CZ.NIC and CSIRT.CZ

Incident handling in 2015

Zuzana Duračinská • zuzana.duracinska@nic.cz •
15.03.2016

CZ DOMAIN REGISTRY

National CSIRT

- Roles derived from Act on Cybersecurity

  - receives notifications of contact information and incidents

  - acts as a contact point for our constituency

  - performs vulnerability assessments

  - provides methodological support, assistance and cooperation in case of cyber incident

- Roles derived from the CSIRT's 'nature'

Incident handling/response

- No executive powers
- No end users support
- IH within “only” within our constituency
- Incidents are reported to us in cases of:

  - persisting incidents

  - incidents with possible wider implications

  - incidents where the other side does not respond (or responds negatively)

  - cross border incidents (lists of IP addresses belonging to various operators)

Incident response in 2015

- 1160 reported incidents (excluding IDS) (not that big of a rise comparing to 2014)
- 376 phishing incidents
- 242 malware related incidents
- Still 'popular' targeted phishing campaigns
- Rising number of incidents related to SOHO routers

Incident handling in 2015

- 2 new employees trained on IH procedures
- Endless training needed (in technical and operational manner)
- More semi-automated IH

Incident Handling in 2015

- As a result of services integration we get new data from honeypots
- Thanks to that we have detected 22 new malware samples (double check with Virustotal)
- New samples were handed to antivirus companies
- Each month detected from 500-2000 new unique IP addresses (april-october 2015)
- Almost 50 countries were contacted

Incident Handling in 2015

- **Ramnit Botnet**

  - thanks to coordination from Europol the net of almost 3 million computers was shrinking

  - we obtained 222 emails with logs of communication with blackholes

  - over 335 thousand of records with 363 unique IP addresses

- **DoS/DdoS again and again**

  -Attacks were directed on number of czech ISPs

  - solving issues with attacks coming to and from :/ Czech Republic

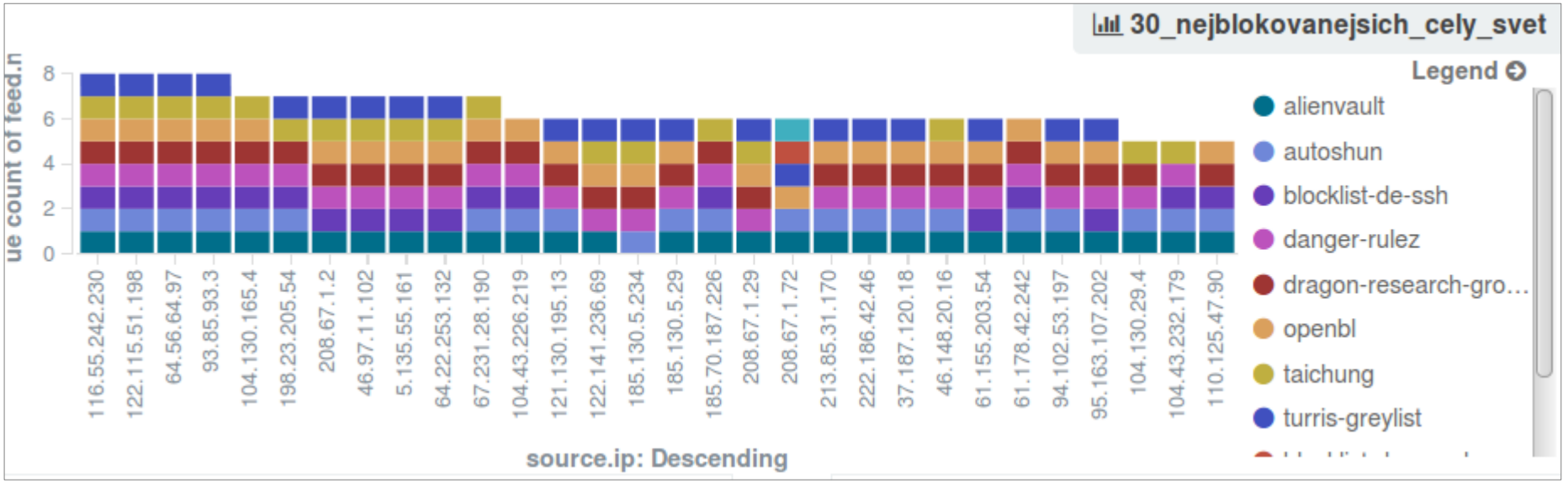
Malicious Domain Manager

- Service related to website security within .CZ ccTLD
- Open-source application developed in CZ.NIC's research dept.
- Collects information from publicly available sources about malicious URLs
- Creates a ticket about all the URL's which are malicious on the .CZ domain
- Through the app we can contact the domain owner

Malicious Domain Manager 2015

- Since 2015....
- 1. Infected domain is opened in isolated browser
- 2.Selects the domains infected website is connecting to
- 3.Analyst manually selects which domains are probably malicious
- 4.Push the selected domains either in greylists or blacklists incorporated in Turris router
- 5.Turris users connection to greylists' domains are logged / connections to blacklists domains are blocked

Contribution to greylists on Turris home router



PROKI 2015 – a new start

- Selection of security reports from CZ IP range only
- Possibility to filter through the incidents (by IP)
- Possible to follow security “trends” more closely
- Easier to follow more data sources (from the prospective of relevance)
- Operators will receive complex report for their IP range
- Looking for an good solutions (it will never be ideal)

Questions? Comments? Ideas?

Zuzana Duracinska • zuzana.duracinska@nic.cz