td>
<td>PE</td>
<td>5661</td>
</tr>
<tr>
<td>13</td>
<td>GB</td>
<td>4938</td>
</tr>
<tr>
<td>14</td>
<td>CL</td>
<td>3890</td>
</tr>
<tr>
<td>15</td>
<td>UA</td>
<td>3881</td>
</tr>
</tbody>
</table>
Overview

Number of unique attackers during the time
### Most abused passwords

<table>
<thead>
<tr>
<th></th>
<th>Password</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>123456</td>
<td>17234615</td>
</tr>
<tr>
<td>2</td>
<td>1234</td>
<td>16556947</td>
</tr>
<tr>
<td>3</td>
<td>123456789</td>
<td>16125017</td>
</tr>
<tr>
<td>4</td>
<td>12345</td>
<td>12756812</td>
</tr>
<tr>
<td>5</td>
<td>1QAZ2wxx</td>
<td>2510207</td>
</tr>
<tr>
<td>6</td>
<td>P@ssw0rd</td>
<td>1239915</td>
</tr>
<tr>
<td>7</td>
<td>password</td>
<td>814462</td>
</tr>
<tr>
<td>8</td>
<td>12345678</td>
<td>722862</td>
</tr>
<tr>
<td>9</td>
<td>123</td>
<td>676016</td>
</tr>
<tr>
<td>10</td>
<td>abc123</td>
<td>442035</td>
</tr>
<tr>
<td>11</td>
<td>P@$w0rd123</td>
<td>439636</td>
</tr>
<tr>
<td>12</td>
<td>123123</td>
<td>437381</td>
</tr>
<tr>
<td>13</td>
<td>1qaz@WSX</td>
<td>428484</td>
</tr>
<tr>
<td>14</td>
<td>1</td>
<td>423737</td>
</tr>
<tr>
<td>15</td>
<td>Aa123456</td>
<td>417752</td>
</tr>
</tbody>
</table>

### Password Details

#### Password Usage during the Time

#### Password's top usernames

<table>
<thead>
<tr>
<th></th>
<th>Username</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>admin</td>
<td>59880</td>
</tr>
<tr>
<td>2</td>
<td>root</td>
<td>42716</td>
</tr>
<tr>
<td>3</td>
<td>user</td>
<td>20933</td>
</tr>
<tr>
<td>4</td>
<td>root</td>
<td>14343</td>
</tr>
<tr>
<td>5</td>
<td>user</td>
<td>13960</td>
</tr>
<tr>
<td>6</td>
<td>root</td>
<td>11089</td>
</tr>
<tr>
<td>7</td>
<td>root</td>
<td>11761</td>
</tr>
<tr>
<td>8</td>
<td>root</td>
<td>11227</td>
</tr>
<tr>
<td>9</td>
<td>user</td>
<td>10713</td>
</tr>
<tr>
<td>10</td>
<td>root</td>
<td>10338</td>
</tr>
<tr>
<td>11</td>
<td>root</td>
<td>10107</td>
</tr>
<tr>
<td>12</td>
<td>root</td>
<td>9991</td>
</tr>
<tr>
<td>13</td>
<td>user</td>
<td>9470</td>
</tr>
<tr>
<td>14</td>
<td>root</td>
<td>8837</td>
</tr>
<tr>
<td>15</td>
<td>root</td>
<td>8246</td>
</tr>
<tr>
<td>16</td>
<td>root</td>
<td>8108</td>
</tr>
<tr>
<td>17</td>
<td>root</td>
<td>8095</td>
</tr>
<tr>
<td>18</td>
<td>root</td>
<td>7837</td>
</tr>
</tbody>
</table>
Sentinel Password Checker

Check if your password had been used by hackers to access minpots 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 attacks had been captured onto.

Check password

Enter your password

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

Thank you for your attention.